ArubaOS 8.3.0.x Command-Line Interface

Reference Guide

a Hewlett Packard Enterprise company

Copyright Information

© Copyright 2018 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

The ArubaOS 8.3.0.0 CLI allows you to configure and manage Mobility Master and managed devices. The CLI is accessible from a local console connected to the serial port on the Mobility Master or through a Telnet or Secure Shell (SSH) session from a remote management console or workstation.

Telnet access is disabled by default. To enable Telnet access, enter the **telnet** CLI command from a serial connection or an SSH session, or in the WebUI navigate to the **Configuration > System > Admin** page.

What's New In ArubaOS 8.3.0.0

This section lists the commands introduced, modified, or deprecated in ArubaOS 8.3.0.0.

Commands in ArubaOS 8.3.0.0

New Commands

The following new commands are introduced in ArubaOS 8.3.0.0:

Command	Description
iot transportProfile	This command configures an IoT transport profile.
iot usetransportProfile	This command sets an IoT management server profile.
show iot transportProfile	This command displays information about the IoT profile status.
show airmatch debug apinfo	This command displays information about the AirMatch debug data of an AP.
show airmatch debug db-dump status	This command displays information about the status of the AirMatch debug database dump.
show airmatch debug pathloss history rep-radio	This command displays information about the recent AirMatch debug path loss.
show airmatch network-tech-support	This command collects the output for all the radios that are in the same partition for a specified radio AP name.
show airmatch tech-support	Displays the AirMatch technical support information of an AP.
show airmatch debug advanced stat	This command displays detailed information about the AirMatch debug status of an AP.
show ble_relay disp-attr	This command shows the BLE relay attributes.
show ble_relay iot-profile	This command shows the BLE relay IoT profile details.
show ble_relay tag-report	This command shows the BLE relay tag data.
show ble_relay ws-log	This command shows the BLE relay WebSocket logs.

Modified Commands

The following commands are modified in ArubaOS 8.3.0.0:

Command	Description
aaa authentication via connection-profile	The following changes are introduced: ■ A new parameter, **tos-dscp**, is introduced to support IPsec packets with higher QoS-DSCP. ■ The description of the **whitelist** parameter is updated to display the maximum limit of allowable entries.

Command	Description
aaa profile	The following new parameters are introduced: ■ **radius-acct-session-id-in-access** ■ **reauth-wired-user-vlan-change**
ap system-profile	The following new parameters are introduced: ■ **dual-5ghz-mode** ■ **recovery-mode**
ap wired-port-profile	The following new parameters are introduced: ■ **auto-recovery-enable** ■ **auto-recovery-interval** ■ **loop-detection-interval** ■ **loop-protect-enable**
configuration device	The **A7280**option was added under the **device-model** parameter.
show ap active	The new flags, **T**, **U**, **V**, and **W** are introduced. In addition, the output parameters for this command are modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation modes for the dual 5GHz mode settings.
show ap arm client-match history	A new output value, **AS** is introduced for the **Signal** output column.
show ap arm client-match summary	A new parameter, **brief**, is introduced to display brief statistical information of the output parameters.
show ap details	The output of the command is modified to include AP Fast Recovery statistics.
show airmatch debug feasibility	The following parameters are introduced in the output of this command: ■ **Current Opmode** ■ **HW Supported Opmodes** ■ **Configured Opmodes** ■ **Feasible Opmodes** ■ **Config BW range(MHz)** ■ **Hardware BW range(MHz)** ■ **Eirp Range Chan 20MHz** ■ **Eirp Range Chan 40MHz** ■ **Eirp Range Chan 80MHz** ■ **Eirp Range Chan 160MHz** ■ **Config EIRP range(dBm)** ■ **Hardware EIRP range(dBm)** ■ **EIRP Offset(dB)** ■ **Band** ■ **Band Range**
show ap debug radio-stats	The output of this command includes MCS bucket mapping information with channel width, number of spatial streams, and guard interval information of 802.11ac APs.
show ap debug bss-stats	
show ap debug client-stats	

Command	Description
show ap wired-port-profile	The following parameters are introduced in the output of this command: ■ **Loop Protect Enable** ■ **Loop Detection Interval** ■ **Loop Protect Auto Recovery Enable** ■ **Loop Protect Auto Recovery Interval**
ssh	The **disable-ciphers** and **disable-mac** parameters have been introduced in this command to configure ciphers and MAC algorithms, respectively.
show ssh	The **ssh disable-ciphers** and **ssh disable-mac** parameters are introduced to the output of this show command.
show datapath	The **current standby entries** counter is added to the **station** parameter.

About this Guide

This guide describes the ArubaOS 8.3.0.x command syntax. The commands in this guide are listed alphabetically.

The following information is provided for each command:

- Command Syntax—The complete syntax of the command.
- Description—A brief description of the command.
- Syntax—A description of the command parameters, including license requirements for specific parameters if needed. The applicable ranges and default values, if any, are also included.
- Usage Guidelines—Information to help you use the command, including: prerequisites, prohibitions, and related commands.
- Example—An example of how to use the command.
- Command History—The version of ArubaOS in which the command was first introduced. Modifications and changes to the command are also noted.
- Command Information—This table describes any licensing requirements, command modes and platforms for which this command is applicable. For more information about available licenses, refer to the *Aruba Mobility Master Licensing Guide.*

Connecting to the Mobility Master or Managed Device

This section describes how to connect to the Mobility Master or Managed Device to use the CLI.

Serial Port Connection

The serial port is located on the front panel of the managed device. Connect a terminal or PC or workstation running a terminal emulation program to the serial port on the managed device to use the CLI. Configure your terminal or terminal emulation program to use the following communication settings.

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

The Aruba 7200 Series controller supports baud rates between 9600 and 115200.

Telnet or SSH Connection

Telnet or SSH access requires that you configure an IP address and a default gateway on Mobility Master/Managed Device and connect the Mobility Master/Managed Device to your network. This is typically performed when you run the initial setup on the Mobility Master/Managed Device, as described in the *ArubaOS 8.3.0.x Quick Start Guide*. In certain deployments, you can also configure a loopback address for the Mobility Master/Managed Device; see interface loopback on page 549 for more information.

Configuration changes on Mobility Master

Some commands can only be issued when connected to Mobility Master. If you make a configuration change on Mobility Master, all connected managed devices using that configuration will subsequently update their settings as well.

CLI Access

When you connect to the Mobility Master using the CLI, the system displays the login prompt. Log in using the admin user account and the password you entered during the initial setup on the Mobility Master . For example:

```
login as: admin
admin@192.0.2.1's password:
Last login: Sat Jun 25 01:17:11 2016 from 192.0.2.77
```

When you are logged in, the *enable* mode CLI prompt displays. For example:

```
(host) [mynode] #
```

All **show** commands and certain management functions are available in the enable (also called "privileged") mode.

Configuration commands are available in *config* mode. Move from enable mode to config mode by entering **configure terminal** at the # prompt:

```
(host) [mynode]# configure terminal
Enter Configuration commands, one per line. End with CNTL/Z
```

When you are in basic config mode, (config) appears before the # prompt:

```
(host) [mynode] (config) #
```

There are several other sub-command modes that allow users to configure individual interfaces, sub-interfaces, loopback addresses, GRE tunnels and cellular profiles. For details on the prompts and the available commands for each of these modes, see Appendix A: Command Modes on page 2692.

Command Help

You can use the question mark (**?**) to view various types of command help.

When typed at the beginning of a line, the question mark lists all the commands available in your current mode or sub-mode. A brief explanation follows each command. For example:

```
(host) [mynode] #aaa ?
authentication          Authentication
inservice               Bring authentication server into service
ipv6                    Internet Protocol Version 6
query-user              Query User
test-server             Test authentication server
user                    User commands
```

When typed at the end of a possible command or abbreviation, the question mark lists the commands that match (if any). For example:

```
(host) [mynode] #c?
ccm-debug               Centralized Configuration Module debug information
cd                      Change current config node
change-config-node      Change current config node
clear                   Clear configuration
clock                   Append clock to cli output
cluster-debug           Cluster Debug
configure               Configuration Commands
copy                    Copy Files
copy-provisioning-par.. Copy a provisioning-ap-list entry to provisioning-params
crypto                  Configure IPsec, IKE, and CA
```

If more than one item is shown, type more of the keyword characters to distinguish your choice. However, if only one item is listed, the keyword or abbreviation is valid and you can press tab or the spacebar to advance to the next keyword.

When typed in place of a parameter, the question mark lists the available options. For example:

```
(host) [mynode] #write ?
erase                    Erase and start from scratch
memory                   Write to memory
terminal                 Write to terminal
<cr>
```

The <cr> indicates that the command can be entered without additional parameters. Any other parameters are optional.

Command Completion

To make command input easier, you can usually abbreviate each key word in the command. You need type only enough of each keyword to distinguish it from similar commands. For example:

```
(host) [mynode] #configure terminal
```

could also be entered as:

```
(host) [mynode] #con t
```

Three characters (**con**) represent the shortest abbreviation allowed for **configure**. Typing only **c** or **co** would not work because there are other commands (like **copy**) which also begin with those letters. The configure command is the only one that begins with **con**.

As you type, you can press the spacebar or tab to move to the next keyword. The system then attempts to expand the abbreviation for you. If there is only one command keyword that matches the abbreviation, it is filled in for you automatically. If the abbreviation is too vague (too few characters), the cursor does not advance and you must type more characters or use the help feature to list the matching commands.

Deleting Configuration Settings

Use the **no** command to delete or negate previously-entered configurations or parameters.

- To view a list of no commands, type **no** at the enable or config prompt followed by the question mark. For example:

  ```
  (host) [mynode] (config) # no?
  ```

- To delete a configuration, use the **no** form of a configuration command. For example, the following command removes a configured user role:

  ```
  (host) [mynode] (config) # no user-role <name>
  ```

- To negate a specific configured parameter, use the **no** parameter within the command. For example, the following commands delete the DSCP priority map for a priority map configuration:

  ```
  (host) [mynode] (config) # priority-map <name>
  (host) [mynode] (config-priority-map) # no dscp priority high
  ```

Saving Configuration Changes

Mobility Master has the running configuration images. The *running-config* holds the current controller configuration, including all pending changes which have yet to be saved. To view the running-config, use the following command:

```
(host) [mynode]# show running-config
```

When you make configuration changes via the CLI, those changes affect the current running configuration only. If the changes are not saved, they will be lost after the Mobility Master reboots. To save your configuration changes so they are retained after the Mobility Master reboots, use the following command in the enable or config mode:

```
(host) ^[mynode]# write memory
Saving Configuration...
Saved Configuration
```

The running configuration can also be saved to a file or sent to a TFTP server for backup or transfer to another system.

The **^** indicator appears between the (host) and [node] portions of the command prompt if the configuration contains unsaved changes. ArubaOS includes the following command prompts:

- `(host)^[mynode]` – This indicates unsaved configuration.
- `(host)*[mynode]` – This indicates available crash information.
- `(host) [mynode]` – This indicates a saved configuration.

Commands That Reset the Mobility Master or AP

If you use the CLI to modify a currently provisioned and running radio profile, those changes take place immediately; you do not reboot the Mobility Master or the AP for the changes to affect the current running configuration. Certain commands, however, automatically force the Mobility Master or AP to reboot. You may want to consider current network loads and conditions before issuing these commands, as they may cause a momentary disruption in service as the unit resets. Note also that changing the **lms-ip** parameter in an AP system profile associated with an AP group will cause all APs in that AP group to reboot.

Table 2: *Reset Commands*

Commands that Reset an AP	Commands that Reset a Mobility Master
■ ap-regroup ■ ap-rename ■ apboot ■ provision-ap ■ ap wired-ap-profile {default | <profile-name>} forward-mode {bridge|split-tunnel|tunnel} ■ wlan virtual-ap <profile-name> {aaa-profile <profile-name> |forward-mode {tunnel|bridge|split-tunnel|decrypt-tunnel} |ssid-profile <profile-name>|vlan <vlan>...} ■ ap system-profile <profile-name> {bootstrap-threshold <number> |lms-ip <ipaddr> |} ■ wlan ssid-profile <profile-name> {battery-boost|deny-bcast|essid|opmode|strict-svp |wepkey1 <key> |wepkey2 <key>|wepkey3 <key>|wepkey4 <key>|weptxkey <index> |wmm |wmm-be-dscp <best-effort>|wmm-bk-dscp <background>|wmm-ts-min-inact-int <milliseconds>|wmm-vi-dscp <video>|wmm-vo-dscp <voice>|wpa-hexkey <psk> |wpa-passphrase <string> } ■ wlan dot11k <profile-name> {bcn-measurement-mode|dot11k-enable|force-dissasoc	■ reload

Typographic Conventions

The following conventions are used throughout this manual to emphasize important concepts:

Table 3: *Text Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
Boldface	This style is used to emphasize command names and parameter options when mentioned in the text.
`Commands`	This fixed-width font depicts command syntax and examples of commands and command output.
`<angle brackets>`	In the command syntax, text within angle brackets represents items that you should replace with information appropriate to your specific situation. For example: ping <ipaddr> In this example, you would type “ping” at the system prompt exactly as shown, followed by the IP address of the system to which ICMP echo packets are to be sent. Do not type the angle brackets.
`[square brackets]`	In the command syntax, items enclosed in brackets are optional. Do not type the brackets.
`{Item_A|Item_B}`	In the command examples, single items within curled braces and separated by a vertical bar represent the available choices. Enter only one choice. Do not type the braces or bars.
`{ap-name <ap-name>}|{ipaddr <ip-addr>}`	Two items within curled braces indicate that both parameters must be entered together. If two or more sets of curled braces are separated by a vertical bar, like in the example to the left, enter only one choice Do not type the braces or bars.

Command Line Editing

The system records your most recently entered commands. You can review the history of your actions, or reissue a recent command easily, without having to retype it.

To view items in the command history, use the *up* arrow key to move back through the list and the *down* arrow key to move forward. To reissue a specific command, press **Enter** when the command appears in the command history. You can even use the command line editing feature to make changes to the command prior to entering it. The command line editing feature allows you to make corrections or changes to a command without retyping. Table 4 lists the editing controls. To use key shortcuts, press and hold the **Ctrl** button while you press a letter key.

Table 4: Line Editing Keys

Key	Effect	Description
Ctrl A	Home	Move the cursor to the beginning of the line.
Ctrl B or the left arrow	Back	Move the cursor one character left.
Ctrl D	Delete Right	Delete the character to the right of the cursor.
Ctrl E	End	Move the cursor to the end of the line.
Ctrl F or the right arrow	Forward	Move the cursor one character right.
Ctrl K	Delete Right	Delete all characters to the right of the cursor.
Ctrl N or the down arrow	Next	Display the next command in the command history.
Ctrl P or up arrow	Previous	Display the previous command in the command history.
Ctrl T	Transpose	Swap the character to the left of the cursor with the character to the right of the cursor.
Ctrl U	Clear	Clear the line.
Ctrl W	Delete Word	Delete the characters from the cursor up to and including the first space encountered.
Ctrl X	Delete Left	Delete all characters to the left of the cursor.

Specifying Addresses and Identifiers in Commands

This section describes addresses and other identifiers that you can reference in CLI commands.

Table 5: *Addresses and Identifiers*

Address or Identifier	Description
IP address	For any command that requires entry of an IP address to specify a network entity, use IPv4 network address format in the conventional dotted decimal notation (for example, 10.4.1.258).
Netmask address	For subnet addresses, specify a netmask in dotted decimal notation (for example, 255.255.255.0).
MAC	For any command that requires entry of a device's hardware address, use the hexadecimal format (for example, 00:05:4e:50:14:aa).
SSID	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN-01).

Address or Identifier	Description
BSSID	This entry is the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency— 802.11a and 802.11g—used from the AP. Use the same format as for a MAC address.
ESSID	Typically the unique logical name of a wireless network. If the ESSID includes spaces, you must enclose the name in quotation marks.
Fast Ethernet or Gigabit Ethernet interface	Any command that references a Fast Ethernet or Gigabit Ethernet interface requires that you specify the corresponding port on the managed device in the format <slot>/<module>/<port>: Use the **show port status** command to obtain the interface information currently available from a managed device.

Contacting Support

Table 6: *Contact Information*

Main Site	arubanetworks.com
Support Site	support.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	hpe.com/networking/support
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: sirt@arubanetworks.com

aaa alias-group

```
aaa alias-group <ag-name>
   clone <group>
   no ...
   set vlan condition essid|location equals <operand> set-value <set-value-string>
```

Description

This command configures a AAA alias with set of VLAN derivation rules that could speed up user rule derivation processing for deployments with a very large number of UDRs.

Syntax

Parameter	Description
`<ag-name>`	Name of the alias group.
`clone <group>`	Copy data from another alias group.
`set vlan condition essid|location equals <operand> set-value <set-value-string>`	Specify rules to derive role and VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

aaa auth-survivability

```
aaa auth-survivability
   cache-lifetime
   enable
   server-cert
```

Description

This command configures Authentication Survivability on a managed device.

Syntax

Parameter	Description	Default
`cache-lifetime <hrs>`	This parameter specifies the lifetime in hours for the cached access credential in the local Survival Server. When the specified cache-lifetime expires, the cached access credential is deleted from the managed device. The valid range is from 1 to 72 hours.	24 hours
`enable`	This parameter controls whether to use the Survival Server when no other servers in the server group are in-service. This parameter also controls whether to store the user access credential in the Survival Server when it is authenticated by an external RADIUS or LDAP server in the server group. Authentication Survivability is enabled or disabled on each managed device. **NOTE:** Authentication survivability will not activate if the Authentication Server Dead Time is configured as 0	Disabled
`server-cert`	This parameter allows you to view the name of the server certificate used by the local Survival Server. The local Survival Server is provided with a default server certificate from AOS. The customer server certificate must be imported into the managed device first, and then you can assign the server certificate to the local Survival Server. **NOTE:** In the deployment environment, it is recommended that you switch to a customer server certificate.	—

Usage Guidelines

Use this command to configure authentication survivability on Mobility Master mode in the managed device node.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa auth-trace

```
aaa auth-trace
   loglevel
```

Description

This command sets parameters for debug tracing in AUTH (light weight tracing).

Syntax

Parameter	Description
`loglevel`	Specify the loglevel of syslogs that will be included in the trace.
`alert`	Trace all logs equal or higher than LOG_ALERT.
`critical`	Trace all logs equal or higher than LOG_CRIT.
`debug`	Trace all logs equal or higher than LOG_DEBUG.
`emergency`	Trace all logs equal or higher than LOG_EMERG.
`error`	Trace all logs equal or higher than LOG_ERR.
`info`	Trace all logs equal or higher than LOG_INFO.
`notice`	Trace all logs equal or higher than LOG_NOTICE.
`warn`	Trace all logs equal or higher than LOG_WARN.

Usage Guidelines

Use this command to set the parameters for debug tracing in AUTH (light weight tracing).

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master in the managed device node.

aaa authentication captive-portal

```
aaa authentication captive-portal <profile>
   apple-cna-bypass
   auth-protocol mschapv2|pap|chap
   black-list <black-list>
   clone <source-profile>
   default-guest-role <role>
   default-role <role>
   enable-welcome-page
   guest-logon
   ip-addr-in-redirection <ipaddr>
   login-page <url>
   logon-wait {cpu-threshold <percent>}|{maximum-delay <seconds>}|{minimum-delay <seconds>}
   logout-popup-window
   max-authentication-failures <number>
   no ...
   protocol-http
   proxy <ipaddr> port <port>
   redirect-pause <seconds>
   redirect-url <url>
   server-group <group-name>
   show-acceptable-use-policy
   show-fqdn
   single-session
   switchip-in-redirection-url
   url-hash-key <key>
   user-idle-timeout
   user-logon
   user-vlan-in-redirection-url
   welcome-page <url>
   white-list <white-list>
```

Description

This command configures a Captive Portal authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	default
`apple-cna-bypass`	Enable this knob to bypass Apple CNA on iOS devices such as iPad, iPhone, and iPod. You need to perform Captive Portal authentication from browser.	—	—
`authentication-protocol chap|mschapv2|pap`	This parameter specifies the type of authentication required by this profile, PAP is the default authentication type.	mschapv2 pap chap	pap

Parameter	Description	Range	Default
`black-list`	Name of an existing black list on an IPv4 or IPv6 network destination. The black list contains websites (unauthenticated) that a guest cannot access. Specify a netdestination host or subnet to add that netdestination to the captive portal blacklist. If you have not yet defined a netdestination, use the CLI command netdestination to define a destination host or subnet before you add it to the blacklist.	—	—
`clone`	Name of an existing Captive Portal profile from which parameter values are copied.	—	—
`default-guest-role`	Role assigned to guest.	—	guest
`default-role <role>`	Role assigned to the Captive Portal user when that user logs in. When both user and guest logons are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the guest role.	—	guest
`enable-welcome-page`	Displays the configured welcome page before the user is redirected to their original URL. If this option is disabled, redirection to the web URL happens immediately after the user logs in.	enabled or disabled	enabled
`guest-logon`	Enables Captive Portal logon without authentication.	enabled or disabled	disabled
`ipaddr-in-redirection-url`	Sends the interface IP address of the managed device in the redirection URL when external captive portal servers are used. An external captive portal server can determine the managed device from which a request originated by parsing the switchip variable in the URL.	—	—
`login-page <url>`	URL of the page that appears for the user logon. This can be set to any URL.	—	/auth/index.html
`logon-wait`	Configure parameters for the logon wait interval.	1-100	60%
`cpu-threshold <percent>`	CPU utilization percentage above which the logon wait interval is applied when presenting the user with the logon page.	1-100	60%

Parameter	Description	Range	Default
`maximum-delay <seconds>`	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.	1-10	10 seconds
`minimum-delay <seconds>`	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter.	1-10	5 seconds
`logout-popup-window`	Enables a pop-up window with the Logout link that allows the user to log out. If this option is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads.	enabled or disabled	enabled
`max-authentication-failures <number>`	Maximum number of authentication failures before the user is blacklisted.	0-10	0
`no`	Negates any configured parameter.	—	—
`protocol-http`	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captive portal policy to allow HTTP traffic.	enabled or disabled	disabled (HTTPS is used)
`proxy`	Update IP address of the proxy host.	—	—
`redirect-pause <secs>`	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.	1-60	10 seconds
`redirect-url <url>`	URL to which an authenticated user will be directed. This parameter must be an absolute URL that begins with either **http://** or **https://**.	—	—
`server-group <group-name>`	Name of the group of servers used to authenticate Captive Portal users. See aaa server-group on page 103.	—	—
`show-fqdn`	Allows the user to see and select the FQDN on the login page. The FQDNs shown are specified when configuring individual servers for the server group used with captive portal authentication.	enabled or disabled	disabled

Parameter	Description	Range	Default
`single-session`	Allows only one active user session at a time.	—	disabled
`show-acceptable-use-policy`	Show the acceptable use policy page before the login page.	enabled or disabled	disabled
`switchip-in-redirection-url`	Sends the IP address of the managed device in the redirection URL when external captive portal servers are used. An external captive portal server can determine the managed device from which a request originated by parsing the switchip variable in the URL.	enabled or disabled	disabled
`url-hash-key <key>`	Issue this command to hash the redirection URL using the specified key.	—	disabled
`user-idle-timeout`	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.	—	disabled
`user-logon`	Enables Captive Portal with authentication of user credentials.	enabled or disabled	enabled
`user-vlan-in-redirection-url`	Add the user VLAN in the redirection URL.	enabled disabled	disabled
`welcome-page <url>`	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL.	—	/auth/welcome .html
`white-list <white-list>`	Name of an existing white list on an IPv4 or IPv6 network destination. The white list contains authenticated websites that a guest can access. If you have not yet defined a netdestination, use the CLI command netdestination to define a destination host or subnet before you add it to the whitelist.	—	—

Usage Guidelines

You can configure the Captive Portal authentication profile in the base operating system or with the PEFNG license installed. When you configure the profile in the base operating system, the name of the profile must be entered for the initial role in the AAA profile. Also, when you configure the profile in the base operating system, you cannot define the default-role.

Example

The following example configures a Captive Portal authentication profile that authenticates users against the internal database. Users who are successfully authenticated are assigned the auth-guest role.

To create the auth-guest user role shown in this example, the PEFNG license must be installed in the Mobility Master.

```
(host)^[md] (config) #aaa authentication captive-portal guestnet
   (host) ^[md] (Captive Portal Authentication Profile "guestnet") #default-role auth-guest
   (host) ^[md] (Captive Portal Authentication Profile "guestnet") #user-logon
   (host) ^[md] (Captive Portal Authentication Profile "guestnet") #no guest-logon
   (host) ^[md] (Captive Portal Authentication Profile "guestnet") #server-group internal
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on managed devices.

aaa authentication dot1x

```
aaa authentication dot1x {<profile>|countermeasures}
   ca-cert <certificate>
   cert-cn-lookup
   clear
   clone <profile>
   delete-keycache
   eapol-logoff
   enforce-suite-b-128
   enforce-suite-b-192
   framed-mtu <mtu>
   heldstate-bypass-counter <number>
   ignore-eap-id-match
   ignore-eapolstart-afterauthentication
   key-cache clear
   machine-authentication blacklist-on-failure|{cache-timeout <hours>}|enable|
     {machine-default-role <role>}|{user-default-role <role>}
   max-authentication-failures <number>
   max-requests <number>
   multicast-keyrotation
   no ...
   opp-key-caching
   reauth-max <number>
   reauth-server-termination-action
   reauthentication
   reload-cert
   server {server-retry <number>|server-retry-period <seconds>}
   server-cert <certificate>
   termination {eap-type <type>}|enable|enable-token-caching|{inner-eap-type (eap-  gtc|eap-
   mschapv2)}|{token-caching-period <hours>}
   timer {idrequest_period <seconds>}|{keycache-tmout <kc-tmout>}|{mkey-rotation-period
   <seconds>}|{quiet-period   <seconds>}|{reauth-period <seconds>}|{ukey-rotation-period
   <seconds>}|{wpa-  groupkey-delay <seconds>}|{wpa-key-period <milliseconds>}|wpa2-key-delay
   <milliseconds>
   tls-guest-access
   tls-guest-role <role>
   unicast-keyrotation
   use-session-key
   use-static-key
   validate-pmkid
   wep-key-retries <number>
   wep-key-size {40|128}
   wpa-fast-handover
   wpa-key-retries <number>
   xSec-mtu <mtu>
```

Description

This command configures the 802.1X authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	default
`clear`	Clear the Cached PMK, Role and VLAN entries. This command is available in enable mode only.	—	—
`countermeasures`	Scans for message integrity code failures in traffic received from clients. If there are more than 2 message integrity code failures within 60 seconds, the AP is shut down for 60 seconds. This option is intended to slow down an attacker who is making a large number of forgery attempts in a short time.	—	disabled
`ca-cert <certificate>`	CA certificate for client authentication. The CA certificate needs to be loaded in the Mobility Master.	—	—
`ca-cert-name`	Name of the CA certificate.	—	—
`cert-cn-lookup`	If you use client certificates for user authentication, enable this option to verify that the CN of the certificate exists in the server. This parameter is disabled by default.	—	—
`delete-keycache`	Delete the key cache entry when the user entry is deleted.	—	disabled
`eapol-logoff`	Enables handling of EAPOL-LOGOFF messages.	—	disabled
`enforce-suite-b-128`	Configure Suite-B 128 bit or more security level authentication enforcement.	—	disabled
`enforce-suite-b-192`	Configure Suite-B 192 bit or more security level authentication enforcement	—	disabled
`framed-mtu <MTU>`	Sets the framed MTU attribute sent to the authentication server.	500-1500	1100

Parameter	Description	Range	Default
`heldstate-bypass-counter <number>`	This parameter is applicable when 802.1X authentication is terminated on the Mobility Master, also known as AAA FastConnect. Number of consecutive authentication failures which, when reached, causes the Mobility Master to not respond to authentication requests from a client while the Mobility Master is in a held state after the authentication failure. Until this number is reached, the Mobility Master responds to authentication requests from the client even while the Mobility Master is in its held state.	0-3	0
`ignore-eap-id-match`	Ignore EAP ID during negotiation.	—	disabled
`ignore-eapol start-afterauthentication`	Ignores EAPOL-START messages after authentication.	—	disabled
`key-cache clear`	Clears the Cached PMK, Role and VLAN.	—	—
`machine-authentication`	This parameter is applicable in Windows environments only. These parameters set machine authentication. **NOTE:** This parameter requires the PEFNG license.	—	—
`blacklist-on-failure`	Blacklists the client if machine authentication fails.	—	disabled
`cache-timeout <hours>`	The timeout, in hours, for machine authentication.	1-1000	24 hours
`enable`	Select this option to enforce machine authentication before user authentication. If selected, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful.	—	disabled
`machine-default-role <role>`	Default role assigned to the user after completing only machine authentication.	—	guest
`user-default-role <role>`	Default role assigned to the user after 802.1X authentication.	—	guest

Parameter	Description	Range	Default
`max-authentication-failures <number>`	Number of times a user can try to login with wrong credentials after which the user is blacklisted as a security threat. Set to 0 to disable blacklisting, otherwise enter a non-zero integer to blacklist the user after the specified number of failures.	0-5	0 (disabled)
`max-requests <number>`	Maximum number of times ID requests are sent to the client.	1-10	5
`multicast-key rotation`	Enables multicast key rotation	—	disabled
`no`	Negates any configured parameter.	—	—
`opp-key-caching`	Enables a cached PMK derived with a client and an associated AP to be used when the client roams to a new AP. This allows clients faster roaming without a full 802.1X authentication. **NOTE:** Make sure that the wireless client (the 802.1X supplicant) supports this feature. If the client does not support this feature, the client will attempt to renegotiate the key whenever it roams to a new AP. As a result, the key cached on the managed device can be out of sync with the key used by the client.	—	enabled
`reauth-max <number>`	Maximum number of reauthentication attempts.	1-10	3
`reauth-server-termination-action`	Specifies the termination-action attribute from the server.		
`reauthentication`	Select this option to force the client to do a 802.1X reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.) If the user fails to reauthenticate with valid credentials, the state of the user is cleared. If derivation rules are used to classify 802.1X-authenticated users, then the reauthentication timer per role overrides this setting.	—	disabled
`reload-cert`	Reload certificate for 802.1X termination. This command is available in enable mode only.	—	—

Parameter	Description	Range	Default
`server`	Sets options for sending authentication requests to the authentication server group.		
`server-retry <number>`	Maximum number of authentication requests that are sent to server group.	0-5	3
`server-retry-period <seconds>`	Server group retry interval, in seconds.	2-65535	5 seconds
`server-cert <certificate>`	Server certificate used by the managed device to authenticate itself to the client.	—	—
`termination`	Sets options for terminating 802.1X authentication on the managed device.		
`eap-type <type>`	The EAP method, either EAP-PEAP or EAP-TLS.	eap-peap or eap-tls	eap-peap
`enable`	Enables 802.1X termination on the managed device.	—	disabled
`enable-token -caching`	If you select EAP-GTC as the inner EAP method, you can enable the Mobility Master to cache the username and password of each authenticated user. The Mobility Master continues to reauthenticate users with the remote authentication server, however, if the authentication server is not available, the Mobility Master will inspect its cached credentials to reauthenticate users.	—	disabled
`inner-eap-type eap-gtc|eap-mschapv2`	When EAP-PEAP is the EAP method, one of the following inner EAP types is used: **EAP-GTC**: Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the Mobility Master as a backup to an external authentication server. **EAP-MSCHAPv2**: Described in RFC 2759, this EAP method is widely supported by Microsoft clients.	eap-gtc or eap-mschapv2	eap-mschap v2

Parameter	Description	Range	Default
token-caching-period <hours>	If you select EAP-GTC as the inner EAP method, you can specify the timeout period, in hours, for the cached information.	(any)	24 hours
timer	Sets timer options for 802.1X authentication:		
idrequest-period <seconds>	Interval, in seconds, between identity request retries.	1-65535	5 seconds
keycache-tmout	Set the per BSSID PMKSA cache interval. Cache is deleted within 2 hours of the interval.	1-2000 (hours)	8 hours
mkey-rotation-period <seconds>	Interval, in seconds, between multicast key rotation.	60-864000	1800 seconds
quiet-period <seconds>	Interval, in seconds, following failed authentication.	1-65535	30 seconds
reauth-period <seconds>	Interval, in seconds, between reauthentication attempts, or specify server to use the server-provided reauthentication period.	60-864000	86400 seconds (1 day)
ukey-rotation-period <seconds>	Interval, in seconds, between unicast key rotation.	60-864000	900 seconds
wpa-groupkey -delay <milliseconds>	Interval, in milliseconds, between unicast and multicast key exchanges.	0-2000	0 ms (no delay)
wpa-key-period <milliseconds>	Interval, in milliseconds, between each WPA key exchange.	10-5000	1000 ms
wpa2-key-delay <milliseconds>	Set the delay between EAP-Success and unicast key exchange.	1-2000	0 ms (no delay)
tls-guest-access	Enables guest access for EAP-TLS users with valid certificates.	—	disabled
tls-guest-role <role>	User role assigned to EAP-TLS guest. **NOTE:** This parameter requires the PEFNG license.	—	guest
unicast-keyrotation	Enables unicast key rotation.	—	disabled
use-session-key	Use RADIUS session key as the unicast WEP key.	—	disabled
use-static-key	Use static key as the unicast or multicast WEP key.	—	disabled

Parameter	Description	Range	Default
validate-pmkid	This parameter instructs the Mobility Master to check the PMK ID sent by the client. When this option is enabled, the client must send a PMK ID in the associate or reassociate frame to indicate that it supports OKC or PMK caching; otherwise, full 802.1X authentication takes place. (This feature is optional, since most clients that support OKC and PMK caching do not send the PMKID in their association request.)	—	disabled
wep-key-retries <number>	Number of times WPA or WPA2 key messages are retried.	1-3	2
wep-key-size	Dynamic WEP key size, either 40 or 128 bits.	40 or 128	128 bits
wpa-fast-handover	Enables WPA-fast-handover. This is only applicable for phones that support WPA and fast handover.	—	disabled
wpa-key-retries	Set the number of times WPA or WPA2 Key Messages are retried. The supported range is 1-10 retries, and the default value is 3.	1-10	3
xSec-mtu <mtu>	Sets the size of the MTU for xSec.	1024-1500	1300 bytes

Usage Guidelines

The 802.1X authentication profile allows you to enable and configure machine authentication and 802.1X termination on the managed device (also called AAA FastConnect).

In the AAA profile, specify the 802.1X authentication profile, the default role for authenticated users, and the server group for the authentication.

Examples

The following example enables authentication of the user's client device before user authentication. If machine authentication fails but user authentication succeeds, the user is assigned the restricted guest role:

```
(host) ^[md] (config) #aaa authentication dot1x dot1x
(host) ^[md] (802.1X Authentication Profile "dot1x") machine-authentication enable
(host) ^[md] (802.1X Authentication Profile "dot1x") machine-authentication machine-default-
role computer
(host) ^[md] (802.1X Authentication Profile "dot1x") machine-authentication user-default-role
guest
```

The following example configures an 802.1X profile that terminates authentication on the managed device, where the user authentication is performed with the internal database of the managed device or to a "backend" non-802.1X server:

```
(host) ^[md] (config) #aaa authentication dot1x dot1x
(host) ^[md] (802.1X Authentication Profile "dot1x") #termination enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system. The voice-aware parameter requires the PEFNG license.	Config mode on Mobility Master.

aaa authentication mac

```
aaa authentication mac <profile>
   case upper|lower
   clone <profile>
   delimiter {colon|dash|none}
   max-authentication-failures <number>
   no ...
   reauthentication
   timer reauth period {<ra-period>|server}
```

Description

This command configures the MAC authentication profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	default
`case`	The case (upper or lower) used in the MAC string sent in the authentication request. If there is no delimiter configured, the MAC address in lower case is sent in the format xxxxxxxxxxxx, while the MAC address in upper case is sent in the format XXXXXXXXXXXX.	upper lower	lower
`clone <profile>`	Name of an existing MAC profile from which parameter values are copied.	—	—
`delimiter`	Delimiter (colon, dash, none, oui-nic) used in the MAC string.	colon dash none oui-nic	none
`max-authentication-failures <number>`	Number of times a client can fail to authenticate before it is blacklisted. A value of 0 disables blacklisting.	0-10	0 (disabled)
`no`	Negates any configured parameter.	—	—
`reauthentication`	Use this parameter to enable or disable reauthentication.	—	Disabled
`timer reauth period <ra-period>|server`	**<ra-period>** specifies the period between reauthentication attempts in seconds. The **server** parameter specifies the server-provided reauthentication interval.	60-864000 seconds	86400 seconds (1 day)

Usage Guidelines

MAC authentication profile configures authentication of devices based on their physical MAC address. MAC-based authentication is often used to authenticate and allow network access through certain devices while denying access to all other devices. Users may be required to authenticate themselves using other methods, depending upon the network privileges.

Example

The following example configures a MAC authentication profile to blacklist client devices that fail to authenticate.

```
(host) ^[md] (config) #aaa authentication mac mac-blacklist
(host) ^[md] (MAC Authentication Profile "mac-blacklist") #max-authentication-failures 3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication mgmt

```
aaa authentication mgmt
   default-role {ap-provisioning|guest-provisioning|location-api-mgmt|nbapi-mgmt|network-
   operations|no-access|read-only|root|standard}
   enable
   mchapv2
   no ...
   server-group <group>
```

Description

This command configures authentication for administrative users.

Syntax

Parameter	Description	Range	Default
`default-role`	Select a predefined management role to assign to authenticated administrative users:	—	default
`ap-provisioning`	AP provisioning role.	—	—
`guest-provisioning`	Guest provisioning role.	—	—
`location-api-mgmt`	Location API management role.	—	—
`nbapi-mgmt`	NBAPI management role.	—	—
`network-operations`	Network operator role.	—	—
`read-only`	Read-only role.	—	—
`root`	Default role or superuser role.	—	—
`standard`	Standard role	—	—
`enable`	Enables authentication for administrative users.	enabled| disabled	disabled
`mchapv2`	Enable MSCHAPv2.	enabled| disabled	disabled
`no`	Negates any configured parameter.	—	—
`server-group <group>`	Name of the group of servers used to authenticate administrative users. See aaa server-group on page 103.	—	default

Usage Guidelines

If you enable authentication with this command, users configured with the **mgmt-user** command must be authenticated using the specified server-group.

You can configure the management authentication profile in the base operating system or with the PEFNG license installed.

Example

The following example configures a management authentication profile that authenticates users against the internal database f the Mobility Master. Users who are successfully authenticated are assigned the read-only role.

```
(host) [mynode] (config) aaa authentication mgmt
   default-role read-only
   server-group internal
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **standard** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication-server internal

```
aaa authentication-server internal use-local-switch
```

Description

This command specifies that the internal database on a managed device be used for authenticating clients.

Usage Guidelines

By default, the internal database in the Mobility Master is used for authentication. This command directs authentication to the internal database on the local managed device where you run the command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master executed on the managed device node.

aaa authentication-server ldap

```
aaa authentication-server ldap <server>
   admin-dn <name>
   admin-passwd <string>
   allow-cleartext
   authport <port>
   base-dn <name>
   clone <server>
   enable
   filter <filter>
   host <ipaddr>
   key-attribute <string>
   max-connection <number>
   no ...
   preferred-conn-type ldap-s|start-tls|clear-text
   timeout <seconds>
```

Description

This command configures an LDAP server.

A maximum of 128 LDAP servers can be configured on the Mobility Master.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`admin-dn <name>`	DN for the admin user who has read or search privileges across all of the entries in the LDAP database (the user does not need write privileges but should be able to search the database and read attributes of other users in the database).	—	—
`admin-passwd <string>`	Password for the admin user.	—	—
`allow-cleartext`	Allows clear-text (unencrypted) communication with the LDAP server.	enabled| disabled	disabled
`authport <port>`	Port number used for authentication. Port 636 will be attempted for LDAP over SSL-LDAP, while port 389 will be attempted for SSL over LDAP, Start TLS operation and clear text.	1-65535	389
`base-dn <name>`	DN name of the node which contains the entire user database to use.	—	—
`chase-referrals`	Chase referrals anonymously.		
`clone <server>`	Name of an existing LDAP server configuration from which parameter values are copied.	—	—

Parameter	Description	Range	Default
`enable`	Enables the LDAP server.	—	
`filter <filter>`	Filter that should be applied to search of the user in the LDAP database. The default filter string is (objectclass=*).	—	(objectclass=*)
`host <ip-addr>`	IP address of the LDAP server, in dotted-decimal format.	—	—
`key-attribute <string>`	Attribute that should be used as a key in search for the LDAP server. For PAP, the value is sAMAccountName. For EAP-TLS termination the value is userPrincipalName.	—	sAMAccountName
`max-connection`	Maximum number of simultaneous non-admin connections to an LDAP server.	—	—
`no`	Negates any configured parameter.	—	—
`preferred-conn-type`	Preferred connection type. The default order of connection type is: 1. ldap-s 2. start-tls 3. clear-text The Mobility Master will first try to contact the LDAP server using the preferred connection type, and will only attempt to use a lower-priority connection type if the first attempt is not successful. **NOTE:** You enable the **allow-cleartext** option before you select **clear-text** as the preferred connection type. If you set clear-text as the preferred connection type but do not allow clear-text, the Mobility Master will only use ldap-s or start-tls to contact the LDAP server.	ldap-s start-tls clear-text	ldap-s
`timeout <seconds>`	Timeout period of a LDAP request, in seconds.	1-30	20 seconds

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see aaa server-group on page 103).

Example

The following command configures and enables an LDAP server:

```
(host) ^[md] (config) #aaa authentication-server ldap ldap1
(host) ^[md] (LDAP Server "ldap1") #host 10.1.1.243
(host) ^[md] (LDAP Server "ldap1") #base-dn cn=Users,dc=1m,dc=corp,dc=com
(host) ^[md] (LDAP Server "ldap1") #admin-dn cn=corp,cn=Users,dc=1m,dc=corp,dc=com
(host) ^[md] (LDAP Server "ldap1") #admin-passwd abc10
(host) ^[md] (LDAP Server "ldap1") #key-attribute sAMAccountName
(host) ^[md] (LDAP Server "ldap1") #filter (objectclass=*)
(host) ^[md] (LDAP Server "ldap1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication-server radius

```
aaa authentication-server radius <rad_server_name>
   acct-modifier <profile_name>
   acctport <port>
   authport <port>
   auth-modifier <profile_name>
   called-station-id type
           {ap-group | ap-macaddr | ap-name | ipaddr | macaddr | vlan-id}
           [delimiter {colon | dash | none}] [include-ssid {enable |disable}]
   clone <server>
   cppm username <username> password <password>
   enable
   enable-ipv6
   enable-radsec
   host <ipaddr>|<FQDN>
   key <psk>
   mac-delimiter [colon | dash | none | oui-nic]
   mac-lowercase
   nas-identifier <string>
   nas-ip <ipaddr>
   nas-ip6 <ipv6-adrress>
   no
   radsec-client-cert-name <name>
   radsec-port <radsec-port>
   radsec-trusted-cacert-name <radsec-trusted-ca>
   radsec-trusted-servercert-name <name>
   retransmit <number>
   service-type-framed-user
   source-interface vlan <vlan> ip6addr <ipv6addr>
   timeout <seconds>
   use-ip-for-calling-station
   use-md5
```

Description

This command configures a RADIUS server.

Syntax

Parameter	Description	Range	Default
`<rad_server_name>`	Name that identifies the server.	—	—
`acct-modifier <profile_name>`	Attributes modifier for accounting-request.	—	—
`acctport <port>`	Accounting port on the server.	1-65535	1813
`authport <port>`	Authentication port on the server	1-65535	1812
`auth-modifier`	Attributes modifier for access-request.	—	—

Parameter	Description	Range	Default
`called-station-id type {ap-group | ap-macaddr | ap-name | ipaddr | macaddr | vlan-id}`	Configure this parameter to be sent with the RADIUS attribute Called Station ID for authentication and accounting requests. The **called-station-id** parameter can be configured to include AP group, AP MAC address, AP name, Mobility Master IP, Mobility Master MAC address, or user vlan. The default value is Mobility Master MAC address.	—	macaddr
`clone <server>`	Name of an existing RADIUS server configuration from which parameter values are copied.	—	—
`cppm username <username> password <password>`	Configure the ClearPass Policy Manager username and password. The Mobility Master authenticating to ClearPass Policy Manager is enhanced to use configurable username and password instead of support password. The support password is vulnerable to attacks as the server certificate presented by ClearPass Policy Manager server is not validated.	—	—
`enable`	Enables the RADIUS server.	—	—
`enable-ipv6`	Enables the RADIUS server in IPv6 mode.	—	—
`enable-radsec`	Enables RadSec for RADIUS data transport over TCP and TLS.	—	—
`host`	Identify the RADIUS server either by its IP address or FQDN.	—	—
`<ipaddr>`	IPv4 or IPv6 address of the RADIUS server.	—	—
`<FQDN>`	FQDN of the RADIUS server. The maximum supported length is 63 characters.	—	—
`key <psk>`	Shared secret between the Mobility Master and the authentication server. The maximum length is 128 characters.	—	—
`mac-delimiter [colon | dash | none | oui-nic]`	Send MAC address with user-defined delimiter.	—	none
`mac-lowercase`	Send MAC addresses as lowercase.	—	—
`nas-identifier <string>`	NAS identifier to use in RADIUS packets.	—	—

Parameter	Description	Range	Default
`nas-ip <ip-addr>`	The NAS IP address to be sent in RADIUS packets from that server. If you define a local NAS IP setting using this command and also define a global NAS IP using the command **ip radius nas-ip <ip-addr>**, the global NAS IP address takes precedence.	—	—
`nas-ip6 <ipv6-address>`	NAS IPv6 address to send in RADIUS packets. You can configure a global NAS IPv6 address that the Mobility Master uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IPv6, the global NAS IPv6 is used. To set the global NAS IPv6, enter the **ipv6 radius nas-ip6 <ipv6-address>** command.	—	—
`no`	Negates any configured parameter.	—	—
`radsec-client-cert <radsec-client-cert>`	Configures a RadSec client certificate on the RADIUS server to identify and authenticate clients.	—	—
`radsec-port <radsec-port>`	Designates a RadSec port for RADIUS data transport.	1-65535	2083
`radsec-trusted-cacert-name <radsec-trusted-ca>`	Designates a CA to sign RadSec certificates.	—	—
`radsec-trusted-servercert-name <radsec-trusted-ca>`	Designates a trusted RadSec server certificate.	—	—
`retransmit <number>`	Maximum number of retries sent to the server by the Mobility Master before the server is marked as down.	0-3	3
`service-type-framed-user`	Send the service-type as FRAMED-USER instead of LOGIN-USER. This option is disabled by default.	—	disabled

Parameter	Description	Range	Default
`source-interface vlan <vlan> ip6addr <ipv6addr>`	This option associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. ■ If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet will be that interface's IP address. ■ If you do not associate the Source Interface with a configured server (leave the field blank), then the IP address of the global Source Interface will be used. ■ If you want to configure an IPv6 address for the Source Interface, specify the IPv6 address for the **ip6addr** parameter.	—	—
`timeout <seconds>`	Maximum time, in seconds, that the Mobility Master waits before timing out the request and resending it.	1-30	5 seconds
`use-ip-for-calling-station`	Use an IP address instead of a MAC address for calling station IDs. This option is disabled by default.	—	disabled
`use-md5`	Use MD5 hash of cleartext password.	—	disabled

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see aaa server-group on page 103).

Example

The following command configures and enables a RADIUS server:

```
(host) [md] (config) #aaa authentication-server radius radius
(host) [md] (RADIUS Server "radius") #host 10.1.1.244
(host) [md] (RADIUS Server "radius") #key qwERtyuIOp
(host) [md] (RADIUS Server "radius") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **acct-modifier** and **auth-modifier** parameters were introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication-server tacacs

```
aaa authentication-server tacacs <server>
   clone <source>
   enable
   host <host>
   key <psk>
   no ...
   retransmit <number>
   session-authorization
   source-interface
   tcp-port <port>
   timeout <seconds>
```

Description

This command configures a TACACS+ server.

A maximum of 128 TACACS servers can be configured on the Mobility Master.

Syntax

Parameter	Description	Range	Default
`<server>`	Name that identifies the server.	—	—
`clone <source>`	Name of an existing TACACS server configuration from which parameter values are copied.	—	—
`enable`	Enables the TACACS server.	—	
`host <host>`	IPv4 or IPv6 address of the TACACS server.	—	—
`key`	Shared secret to authenticate communication between the TACACS client and server.	—	—
`no`	Negates any configured parameter.	—	—
`retransmit <number>`	Maximum number of times a request is retried.	0-3	3
`session-authorization`	Enables TACACS+ authorization. Session-authorization turns on the optional authorization session for admin users.	—	disabled
`source-interface`	Select source address of outgoing TACACS requests to the server.	—	—
`vlan <vlan_id>`	Select VLAN of outgoing TACACS requests to the server.	1-4094	—
`tcp-port <port>`	TCP port used by the server.	1-65535	49
`timeout <timeout>`	Timeout period of a TACACS request, in seconds.	1-30	20 seconds

Usage Guidelines

You configure a server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see aaa server-group on page 103).

Example

The following command configures, enables a TACACS+ server and enables session authorization:

```
(host) ^[md] (config) #aaa authentication-server tacacs tacacs1
(host) ^[md] (TACACS Server "tacacs1")clone default
(host) ^[md] (TACACS Server "tacacs1")host 10.1.1.245
(host) ^[md] (TACACS Server "tacacs1")key qwERtyuIOp
(host) ^[md] (TACACS Server "tacacs1")enable
(host) ^[md] (TACACS Server "tacacs1")session-authorization
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **source-interface** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication-server windows

```
aaa authentication-server windows <windows_server_name>
   clone <source>
   domain <domain>
   enable
   host <ipaddr>
   no
```

Description

This command configures a windows server for stateful-NTLM authentication.

Syntax

Parameter	Description
`<windows_server_name>`	Name of the windows server. You will use this name when you add the windows server to a server group.
`clone <source>`	Name of a Windows Server from which you want to make a copy.
`domain <domain>`	The Windows domain for the authentication server.
`enable`	Enables the Windows server.
`host <ipaddr>`	IP address of the Windows server.
`no`	Delete command.

Usage Guidelines

You must define a Windows server before you can add it to one or more server groups. You create a server group for a specific type of authentication (see aaa server-group on page 103). Windows servers are used for stateful-NTLM authentication.

Example

The following command configures and enables a windows server:

```
(host) ^[md] (config) #aaa authentication-server windows IAS_1
(host) ^[md] (Windows Server "IAS_1") #host 10.1.1.245
(host) ^[md] (Windows Server "IAS_1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication stateful-dot1x

```
aaa authentication stateful-dot1x
   default-role <role>
   enable
   no ...
   server-group <group>
   timeout <seconds>
```

Description

This command configures 802.1X authentication for clients on non-Aruba APs.

Syntax

Parameter	Description	Range	Default
`default-role <role>`	Role assigned to the 802.1X user upon login. **NOTE:** The PEFNG license must be installed.	—	guest
`enable`	Enables 802.1X authentication for clients on non-Aruba APs. Use **no enable** to disable stateful 8021.X authentication.	—	enabled
`no`	Negates any configured parameter.	—	—
`server-group <group>`	Name of the group of RADIUS servers used to authenticate the 802.1X users. See aaa server-group on page 103.	—	—
`timeout <seconds>`	Timeout period, in seconds.	1-20	10 seconds

Usage Guidelines

This command configures 802.1X authentication for clients on non-Aruba APs. The Mobility Master maintains user session state information for these clients.

Example

The following command assigns the employee user role to clients who successfully authenticate with the server group corp-rad:

```
(host) ^[md] (config) aaa authentication stateful-dot1x
   default-role employee
   server-group corp-rad
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication stateful-dot1x clear

```
aaa authentication stateful-dot1x clear
```

Description

This command clears automatically-created control path entries for 802.1X users on non-Aruba APs.

Syntax

No parameters.

Usage Guidelines

Run this command after changing the configuration of a RADIUS server in the server group configured with the **aaa authentication stateful-dot1x** command. This causes entries for the users to be created in the control path with the updated configuration information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master in the managed device node.

aaa authentication stateful-kerberos

```
aaa authentication stateful-kerberos <profile-name>
   clone
   default-role <role>
   no
   server-group <server-group>
   timeout <timeout>
```

Description

This command configures stateful Kerberos authentication.

Syntax

Parameter	Description	Range	Default
`clone <source>`	Create a copy of an existing stateful Kerberos profile	—	—
`default-role`	Select an existing role to assign to authenticated users.	—	guest
`no`	Negates any configured parameter.	—	—
`server-group <server-group>`	Name of a server group.	—	default
`timeout <timeout>`	Amount of time, in seconds, before the request times out.	1-20 seconds	10 seconds

Example

```
(host) ^[md] (config) #aaa authentication stateful-kerberos default
(host) ^[md] (Stateful Kerberos Authentication Profile "default") #default-role guest
(host) ^[md] (Stateful Kerberos Authentication Profile "default") #timeout 10
(host) ^[md] (Stateful Kerberos Authentication Profile "default") #server-group internal
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication stateful-ntlm

```
aaa authentication stateful-ntlm <profile-name>
   clone
   default-role <role>
   enable
   no
   server-group <server-group>
   timeout <timeout>
```

Description

This command configures stateful NTLM authentication.

Syntax

Parameter	Description	Range	Default
`clone`	Create a copy of an existing stateful NTLM profile	—	—
`default-role`	Select an existing role to assign to authenticated users.	—	guest
`enable`	Enables stateful ntlm authentication profile for clients. Use **no enable** to disable stateful ntlm authentication.	—	enabled
`no`	Negates any configured parameter.	—	—
`server-group <server-group>`	Name of a server group.	—	default
`timeout <timeout>`	Amount of time, in seconds, before the request times out.	1-20 seconds	10 seconds

Usage Guidelines

NTLM is a suite of Microsoft authentication and session security protocols. You can use a stateful NTLM authentication profile to configure a managed device to monitor the NTLM authentication messages between clients and an authentication server. The managed device can then use the information in the SMB headers to determine the username and IP address of the client, the server IP address and the current authentication status client. If the client successfully authenticates via an NTLM authentication server, the managed device can recognize that the client has been authenticated and assign that client a specified user role. When the user logs off or shuts down the client machine, the user will remain in the authenticated role until the user's authentication is aged out.

The stateful NTLM Authentication profile requires that you specify a server group which includes the servers performing NTLM authentication, and a default role to be assigned to authenticated users. For details on defining a windows server used for NTLM authentication, see aaa authentication-server windows.

Example

The following example configures a stateful NTLM authentication profile that authenticates clients via the server group "Windows1." Users who are successfully authenticated are assigned the "guest2" role.

```
(host) ^[md] (config) #aaa authentication stateful-ntlm ntlm1
(host) ^[md] (Stateful NTLM Authentication Profile "ntlm1") #default-role guest2
```

```
(host) ^[md] (Stateful NTLM Authentication Profile "ntlm1") #server-group Windows1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication via auth-profile

```
aaa authentication via auth-profile <profile>
   auth-protocol {mschapv2|pap}
   cert-cn-lookup
   client-cert-enable
   clone <source>
   default-role <default-role>
   desc <description>
   max-authentication-failures <max-authentication-failures>
   no
   pan-integration
   radius-accounting <server_group_name>
   rfc-3576-server <rfc-server>
   server-group <server-group>
```

Description

This command configures the VIA authentication profile.

Syntax

Parameter	Description	Default
`auth-protocol {mschapv2|pap}`	Authentication protocol support for VIA authentication; MSCHAPv2 or PAP	PAP
`cert-cn-lookup`	Check certificate CN against AAA server.	Enabled
`client-cert-enable`	If selected, this option enables client certificate-based authentication for VPN profile download.	Disabled
`clone <source>`	Name of an existing profile from which configuration values are copied.	—
`default-role <default-role>`	Name of the default VIA authentication profile.	—
`desc <description>`	Description of this profile for reference.	—
`max-authentication-failures <max-authentication-failures>`	Number of times VIA will prompt user to login due to incorrect credentials. After the maximum authentication attempts failures VIA will exit.	0
`pan-integration`	Requires IP mapping at Palo Alto Network.	—
`radius-accounting <server_group_name>`	Server group for RADIUS accounting.	—
`rfc-3576-server <rfc-server>`	Configures the RFC 3576 server.	—
`server-group <server-group>`	Server group against which the user is authenticated.	—

Usage Guidelines

Use this command to create VIA authentication profiles and associate user roles to the authentication profile.

Example

```
(host) [md] (config) #aaa authentication via auth-profile default
(host) [md] (VIA Authentication Profile "default") #auth-protocol mschapv2
(host) [md] (VIA Authentication Profile "default") #default-role example-via-role
(host) [md] (VIA Authentication Profile "default") #desc "Default VIA Authentication Profile"
(host) [md] (VIA Authentication Profile "default") #server-group "via-server-group"
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication via connection-profile

```
aaa authentication via connection-profile <profile>
   admin-logoff-script
   admin-logon-script
   allow-user-disconnect
   allow-whitelist-traffic
   auth-profile
   auth_domain_suffix
   auto-launch-supplicant
   auto-login
   auto-upgrade
   banner-message-reappear-timeout <mins>
   block-dest-traffic
   block-destination-traffic-selector
   certificate-criteria
   client-logging
   client-netmask
   client-wlan-profile <client-wlan-profile> position <position>
   clone <source>
   controllers-load-balance
   csec-gateway-url <URL>
   csec-http-ports <comma separated port numbers>
   dn-profile
   dns-suffix-list <dns-suffix-list>
   domain-pre-connect
   DPC-generate-profile
   enable-csec
   enable-fips
   enable-supplicant
   ext-download-url <ext-download-url>
   ike-policy <ike-policy>
   ikev2-policy
   ikev2-proto
   ikev2auth
   ipsec-cryptomap map <map> number <number>
   ipsecv2-cryptomap
   lockdown-all-settings
   max-reconnect-attempts <max-reconnect-attempts>
   max-timeout <value>
   minimized
   no
   ocsp-responder
   save-passwords
   server
   split-tunneling
   suiteb-crypto
   support-email
   tos-dscp {0-63}
   tunnel
   user-idle-timeout
   validate-server-cert
   whitelist
   windows-credentials
```

Description

This command configures the VIA connection profile.

Syntax

Parameter	Description	Default
`admin-logoff-script`	Enables VIA logoff script.	Disabled
`admin-logon-script`	Enables VIA logon script.	Disabled
`allow-user-disconnect`	Enable or disable users to disconnect their VIA sessions.	Enabled
`allow-whitelist-traffic`	If enabled, this feature will block network access until the VIA VPN connection is established.	Disabled
`auth-profile <auth-profile>`	This is the list of VIA authentication profiles that will be displayed to users in the VIA client.	—
`auth_domain_suffix`	Enables a domain suffix on VIA Authentication, so client credentials are sent as *domainname\username* instead of just *username*.	—
`auto-launch-supplicant`	Allows you to connect automatically to a configured WLAN network.	Disabled
`auto-login`	Enable or disable VIA client to auto login and establish a secure connection to the managed device.	Enabled
`auto-upgrade`	Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the managed device.	Enabled
`banner-message-reappear-timeout`	Timeout value, in minutes, after which the user session will end and the VIA Login banner message reappears.	1440 minutes
`block-destination-traffic-selector-ON`	Turn ON feature to block Destination Traffic .	—
`block-dest-traffic-address`	Destination Traffic selector.	—

Parameter	Description	Default
`certificate-criteria`	Allows admin users to filter the certificates that can be used to establish the IPsec connection when a user certificate or EAP-TLS is used as the authentication method. Use the following certificate attributes or OIDs to set the certificate criteria: ■ **commonName** (OID 2.5.4.3) ■ **organizationalUnitName** (OID 2.5.4.11) ■ **organizationName** (OID 2.5.4.10) ■ **subjectAltName** (OID 2.5.29.17) ■ **certificateIssuer** (OID 2.5.29.29) ■ **userPrincipalName** (OID 1.3.6.1.4.1.311.20.2.3) ■ **emailAddress** (OID 1.2.840.113549.1.9.1) ■ **friendlyName** (OID 1.2.840.113549.1.9.20) The maximum length is 256 characters. Each attribute or OID must be separated by a semicolon. If an attribute or OID contains any spaces, the entire string must be enclosed in quotation marks.	—
`client-logging`	Enable or disable VIA client to auto login and establish a secure connection to the managed device.	Enabled
`client-netmask <client-netmask>`	The network mask that has to be set on the client after the VPN connection is established.	255.255.255.255
`client-wlan-profile <client-wlan-profile>`	A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config to configure or manage their wireless networks.	—
`clone <source>`	Create a copy of connection profile from an another VIA connection profile.	—

Parameter	Description	Default
`controllers-load-balance`	Enable this option to allow the VIA client to failover to the next available selected randomly from the list as configured in the VIA Servers option. If disabled, VIA will failover to the next in the sequence of ordered list of VIA servers.	Disabled
`csec-gateway-url`	Specify the content security service providers URL here. You must provide a FQDN.	—
`csec-http-ports`	Specify the ports (separated by comma) that will be monitored by the content security service provider. Do not add space before or after the comma.	—
`dn-profile` `CN | ORG | OU | Country`	Configure VIA dn profile.	—
`dns-suffix-list <dns-suffix-list>`	The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established.	None
`domain-preconnect`	Enable this option to allow users with lost or expired passwords to establish a VIA connection to corporate network. This option authenticates the user's device and establishes a VIA connection that allows users to reset credentials and continue with corporate access.	Enabled
`dpc-generate-profile`	Optionally enable generating common profile in DPC is enabled.	—
`enable-csec`	Use this option to enable the content security service.	—
`enable-fips`	Enable the VIA FIPS module so VIA checks for FIPS compliance during startup.	Disabled
`enable-supplicant`	If enabled, VIA starts in bSec mode using L2 suite-b cryptography. This option is disabled by default.	Disabled
`ext-download-url <ext-download-url>`	End users will use this URL to download VIA on their computers.	—

Parameter	Description	Default
`ike-policy <ike-policy>`	List of IKE policies that the VIA Client has to use to connect to the managed device.	—
`ikev2-policy`	List of IKE V2 policies that the VIA Client has to use to connect to the managed device.	—
`ikev2-proto`	Enable this to use IKEv2 protocol to establish VIA sessions.	Disabled
`ikev2auth`	Use this option to set the IKEv2 authentication method. By default user certificate is used for authentication. The other supported methods are EAP-MSCHAPv2, EAP-TLS. The EAP authentication is done on an external RADIUS server.	User Certificates
`ipsec-cryptomap`	List of IPsec crypto maps that the VIA client uses to connect to the managed device. These IPsec Crypto Maps are configured in the CLI using the `crypto-local ipsec-map <ipsec-map-name>` command.	—
`ipsecv2-cryptomap`	List of IPsec V2 crypto maps that the VIA client uses to connect to the managed device.	—
`lockdown-all-settings`	Allows you to lock down all user-configured settings.	Disabled
`max-reconnect-attempts <max-reconnect-attempts>`	The maximum number of re-connection attempts by the VIA client due to authentication failures.	3
`max-timeout value <value>`	The maximum time (minutes) allowed before the VIA session is disconnected.	1440 min
`minimized`	Use this option to keep the VIA client on a Microsoft Windows operating system minimized to system tray.	—
`ocsp-responder`	OSCP Cert Verification.	—
`enable`	Enable or disable OCSP Cert verification.	—

Parameter	Description	Default
fallback	Action taken when OCSP Cert verification result is unknown.	—
save-passwords	Enable or disable users to save passwords entered in VIA.	Enabled
server	Configure VIA servers.	—
addr <addr>	This is the public IP address or the DNS hostname of the managed device connected to VIA . Users will connect to remote server using this IP address or the host name.	—
<internal-ip <internal-ip>	This is the IP address of any of the VLAN interface IP addresses belongs to this managed device.	—
desc <description>	This is a human-readable description of the managed device.	—
split-tunneling	Enable or disable split tunneling. ■ If enabled, all traffic to the VIA tunneled networks will go through the managed device and the rest is just bridged directly on the client. ■ If disabled, all traffic will flow through the managed device.	off
suiteb-crypto	Use this option to enable Suite-B cryptography. See RFC 4869 for more information about Suite-B cryptography.	Disabled
support-email	The support e-mail address to which VIA users will send client logs.	None
tos-dscp {0-63}	Use this to mark IPsec packets with higher QoS/DSCP than Best Effort. The range is 0–63.	0

Parameter	Description	Default
`tunnel address <address>`	A list of network destination (IP address and netmask) that the VIA client will tunnel through the managed device. All other network destinations will be reachable directly by the VIA client. Enter tunneled IP address and its netmask.	—
`address <address>`		—
`netmask <netmask>`		—
`user-idle-timeout`	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.	Disabled
`validate-server-cert`	Enable or disable VIA from validating the server certificate presented by the managed device.	Enabled
`whitelist addr`	Specify a hostname or IP address and network mask to define a whitelist of users allowed to access the network if the allow-whitelist-traffic option is enabled. **NOTE:** The maximum number of entries allowed is 16.	—
`addr <addr>`	Host name of IP address of a client	—
`netmask <netmask>`	Netmask, in dotted decimal format	—
`description <description>`	(Optional) description of the client	—
`windows-credentials`	Enable or disable the use of the Windows credentials to login to VIA. If enabled, the SSO feature can be utilized by remote users to connect to internal resources.	Enabled

Usage Guidelines

Issue this command to create a VIA connection profile. A VIA connection profile contains settings required by VIA to establish a secure connection to the managed device. You can configure multiple VIA connection profiles. A VIA connection profile is always associated to a user role and all users belonging to that role will use the configured settings. If you do not assign a VIA connection profile to a user role, the default connection profile is used.

Example

The following example shows a simple VIA connection profile:

```
(host) [md] (config) #aaa authentication via connection-profile "via"
(host) [md] (VIA Connection Profile "via") #server addr 202.100.10.100 internal-ip 10.11.12.13
desc "VIA Primary" position 0
(host) [md] (VIA Connection Profile "via") #auth-profile "default" position 0
(host) [md] (VIA Connection Profile "via") #tunnel address 10.0.0.0 netmask 255.255.255.0
(host) [md] (VIA Connection Profile "via") #split-tunneling
(host) [md] (VIA Connection Profile "via") #windows-credentials
(host) [md] (VIA Connection Profile "via") #client-netmask 255.0.0.0
(host) [md] (VIA Connection Profile "via") #dns-suffix-list mycorp.com
(host) [md] (VIA Connection Profile "via") #dns-suffix-list example.com
(host) [md] (VIA Connection Profile "via") #support-email via-support@example.com
(host) [md] (VIA Connection Profile "via") #certificate-criteria certificateIssuer="HPE Root
CA"; 2.5.4.10=SmartCard; emailAddress=support@example.com
```

To configure the **tos-dscp** parameter in the CLI, use the following commands in the managed device node:

```
(host) [mynode] (config) #aaa authentication via connection-profile <profile-name>
(host) [mynode] (VIA Connection Profile "<profile-name>") #tos-dscp <0-63>
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The **tos-dscp** parameter was introduced.
ArubaOS 8.1.0.0	The **certificate-criteria** parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication via global-config

```
aaa authentication via global-config
   no
   ssl-fallback-enable
```

Description

The global config option allows you to enable SSL fallback mode. If the SSL fallback mode is enabled, the VIA client will use SSL to create a secure connection.

Syntax

Parameter	Description	Default
`no`	Disable SSL fallback option.	—
`ssl-fallback-enable`	Use this option to enable an SSL fallback connection.	Disabled

Example

```
(host) [md] (config) #aaa authentication via global-config
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master in the managed device node.

aaa authentication via web-auth

```
aaa authentication via web-auth default
   auth-profile <auth-profile> position <position>
   clone <source>
   no
```

Description

A VIA web authentication profile contains an ordered list of VIA authentication profiles. The web authentication profile is used by end users to login to the VIA download page (*https://<server-IP-address>/via*) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select one during the client login.

Syntax

Parameter	Description	Default
`auth-profile <auth-profile>`	The name of the VIA authentication profile	—
`position <position>`	The position of the profile to specify the order of selection.	—
`clone <source>`	Duplicate an existing authentication profile.	—

Example

```
(host) [md] (config) #aaa authentication via web-auth default
(host) [md] (VIA Web Authentication "default") #auth-profile default position 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

aaa authentication vpn

```
aaa authentication vpn <profile-name>
   cert-cn-lookup
   clone <source>
   default-role <guest>
   export-route
   max-authentication-failures <number>
   no ...
   pan-integration
   radius-accounting
   server-group <group>
   user-idle-timeout
```

Description

This command configures VPN authentication settings.

Syntax

Parameter	Description	Default
`<profile-name>`	There are three VPN profiles: **default**, **default-rap** or **default-cap**. This allows users to use different AAA servers for VPN, Remote AP and Campus AP clients. **NOTE:** The **default** and **default-rap** profiles are configurable. The **default-cap** profile is not configurable and is predefined with the default settings.	—
`cert-cn-lookup`	If you use client certificates for user authentication, enable this option to verify that the CN of the certificate exists in the server. This parameter is enabled by default in the default-cap and default-rap VPN profiles, and disabled by default on all other VPN profiles.	—
`clone <source>`	Copies data from another VPN authentication profile. Source is the profile name from which the data is copied.	—
`default-role <role>`	Role assigned to the VPN user upon login. **NOTE:** This parameter requires PEF for VPN Users license.	guest
`export-route`	Exports a VPN IP address as a route to the external world. See the show ip ospf command to view the link-state advertisement types that are generated.	enabled

Parameter	Description	Default
`max-authentication-failures <number>`	Maximum number of authentication failures before the user is blacklisted. The supported range is 1-10 failures. A value of 0 disables blacklisting. **NOTE:** This parameter requires the RFProtect license.	0 (disabled)
`no`	Negates any configured parameter.	—
`pan-integration`	Require IP mapping at Palo Alto Networks firewalls.	disabled
`radius-accounting`	Configure server group for RADIUS accounting	—
`server-group <group>`	Name of the group of servers used to authenticate VPN users. See aaa server-group on page 103.	internal
`user-idle-timeout`	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.	—

Usage Guidelines

This command configures VPN authentication settings for VPN, Remote AP and Campus AP clients. Use the **vpdn group** command to configure L2TP or IPsec or a PPTP VPN connection. (See vpdn group l2tp on page 2525.)

Example

The following command configures VPN authentication settings for the default-rap profile:

```
(host) ^[md] (config) #aaa authentication vpn default-rap
(host) ^[md] (VPN Authentication Profile "default-rap")default-role guest
(host) ^[md] (VPN Authentication Profile "default-rap")clone default
(host) ^[md] (VPN Authentication Profile "default-rap")max-authentication-failures 0
(host) ^[md] (VPN Authentication Profile "default-rap")server-group vpn-server-group
```

The following message appears when a user tries to configure the non-configurable default-cap profile:

```
(host) ^[md] (config) #aaa authentication vpn default-cap
Predefined VPN Authentication Profile "default-cap" is not editable
```

The following example describes the steps to use the CLI to configure a VPN for Cisco Smart Card Clients using certificate authentication and IKEv1, where the client is authenticated against user entries added to the internal database:

```
(host) ^[md] (config) #aaa authentication vpn default
  server-group internal

(host) ^[md] (config) #no crypto-local isakmp xauth

(host) ^[md] (config) #vpdn group l2tp
```

```
  enable
  client dns 101.1.1.245

(host) ^[md] (config) #ip local pool sc-clients 10.1.1.1 10.1.1.250

(host) ^[md] (config) #crypto-local isakmp server-certificate MyServerCert
(host) ^[md] (config) #crypto-local isakmp ca-certificate TrustedCA

(host) ^[md] (config) #crypto isakmp policy 1
  authentication rsa-sig
```

The following command configures client entries in the internal database:

```
(host) [mynode] #local-userdb add username <name> password <password>
```

The following example configures a VPN for XAuth IKEv1 clients in config mode using a username and password:

```
(host) ^[md] (config) #aaa authentication vpn default
  server-group internal

crypto-local isakmp xauth

(host) ^[md] (config) #vpdn group l2tp
  enable
  client dns 101.1.1.245

(host) ^[md] (config) #ip local pool pw-clients 10.1.1.1 10.1.1.250

(host) ^[md] (config) #crypto isakmp key 0987654 address 0.0.0.0 netmask 0.0.00

(host) ^[md] (config) #crypto isakmp policy 1
  authentication pre-share
```

Enter the following command to configure client entries in the internal database:

```
(host) [mynode] #local-userdb add username <name> password <password>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters. The **default-role** parameter requires PEF for VPN Users license.	Config mode on Mobility Master.

aaa authentication wired

```
aaa authentication wired
   blacklist-time <timer>
   no ...
   profile <aaa-profile>
```

Description

This command configures authentication for a client device that is directly connected to a port on the managed device.

Syntax

Parameter	Description
`blacklist-time <timer>`	Sets the time to blacklist the user. Range: 1-65535 seconds. Default: 3600 seconds.
`no`	Negates any configured parameter.
`profile <aaa-profile>`	Name of the AAA profile that applies to wired authentication. This profile must be configured for a Layer-2 authentication, either 802.1X or MAC. See aaa profile on page 91.

Usage Guidelines

This command references an AAA profile that is configured for MAC or 802.1X authentication. The port on the managed device to which the device is connected must be configured as untrusted.

Example

The following commands configure an AAA profile for 802.1X authentication and a wired profile that references the AAA profile:

```
(host) ^[md] (config) aaa profile sec-wired
   dot1x-default-role employee
   dot1x-server-group sec-svrs
(host) ^[md] (config) aaa authentication wired
   profile sec-wired
```

Related Commands

Command	Description
vlan	Assign an AAA profile to an individual VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the managed device.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **blacklist-time** parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa authentication wispr

```
aaa authentication wispr
   agent string
   clone <source>
   default-role <role>
   logon-wait {cpu-threshold <cpu-threshold>}|{maximum-delay <maximum-delay>}|{minimum-delay
   <minimum-delay>}
   no ...
   max-authentication-failures
   server-group <server-group>
   wispr-location-id-ac <wispr-location-id-ac>
   wispr-location-id-cc <wispr-location-id-cc>
   wispr-location-id-isocc <wispr-location-id-isocc>
   wispr-location-id-network <wispr-location-id-network>
   wispr-location-name-location <wispr-location-name-location>
   wispr-location-name-operator-name <wispr-location-name-operator>
```

Description

This command configures WISPr authentication with the WISPr RADIUS server of an ISP.

Syntax

Parameter	Description
`agent string`	User Agent String to be registered for use in WISPR Profile. Max User Agent String len: 32 characters.Max number of User Agent string: 32.
`clone <source>`	Copy data from another WISPr Authentication Profile.
`default-role`	Default role assigned to users that complete WISPr authentication.
`logon-wait`	Configure the CPU utilization threshold that will trigger logon wait maximum and minimum times.
`CPU-threshold <cpu-threshold>`	Percentage of CPU utilization at which the maximum and minimum login wait times are enforced. Range: 1-100%. Default: 60%.
`max-authentication-failures`	Maximum auth failures before user is blacklisted. Range: 0-10. Default: 0.
`maximum-delay <maximum-delay>`	If the CPU utilization of a managed device has surpassed the **CPU-threshold** value, the **maximum-delay** parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 10 seconds.
`minimum-delay <minimum-delay>`	If the CPU utilization of a managed device has surpassed the **CPU-threshold** value, the **minimum-delay** parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 5 seconds.
`wispr-location-id-ac <wispr-location-id-ac>`	The E.164 Area Code in the WISPr Location ID.

Parameter	Description
`wispr-location-id-cc <wispr-location-id-cc>`	The 1-3 digit E.164 Country Code in the WISPr Location ID.
`wispr-location-id-isocc <wispr-location-id-isocc>`	The ISO Country Code in the WISPr Location ID.
`wispr-location-id-network <wispr-location-id-network>`	The SSID or network name in the WISPr Location ID.
`wispr-location-name-location <wispr-location-name-location>`	A name identifying the hotspot location. If no name is defined, the default ap-name is used.
`wispr-location-name-operator-name <wispr-location-name-operator>`	A name identifying the hotspot operator.

Usage Guidelines

WISPr authentication allows a smart client to remain authenticated on the network when they roam between WISPs, even if the wireless hotspot uses an ISP for which the client may not have an account.

If you are hotstpot operator using WISPr authentication, and a client that has an account with your ISP attempts to access the Internet at your hotspot, then your ISP's WISPr AAA server authenticates that client directly, and allows the client access on the network. If, however, the client only has an account with a partner ISP, then your ISP's WISPr AAA server will forward that client's credentials to the partner ISP's WISPr AAA server for authentication. Once the client has been authenticated on the partner ISP, it will be authenticated on your hotspot's own ISP, as per their service agreements. Once your ISP sends an authentication message to the managed device, the managed device assigns the default WISPr user role to that client.

ArubaOS supports the following smart clients, which enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification redirect, proxy, authentication and logoff messages within HTML messages to the managed device.

- iPass
- Bongo
- Trustive
- weRoam
- AT&T

A WISPr authentication profile includes parameters to define RADIUS attributes, the default role for authenticated WISPr users, maximum numbers of authenticated failures and logon wait times. The WISPr-Location-ID sent from the managed device to the WISPr RADIUS server will be the concatenation of the ISO Country Code, E.164 Country Code, E.164 Area Code and SSID or Zone parameters configured in this profile.

The parameters to define WISPr RADIUS attributes are specific to the RADIUS server your ISP uses for WISPr authentication; contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites www.iso.org and www.itu.int.

A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, you must also configure the **NAS identifier** parameter in the RADIUS server profile for the WISPr server

Example

The following commands configure an WISPr authentication profile:

```
(host) ^[md] (config) aaa authentication wispr
```

```
default-role authuser
max-authentication-failures 5
server-group wispr1
wispr-location-id-ac 408
wispr-location-id-cc 1
wispr-location-id-isocc us
wispr-location-id-network <wispr-location-id-network>
wispr-location-name-location <wispr-location-name-location>
wispr-location-name-operator-name <wispr-location-name-location>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa bandwidth-contract

```
aaa bandwidth-contract <name> {kbits <kbits>}|{mbits <mbits>}|{percentage <percentage>}
```

Description

This command configures a bandwidth contract.

Syntax

Parameter	Description	Range
<name>	Name that identifies this bandwidth contract.	—
kbits <kbwm>	Limit the traffic rate for this bandwidth contract to a specified number of Kbps.	256-2000000
mbits <mbwm>	Limit the traffic rate for this bandwidth contract to a specified number of Mbps.	1-2000
percentage <pbwm>	Specify bandwidth as percentage of link capacity.	1-100%

Usage Guidelines

You can apply a configured bandwidth contract to a user role or to a VLAN. When you apply a bandwidth contract to a user role (see user-role on page 2509), you specify whether the contract applies to upstream traffic (from the client to the managed device) or downstream traffic (from the managed device to the client). You can also specify whether the contract applies to all users in a specified user role or per-user in a user role.

When you apply a bandwidth contract to a VLAN (see interface vlan on page 571), the contract limits multicast traffic and does not affect other data. This is useful because an AP can only send multicast traffic at the rate of the slowest associated client. Thus excessive multicast traffic will fill the buffers of the AP, causing frame loss and poor voice quality. Generally, every system should have a bandwidth contract of 1 Mbps or even 700 Kbps and it should be applied to all VLANs with which users are associated, especially those VLANs that pass through the upstream router. The exception are VLANs that are used for high speed multicasts, where the SSID is configured without low data rates.

Example

The following commands configure a set of bandwidth contracts, then apply those contracts to all upstream and downstream traffic except for the echo, icmp, iperf, icmp6, and synflood applications, and the web, streaming, peer-to-peer, unified-communication, and tunneling application categories.

```
(host) ^[md] (config) #aaa bandwidth-contract up-256k-1 kbits 256
(host) ^[md] (config) #aaa bandwidth-contract up-512k-1 kbits 512
(host) ^[md] (config) #aaa bandwidth-contract up-1m-1 mbits 1
(host) ^[md] (config) #aaa bandwidth-contract up-5m-1 mbits 5
(host) ^[md] (config) #aaa bandwidth-contract up-10m-1 mbits 10
(host) ^[md] (config) #aaa bandwidth-contract up-20m-1 mbits 20
(host) ^[md] (config) #aaa bandwidth-contract up-50m-1 mbits 50
(host) ^[md] (config) #aaa bandwidth-contract up-100m-1 mbits 100
(host) ^[md] (config) #aaa bandwidth-contract up-500m-1 mbits 500
(host) ^[md] (config) #aaa bandwidth-contract up-1000m-1 mbits 1000
(host) ^[md] (config) #aaa bandwidth-contract dw-256k-1 kbits 256
(host) ^[md] (config) #aaa bandwidth-contract dw-512k-1 kbits 512
(host) ^[md] (config) #aaa bandwidth-contract dw-1m-1 mbits 1
(host) ^[md] (config) #aaa bandwidth-contract dw-5m-1 mbits 5
```

```
(host) ^[md] (config) #aaa bandwidth-contract dw-10m-1 mbits 10
(host) ^[md] (config) #aaa bandwidth-contract dw-20m-1 mbits 20
(host) ^[md] (config) #aaa bandwidth-contract dw-50m-1 mbits 50
(host) ^[md] (config) #aaa bandwidth-contract dw-100m-1 mbits 100
(host) ^[md] (config) #aaa bandwidth-contract dw-500m-1 mbits 500
(host) ^[md] (config) #aaa bandwidth-contract dw-1000m-1 mbits 1000
(host) ^[md] (config) #interface gigabitethernet 0/0/1
```

Related Commands

Command	Description	Mode
interface gigabitethernet	Apply a bandwidth contract to downstream or upstream traffic on a specified interface.	Config mode.
show aaa bandwidth-contracts	Use this command to view contracts to limit traffic for a user or VLAN.	Managed device mode (/md)

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa derivation-rules

```
aaa derivation-rules user <name>
   no ...
   set {role|vlan} condition <rule-type> <attribute> <value> set-value {<role>|<vlan>}
   [description <rule description>][position <number>]
```

Description

This command configures rules which assigns a AAA profile, user role or VLAN to a client based upon the client's association with an AP.

A user role cannot be assigned by an AAA derivation rule unless the managed device has a PEFNG license.

Syntax

Parameter	Description
`<name>`	Name that identifies this set of UDRs.
`no`	Negates a configured rule.
`set {role|vlan}`	Specify whether the action of the rule is to set the role or the VLAN.
`condition`	Condition that should be checked to derive role or VLAN.
`<rule-type>`	For a rule that sets an AAA profile, use the **user-vlan** rule type. For a role or VLAN UDR, select one of the following rules: ■ **bssid**: BSSID of access point. ■ **dhcp-option**: Use DHCP signature matching to assign a role or VLAN. ■ **dhcp-option-77**: Enable DHCP packet processing. ■ **encryption-type**: Encryption method used by station. ■ **essid**: ESSID of access point. ■ **location**: user location (AP name). ■ **macaddr**: MAC address of user. **NOTE:** If you use the **dhcp-option** rule type, best practices are to enable the **enforce-dhcp** option in the AAA profile referenced by Virtual AP profile of the AP group.
`<attribute><value>`	Specify one of the following conditions: ■ **contains**: Check if attribute *contains* the string in the <value> parameter. ■ **ends-with**: Check if attribute *ends with* the string in the <value> parameter. ■ **equals**: Check if attribute *equals* the string in the <value> parameter. ■ **not-equals**: Check if attribute *is not equal* to the string in the <value> parameter. ■ **starts-with**: Check if attribute *starts with* the string in the <value> parameter.
`set-value <role>|<vlan>`	Specify the user role or VLAN ID to be assigned to the client if the above condition is met.
`description`	Describes the UDR. This parameter is optional and has a 128 character maximum.
`position`	Position of this rule relative to other rules that are configured.

Usage Guidelines

The user role can be derived from attributes from the client's association with an AP. UDRs are executed before the client is authenticated.

You configure the user role to be derived by specifying condition rules; when a condition is met, the specified user role is assigned to the client. You can specify more than one condition rule; the order of rules is important as the first matching condition is applied. You can also add a description of the rule.

The table below describes the conditions for which you can specify a user role or VLAN.

Rule Type	Condition	Value
bssid: Assign client to a role or VLAN based upon the BSSID of AP to which client is associating.	One of the following: ■ contains ■ ends with ■ equals ■ does not equal ■ starts with	MAC address (xx:xx:xx:xx:xx:xx)
dhcp-option: Assign client to a role or VLAN based upon the DHCP signature ID.	One of the following: ■ equals ■ starts with	DHCP signature ID. **NOTE:** This string is *not* case sensitive.
dhcp-option-77: Assign client to a role or VLAN based upon the user class identifier returned by DHCP server.	equals	string
encryption-type: Assign client to a role or VLAN based upon the encryption type used by the client.	One of the following: ■ equals ■ does not equal	■ Open (no encryption) ■ WPA or WPA2 AES ■ WPA-TKIP (static or dynamic) ■ Dynamic WEP ■ WPA or WPA2 AES PSK ■ Static WEP ■ xSec
essid: Assign client to a role or VLAN based upon the ESSID to which the client is associated.	One of the following: ■ contains ■ ends with ■ equals ■ does not equal ■ starts with ■ value of (does not take *string*; attribute value is used as role)	string
location: Assign client to a role or VLAN based upon the AP name to which the client is associated.	One of the following: ■ equals ■ does not equal	string
macaddr: MAC address of the client.	One of the following: ■ contains ■ ends with ■ equals ■ does not equal ■ starts with	MAC address (xx:xx:xx:xx:xx:xx)

The device identification feature allows you to assign a user role or VLAN to a specific device type by identifying a DHCP option and signature for that device. If you create a user rule with the **DHCP-Option** rule type, the first two characters in the **Value** field must represent the hexadecimal value of the DHCP option that this rule should match, while the rest of the characters in the **Value** field indicate the DHCP signature the rule should match. To create a rule that matches DHCP option 12 (host name), the first two characters of the in the **Value** field must be the hexadecimal value of 12, which is 0C. To create a rule that matches DHCP option 55, the first two characters in the **Value** field must be the hexadecimal value of 55, which is 37.

The following table describes some of the DHCP options that are useful for assigning a user role or VLAN.

DHCP Option	Description	Hexidecimal Equivalent
12	Host name	0C
55	Parameter Request List	37
60	Vendor Class Identifier	3C
81	Client FQDN	51

To identify DHCP strings used by an individual device, access the CLI in config mode and issue the following command to include DHCP option values for DHCP-DISCOVER and DHCP-REQUEST frames in the log file of the managed device:

```
logging level debugging network process dhcpd
```

Now, connect the device you want to identify to the network, and issue the CLI command **show log network**. The sample below is an example of the output that may be generated by this command.

Be aware that each device type may not have a unique DHCP fingerprint signature. For example, devices from different manufacturers may use vendor class identifiers that begin with similar strings. If you create a DHCP-Option rule that uses the starts-with condition instead of the equals condition, the rule may assign a role or VLAN to more than one device type.

```
(host) ^[md] (config) #show log network all | include DISCOVER
Feb 26 02:50:34 :202534:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan1: DISCOVER 00:19:d2:01:0b:84
Options 74:01 3d:010019d2010b84 0c:736861626172657368612d39393730 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b
Feb 26 02:50:42 :202534:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan1: DISCOVER 00:19:d2:01:0b:84
Options 74:01 3d:010019d2010b84 0c:736861626172657368612d39393730 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b
Feb 26 02:50:42 :202534:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan1: DISCOVER 00:19:d2:01:0b:84
Options 74:01 3d:010019d2010b84 0c:736861626172657368612d39393730 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b
Feb 26 02:53:03 :202534:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan10: DISCOVER
00:26:c6:52:6b:7c Options 74:01 3d:010026c6526b7c 0c:41525542412d46416c73653232
3c:4d53465420352e30 37:010f03062c2e2f1f21f92b 2b:dc00
...

(host) ^[md] (config) #show log network all| include REQUEST
Feb 26 02:53:04 :202536:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan10: REQUEST 00:26:c6:52:6b:7c
reqIP=10.10.10.254 Options 3d:010026c6526b7c 36:0a0a0a02 0c:41525542412d46416c73653232
51:00000041525542412d46416c736532322e73757279612e636f6d 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b 2b:dc0100
Feb 26 02:53:04 :202536:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan10: REQUEST 00:26:c6:52:6b:7c
reqIP=10.10.10.254 Options 3d:010026c6526b7c 36:0a0a0a02 0c:41525542412d46416c73653232
51:00000041525542412d46416c736532322e73757279612e636f6d 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b 2b:dc0100
```

```
Feb 26 02:56:02 :202536:  <DBUG> |dhcpdwrap| |dhcp| Datapath vlan10: REQUEST 00:26:c6:52:6b:7c
reqIP=10.10.10.254 Options 3d:010026c6526b7c 0c:41525542412d46416c73653232
51:00000041525542412d46416c736532322e73757279612e636f6d 3c:4d53465420352e30
37:010f03062c2e2f1f21f92b 2b:dc0100
```

Examples

The following command sets the client's user role to "guest" if the client associates to the "Guest" ESSID. The rule description indicates that is was created for special customers.

```
(host) ^[md] (config) aaa derivation-rules user derive1
   set role condition essid equals Guest set-value guest description
   createdforspecialcustomers
```

The example rule shown below sets a user role for clients whose host name (DHCP option 12) has a value of 6C6170746F70, which is the hexadecimal equivalent of the ASCII string "laptop". The first two digits in the Value field are the hexadecimal value of 12 (which is 0C), followed by the specific signature to be matched.

```
(host) ^[md] (config) aaa derivation-rules user device-role
   set role condition dhcp-option equals 0C6C6170746F70 set-value laptop_role
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system. The PEFNG license must be installed for a user role to be assigned.	Config mode on Mobility Master.

aaa dns-query-interval

```
aaa dns-query-interval <minutes>
```

Description

Configure how often the managed device should generate a DNS request to cache the IP address for a RADIUS server identified via its FQDN.

Syntax

Parameter	Description	Default
`<minutes>`	Specify, in minutes, the interval between DNS requests sent from the managed device to the DNS server. Range: 1-1440 minutes.	15 minutes.

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the managed device will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to configure the frequency of these requests.

Example

This command configures a DNS query interval of 30 minutes.

```
(host) ^[md] (config)# aaa dns-query-interval 30
```

Related Commands

To view the current DNS query interval, issue the command show aaa dns-query-interval.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa inservice

```
aaa inservice <server-group> <server>
```

Description

This command designates an “out of service” authentication server to be “in service”.

Syntax

Parameter	Description
`<server-group>`	Server group to which this server is assigned.
`<server>`	Name of the configured authentication server.

Usage Guidelines

By default, Mobility Master marks an unresponsive authentication server as “out of service” for a period of 10 minutes (you can set a different time limit with the **aaa timers dead-time** command). The **aaa inservice** command is useful when you become aware that an “out of service” authentication server is again available before the dead-time period has elapsed. You can use the **aaa test-server** command to test the availability and response of a configured authentication server.

Example

The following command sets an authentication server to be in service:

```
aaa inservice corp-rad rad1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

aaa ipv6 user add

```
aaa ipv6 user add <ipv6addr>
   authentication-method {dot1x|stateful-dot1x}
   mac <macaddr>
   name <username>
   profile <aaa-profile>
   role <role>
```

Description

This command manually assigns a user role or other values to a specified IPv6 client.

Syntax

Parameter	Description
`<ipv6addr>`	IPv6 address of the user to be added.
`authentication-method`	Authentication method for the client.
`dot1x`	802.1X authentication.
`stateful-dot1x`	Stateful 802.1X authentication.
`mac <macaddr>`	MAC address of the client.
`name <username>`	Name of the client.
`profile <aaa-profile>`	AAA profile for the client.
`role <role>`	User role for the client.

Usage Guidelines

This command should only be used for troubleshooting issues with a specific IPv6 client. This command allows you to manually assign a client to a role. For example, you can create a role “debugging” that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the “debugging” role to a specific client. Use the **aaa ipv6 user delete** command to remove the client or device from the role.

Issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the “employee” role when you assign them to the “debugging” role, the client continues any sessions allowed with the “employee” role. Use the **aaa ipv6 user clear-sessions** command to clear ongoing sessions.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific IPv6 client:

```
(host) [\md] (config) #ip access-list session ipv6-log-https
(host) [\md] (config-submode) #any any svc-https permit log
(host) [\md] (config) #user-role ipv6-web-debug
(host) [\md] (config-submode) #session-acl ipv6-log-https

(host) [\md] (config) #aaa ipv6 user add 2002:d81f:f9f0:1000:e409:9331:1d27:ef44 role
ipv6-web-debug
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa ipv6 user clear-sessions

```
aaa ipv6 user clear-sessions <ipaddr>
```

Description

This command clears ongoing sessions for the specified IPv6 client.

Syntax

Parameter	Description
`<ipv6addr>`	IPv6 address of the client.

Usage Guidelines

This command clears any ongoing sessions that the client already had before being assigned a role with the **aaa ipv6 user add** command.

Example

The following command clears ongoing sessions for an IPv6 client:

```
(host) [/md] (config) #aaa user clear-sessions 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

aaa ipv6 user delete

```
aaa ipv6 user delete {<ipv6addr>|all|mac <macaddr>|name <username>|role <role>}
```

Description

This command deletes IPv6 clients, users, or roles.

Syntax

Parameter	Description
`<ipv6addr>`	IPv6 address of the client to be deleted.
`all`	Deletes all connected IPv6 clients.
`mac <macaddr>`	MAC address of the IPv6 client to be deleted.
`name <username>`	Name of the IPv6 client to be deleted.
`role <role>`	Role of the IPv6 client to be deleted.

Usage Guidelines

This command allows you to manually delete clients, users, or roles. For example, if you used to the **aaa ipv6 user add** command to assign a user role to an IPv6 client, you can use this command to remove the role assignment.

Example

The following command a role:

```
(host) [/md] (config) #aaa ipv6 user delete role web-debug
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa ipv6 user logout

```
aaa ipv6 user logout <ipv6addr>
```

Description

This command logs out an IPv6 client.

Syntax

Parameter	Description
`<ipv6addr>`	IPv6 address of the client to be logged out.

Usage Guidelines

This command logs out an authenticated IPv6 client. The client must reauthenticate.

Example

The following command logs out an IPv6 client:

```
(host) [/md] (config) #aaa user logout 2002:d81f:f9f0:1000:e409:9331:1d27:ef44
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa log

```
[no] aaa log
```

Description

Enable per-user log files for AAA events.

Syntax

No parameters

Usage Guidelines

By default, logging is always enabled. Issue the **no aaa log** command to disable per-user logging and re-enable it again using the command **aaa log**.

Example

The example below enables per-user AAA log files.

```
(host) ^[md] (config) #aaa log
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa password-policy mgmt

```
aaa password-policy mgmt
   enable
   no
   password-lock-out
   password-lock-out-time
   password-max-character-repeat.
   password-min-digit
   password-min-length
   password-min-lowercase-characters
   password-min-special-character
   password-min-special-character
   password-min-uppercase-characters
   password-not-username
```

Description

Define a policy for creating management user passwords.

Syntax

Parameter	Description
`enable`	Enable the password management policy.
`password-lock-out`	The number of failed attempts within a 3 minute window that causes the user to be locked out for the period of time specified by the password-lock-out-time parameter. Range: 0-10 attempts. By default, the password lockout feature is disabled, and the default value of this parameter is 0 attempts.
`password-lock-out-time`	The number of minutes a user who has exceeded the maximum number of failed password attempts is locked out of the network. After this period has passed, the lockout is cleared without administrator intervention. Range: 1 min to 1440 min (24 hrs). Default: 3. **NOTE:** When a management user gets locked out, that event is logged in the managed device log file. The management user lockout warning message can have any one of the following warning IDs. ■ 125060 = Password policy locked out a management user created via the **mgmt-user** command in the serial console CLI. ■ 125061 = Password policy locked out a management user created via the WebUI or the **mgmt-user** command in the Telnet or SSH CLI. ■ 133109 = Password policy locked out a management user created via the **local-userdb** command in the CLI.
`password-max-character-repeat`	The maximum number of consecutive repeating characters allowed in a management user password. Range: 0-10 characters. By default, there is no limitation on the numbers of character that can repeat within a password, and the parameter has a default value of 0 characters.

Parameter	Description
password-min-digit	The minimum number of numeric digits required in a management user password. Range: 0-10 digits. By default, there is no requirement for numerical digits in a password, and the parameter has a default value of 0.
password-min-length	The minimum number of characters required for a management user password Range: 6-64 characters. Default: 6.
password-min-lowercase-characters	The minimum number of lowercase characters required in a management user password. Range: 0-10 characters. By default, there is no requirement for lowercase letters in a password, and the parameter has a default value of 0.
password-min-special-characters	The minimum number of special characters (!, @, #, $, %, ^, &, *, <, >, {, }, [,], :, ., comma, |, +, ~, `) in password. Range: 0-10 special characters. Default: 0 (minimum number of special character required is disabled by default, The following (')', '(' ;, -, space, =, /, ?) are dis-allowed).
password-min-special-character	The minimum number of special characters required in a management user password. Range: 0-10 characters. By default, there is no requirement for special characters in a password, and the parameter has a default value of 0. See Usage Guidelines below for a list of allowed and disallowed special characters
password-min-uppercase-characters	The minimum number of uppercase characters required in a management user password. Range: 0-10 characters. By default, there is no requirement for uppercase letters in a password, and the parameter has a default value of 0.
password-not-username	Password cannot be the current username or the username spelled backwards of the management user.

Usage Guidelines

By default, the password for a management user has no requirements other than a minimum length of 6 alphanumeric or special characters. You do not need to configure a different management user password policy unless your company enforces a best practices password policy for management users with root access to network equipment.

Example

The following command sets a management password policy that requires the password to have a minimum of nine characters, including one numerical digit and one special character:

```
(host) ^[md] (config) aaa password-policy mgmt
   enable
   password-min-digit 1
   password-min-length 9
   password-min-special-characters 1
```

Related Commands

Command	Description	Mode
show aaa password-policy mgmt	Use show aaa password-policy mgmt to show the current management password policy.	Managed device mode.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa profile

```
aaa profile <profile>
   authentication-dot1x <dot1x-profile>
   authentication-mac <mac-profile>
   clone <profile>
   devtype-classification
   dot1x-default-role <role>
   dot1x-server-group <group>
   download-role
   enforce-dhcp
   initial-role <role>
   l2-auth-fail-through
   mac-default-role <role>
   mac-server-group <group>
   max-ip ipv4 wireless <max_ipv4_users>
   multiple-server-accounting
   no ...
   open ssid radius accounting
   pan-integration
   radius-accounting <group>
   radius-acct-session-id-in-access
   radius-interim-accounting
   radius-roam-accounting
   reauth-wired-user-vlan-change
   rfc-3576-server <ipaddr>
   user-derivation-rules <profile>
   user-idle-timeout
   username-from-dhcp-opt12

   wired-to-wireless-roam
   xml-api-server <ipaddr>
```

Description

This command configures the authentication for a WLAN.

Syntax

Parameter	Description	Default
`<profile>`	Name that identifies this instance of the profile. The name must be 1-63 characters.	"default"
`authentication-dot1x <dot1x-profile>`	Name of the 802.1X authentication profile associated with the WLAN. See aaa authentication dot1x on page 24.	—
`authentication-mac <mac-profile>`	Name of the MAC authentication profile associated with the WLAN. See aaa authentication mac on page 32.	—
`clone <profile>`	Name of an existing AAA profile configuration from which parameter values are copied.	—

Parameter	Description	Default
`devtype-classification`	The device identification feature can automatically identify different client device types and operating systems by parsing the User-Agent strings in a client's HTTP packets. When the devtype-classification parameter is enabled, the output of the **show user** and **show user-table** commands shows each client's device type, if that client device can be identified.	enabled
`dot1x-default-role <role>`	Configured role assigned to the client after 802.1X authentication. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. **NOTE:** This parameter requires the PEFNG license.	guest
`dot1x-server-group <group>`	Name of the server group used for 802.1X authentication. See aaa server-group on page 103.	—
`download-role`	Enables role download from ClearPass Policy Manager if not defined.	disabled
`enforce-dhcp`	When you enable this option, clients must complete a DHCP exchange to obtain an IP address. Best practices are to enable this option, when you use the aaa derivation-rules command to create a rule with the DHCP-Option rule type. This parameter is disabled by default.	disabled
`initial-role <role>`	Role for unauthenticated users.	logon
`l2-auth-fail-through`	To select different authentication method if one fails.	disabled
`mac-default-role <role>`	Configured role assigned to the user when the device is MAC authenticated. If derivation rules are present, the role assigned to the client through these rules take precedence over the default role. **NOTE:** This parameter requires the PEFNG license.	guest
`mac-server-group group`	Name of the server group used for MAC authentication. See aaa server-group on page 103.	—
`max-ip ipv4 wireless <max_ipv4_users>`	Control the number of IPv4 addresses that can be associated to single wireless user. Range: 1-32 **WARNING:** Increasing the max-ip limit may prevent the system from scaling to maximum users on all Mobility Master or managed devices. For more information, refer to Usage Guidelines for max-ip IPv4 Wireless on page 95.	2

Parameter	Description	Default
`multiple-server-accounting`	If enabled, the Mobility Master sends RADIUS accounting to all servers in RADIUS accounting server group.	disabled
`no`	Negates any configured parameter.	—
`open ssid radius accounting`	Initiates RADIUS accounting as soon as the user associates to an Open SSID without any authentication. **NOTE:** Do not enable this parameter for wired users. If enabled, the Mobility Master sends RADIUS accounting packets for unauthenticated wired users.	disabled
`pan-integration`	The profile requires mapping at a Palo Alto Networks (PAN) firewall.	disabled
`radius-accounting <group>`	Name of the server group used for RADIUS accounting. See aaa server-group on page 103.	—
`radius-acct-session-id-in-access`	Use this to include **Acct-Session-Id** in RADIUS Access-Request.	—
`radius-interim-accounting`	By default, the RADIUS accounting feature sends only start and stop messages to the RADIUS accounting server. Issue the interim-radius-accounting command to allow the managed device to send Interim-Update messages with current user statistics to the server at regular intervals.	disabled
`rfc-3576-server <ip-addr>`	IP address of a RADIUS server that can send user disconnect, session timeout and CoA messages, as described in RFC 3576, Dynamic Authorization Extensions to RADIUS. See aaa rfc-3576-server on page 101. **NOTE:** This parameter requires the PEFNG license.	—
`radius-roam-accounting`	Enable the managed device to send Interim-Update messages (without user statistics) to the server, when a client roams to a different AP.	—
`reauth-wired-user-vlan-change`	Reauthenticate a wired user when changing VLANs.	—
`user-derivation-rules <profile>`	User attribute profile from which the user role or VLAN is derived.	—

Parameter	Description	Default
`user-idle-timeout`	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.	disabled
`username-from-dhcp-opt12`	Enter a username from dhcp option 12 for non-802.1X users.	—
`wired-to-wireless-roam`	Keeps user authenticated when roaming from the wired side of the network.	enabled
`xml-api-server <ip-addr>`	IP address of a configured XML API server. See aaa xml-api on page 123. **NOTE:** This parameter requires the PEFNG license.	—

Usage Guidelines

The AAA profile defines the user role for unauthenticated users, the default user role for MAC or 802.1X authentication, and UDRs. The AAA profile contains the authentication profile and authentication server group.

There are predefined AAA profiles available, default-dot1x, default-mac-auth, and default-open. These profiles have the parameter values shown in the following table.

Parameter	default-dot1x	default-mac-auth	default-open
`authentication-dot1x`	default	N/A	N/A
`authentication-mac`	N/A	default	N/A
`dot1x-default-role`	authenticated	guest	guest
`dot1x-server-group`	N/A	N/A	N/A
`initial-role`	logon	logon	logon
`mac-default-role`	guest	authenticated	guest
`mac-server-group`	default	default	default
`radius-accounting`	N/A	N/A	N/A
`rfc-3576-server`	N/A	N/A	N/A
`user-derivation-rules`	N/A	N/A	N/A
`wired-to-wireless roam`	enabled	enabled	enabled

Usage Guidelines for max-ip IPv4 Wireless

Changing the **max-ip ipv4 wireless** parameter from the default value is recommended for special deployments. If your WLAN has multiple device IP associated to single MAC address, you can increase the this value from the default value of 2.

The default value is 2 IPv4 users per wireless user. Total number of IPv4 users created can be a maximum of two times the license. If you configure 32 max-ip IPv4 users , total number of IPv4 users is 32 times the license. This can prevent the managed device from scaling to the maximum limit of IP users. Total number of IPv4 users should be scaled down to offset this issue.

Increasing the value of the **max-ip ipv4 wireless** parameter may increase the look-up time due to an increase in the creation and deletion of IPv4 users on the managed device. In a deployment where there is Captive Portal and 802.1X authentication implemented, increasing the number of IPv4 users can further deplete performance.

Example

The following command configures an AAA profile that assigns the employee role to clients after they are authenticated using the 802.1X server group radiusnet.

```
(host) ^[md] (config) #aaa profile corpnet
(host) ^[md] (AAA Profile "corpnet")dot1x-default-role employee
(host) ^[md] (AAA Profile "corpnet")dot1x-server-group radiusnet
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **radius-roam-accounting** parameter was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

aaa query-user

```
aaa query-user <auth-server> <user-name> <mac-address>
```

Description

Troubleshoot an authentication failure by verifying that the user exists in the authentication server database.

Syntax

Parameter	Description
`<auth-server>`	Name of a configured authentication server.
`<user-name>`	Name of a user whose authentication record you want to view.
`<mac-address>`	MAC address of the client.

Usage Guidelines

If the Admin-DN binds successfully but the wireless user fails to authenticate, issue this command to troubleshoot whether the problem is with the wireless network, the managed device, or the authentication server. The **aaa query-user <auth_server> <username> <mac-address>** command to make the managed device sends a search query to find the user. If that search fails in spite of the user being in the server database, it is most probable that the base DN where the search was started was not correct. In such case, it is advisable to make the base DN at the root of the authentication server tree.

Example

The example below shows part of the output for an LDAP record for the username JDOE.

```
(host) [mynode] #aaa query-user eng JDOE
(host) [mynode] #objectClass: top
(host) [mynode] #objectClass: person
(host) [mynode] #objectClass: organizationalPerson
(host) [mynode] #objectClass: user
(host) [mynode] #cn: John Doe
(host) [mynode] #sn: Doe
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012H\011\333K
(host) [mynode] #userCertificate: 0\202\005\2240\202\004|\240\003\002\001\002\002\012]
\350\346F
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012\023\001\017\240
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012\031\224/\030
(host) [mynode] #userCertificate:
0\202\005~0\202\004f\240\003\002\001\002\002\012\031\223\246\022
(host) [mynode] #userCertificate:
0\202\005\2240\202\004|\240\003\002\001\002\002\012\037\177\374\305
(host) [mynode] #givenName: JDE
(host) [mynode] #distinguishedName: CN=John Doe,CN=Users,DC=eng,DC=net
(host) [mynode] #instanceType: 4
(host) [mynode] #whenCreated: 20060516232817.0Z
(host) [mynode] #whenChanged: 20081216223053.0Z
(host) [mynode] #displayName: John Doe
(host) [mynode] #uSNCreated: 24599
(host) [mynode] #memberOf: CN=Cert_Admins,CN=Users,DC=eng,DC=net
```

```
(host) [mynode] #memberOf: CN=ATAC,CN=Users,DC=eng,DC=net
(host) [mynode] #uSNChanged: 377560
(host) [mynode] #department: eng
(host) [mynode] #name: John Doe
...
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa radius-attributes

```
aaa radius-attributes add <attribute> <attribute-id> {date|integer|ipaddr|string} [vendor
<name> <vendor-id>]
```

Description

This command configures RADIUS attributes to statically configure values to be included in RADIUS Access-Requests and Accounting-Requests.

Syntax

Parameter	Description
`add <attribute> <attribute-id>`	Adds the specified attribute name (alphanumeric string), associated attribute ID (integer), and type (date, integer, IP address, or string).
`date`	Adds a date attribute.
`integer`	Adds an `integer` attribute.
`ipaddr`	Adds an IP address attribute.
`string`	Adds a string attribute.
`vendor`	(Optional) Display attributes for a specific vendor name and vendor ID.

Usage Guidelines

Add RADIUS attributes for use in SDRs. Use the **show aaa radius-attributes** command to display a list of the current RADIUS attributes recognized by the Mobility Master. To add a RADIUS attribute to the list, use the **aaa radius-attributes** command.

Example

The following command adds the VSA Aruba-User-Role:

```
(host) ^[md] (config) aaa radius-attributes add Aruba-User-Role 1 string vendor Arubas 14823
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa radius modifier

```
aaa radius modifier <rad_modifier_name>
   clone <source>
   exclude <name>
   include <name> {[static <static_val>]|[dynamic <ap-group1>|<ap-macaddr1>|<ap-
   name1>|<essid1>|<user-vlan1>|<with>|<ap-group2>|<ap-macaddr2>|<ap-name2>|<essid2>|<user-
   vlan2>]<delimiter>}
   no..
```

Description

This command configures the RADIUS modifier profile to customize the attributes that are included, excluded and modified in the RADIUS request before it is sent to the authentication server.

Syntax

Parameter	Description
`<rad_modifier_name>`	The specified RADIUS modifier profile name
`clone <source>`	Copy data from another Radius Modifier Profile
`exclude <name>`	Attribute to be excluded in RADIUS request
`include <name>`	Attribute/Value to be included in RADIUS request
`static <static_val>`	Static data. (1-128 bytes string in length)
`dynamic`	First dynamic field. Use the following parameters: ■ **ap-group1**: Use AP group as the first dynamic field. ■ **ap-macaddr1**: Use AP mac address as the first dynamic field. ■ **ap-name1**: Use AP name as the first dynamic field. ■ **essid1**: Use essid as the first dynamic field. ■ **user-vlan1**: Use the current VLAN-ID of user as the first dynamic field.
`with`	(Optional) Connect to the second dynamic field. Use the following parameters: ■ **ap-group2**: Use AP group as the second dynamic field. ■ **ap-macaddr2**: Use AP mac address as the second dynamic field. ■ **ap-name2**: Use AP name as the second dynamic field. ■ **essid2**: Use essid as the second dynamic field. ■ **user-vlan2**: Use the current VLAN-ID of user as the second dynamic field.
`delimiter`	Delimiter (at, colon, dash, dollar, hash, none, percent, semicolon, slash, space) used in the string.
`no`	Delete Command.

Usage Guidelines

Use the **show aaa radius modifier** command to display a list of RADIUS modifier profiles . To create a RADIUS modifier profile with customized attributes, use the **aaa radius-attributes** command.

Example

Example for Included attribute

```
(host) [md](config) #aaa radius-attributes add BW-Area-Code 18 integer vendor Boingo 22472
   (host) [md](Radius Modifier Profile "radmodifier1") # include BW-Area-Code static "212"
   (host) [md](Radius Modifier Profile "radmodifier1") # no include BW-Area-Code
```

Example for excluded attribute

```
(host) [md](config) #aaa radius-attributes add BW-Area-Code 18 integer vendor Boingo 22472
   (host) [md](Radius Modifier Profile "radmodifier1") # exclude BW-Area-Code
   (host) [md](Radius Modifier Profile "radmodifier1") # no exclude BW-Area-Code
```

Example for modified attribute

Default attributes to carry to radius server can be modified with include option.

```
(host) [md](Radius Modifier Profile "radmodifier1") # include "Aruba-location-id" static
"Shim-office"
```

Command History

Version	Modification
ArubaOS 8.2.0.0	The **exclude** and **include** parameters were added.
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

aaa rfc-3576-server

```
aaa rfc-3576-server <ipaddr>
   clone <source>
   enable-radsec
   event-timestamp-requi..
   key <psk>
   no ...
   replay-protection
   window-duration
```

Description

This command configures a RADIUS server that can send user disconnect, session timeout, and CoA messages, as described in RFC 3576, Dynamic Authorization Extensions to RADIUS.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the server.
`clone <source>`	Name of an existing RFC 3576 server configuration from which parameter values are copied.
`enable-radsec`	Enable RADSEC for the server.
`event-timestamp-required`	To enable discard of DAC request, if Event-Timestamp is not present in DAC request. This option will only come into the effect, if replay-protection is enabled.
`key <psk>`	Shared secret to authenticate communication between the RADIUS client and server.
`no`	Negates any configured parameter.
`replay-protection`	Enable replay protection for DAC requests.
`window-duration`	Number in seconds. Default value is 300. This parameter is used: - To check stale DAC requests. - To specify the minimum time-span in seconds between two valid requests with same identifiers, to check replay protection and identify duplicates.

Usage Guidelines

The disconnect, session timeout and change-of-authorization messages sent from the server to managed device contains information to identify the user for which the message is sent. Managed Device supports the following attributes for identifying the users who authenticate with an RFC 3576 server:

- user-name: Name of the user to be authenticated.
- framed-ip-address: IP address of the User.
- calling-station-id: Phone number of a station that originated a call.
- accounting-session-id: Unique accounting ID for the user session.

If the authentication server sends both supported and unsupported attributes to managed device, the unknown or unsupported attributes will be ignored. If no matching user is found managed device will send a 503: Session Not Found error message back to the RFC 3576 server.

Example

The following command configures an RFC 3576 server:

```
(host) ^[md] (config) aaa rfc-3576-server 10.1.1.245
   clone default
   key P@$$w0rD;
```

Related Commands

Command	Description
show aaa state user	View information for a user whose session timeout is altered by a RFC 3576 server.

Command History

Release	Modification
ArubaOS 8.2.0.0	**Event-timestamp-required**, **replay-protection**, and **window-duration** parameters are introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa server-group

```
aaa server-group <group>
   allow-fail-through
   auth-server <name> [match-authstring contains|equals|starts-with <string>] [match-fqdn
   <string>] [position <number>] [trim-fqdn]
   clone <source>
   load-balance
   no ...
   set role|vlan condition <attribute> contains|ends-with|equals|not-equals|starts-with
   <string> set-value <set-value-str> [position <number>]
```

Description

This command allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication.

Syntax

Parameter	Description	Default
`<group>`	Name that identifies the server group. The name must be 32 characters or less.	—
`allow-fail-through`	When this option is configured, an authentication failure with the first server in the group causes the Mobility Master to attempt authentication with the next server in the list. The Mobility Master attempts authentication with each server in the ordered list until either there is a successful authentication or the list of servers in the group is exhausted.	disabled
`auth-server <name>`	Name of a configured authentication server.	—
`match-authstring`	This option associates the authentication server with a match rule that the Mobility Master can compare with the user or client information in the authentication request. With this option, the user or client information in the authentication request can be in any of the following formats: <domain>\<user> <user>@<domain> host/<pc-name>.<domain> An authentication request is sent to the server only if there is a match between the specified match rule and the user or client information. You can configure multiple match rules for an authentication server.	—
`contains`	The rule matches if the user or client information contains the specified string.	—
`equals`	The rule matches if the user or client information exactly matches the specified string.	—
`starts-with`	The rule matches if the user or client information starts with the specified string.	—

Parameter	Description	Default
match-fqdn <string>	This option associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request. With this option, the user information must be in one of the following formats: <domain>\<user> <user>@<domain>	—
position <number>	Position of the server in the server list. 1 is the top.	(last)
trim-fqdn	This option causes the user information in an authentication request to be edited before the request is sent to the server. Specifically, this option: removes the <domain>\ portion for user information in the <domain>\<user> format removes the @<domain> portion for user information in the <user>@<domain> format.	—
clone <source>	Name of an existing server group from which parameter values are copied.	—
load-balance	Enables load-balancing of authentication requests among different servers in a server group.	—
no	Negates any configured parameter.	—
set role|vlan	Assigns the client a user role, VLAN ID or VLAN name based on attributes returned for the client by the authentication server. Rules are ordered: the first rule that matches the configured condition is applied. VLAN IDs and VLAN names cannot be listed together.	—
condition	Attribute returned by the authentication server.	—
contains	The rule is applied if and only if the attribute value contains the specified string.	—
ends-with	The rule is applied if and only if the attribute value ends with the specified string.	—
equals	The rule is applied if and only if the attribute value equals the specified string.	—
not-equals	The rule is applied if and only if the attribute value is not equal to the specified string.	—
starts-with	The rule is applied if and only if the attribute value begins with the specified string.	—
set-value	User role or VLAN applied to the client when the rule is matched.	—
value-of	Sets the user role or VLAN to the value of the attribute returned. The user role or VLAN ID returned as the value of the attribute must already be configured on the Mobility Master when the rule is applied.	—

Usage Guidelines

You create a server group for a specific type of authentication or for accounting. The list of servers in a server group is an ordered list, which means that the first server in the group is always used unless it is unavailable (in which case, the next server in the list is used). You can configure servers of different types in a server group, for example, you can include the internal database as a backup to a RADIUS server. You can add the same server to multiple server groups. There is a predefined server group internal that contains the internal database.

Example

The following command configures a server group corp-servers with a RADIUS server as the main authentication server and the internal database as the backup. The command also sets the client's user role to the value of the returned Class attribute.

```
(host) ^[md] (config) aaa server-group corp-servers
   auth-server radius1 position 1
   auth-server internal position 2
   set role condition Class value-of
   load-balance
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa tacacs-accounting

```
aaa tacacs-accounting
   command {action|all|configuration|show}
   no
   server-group <sg>
```

Description

This command configures reporting of commands issued from a managed device to a TACACS+ server group.

Syntax

Parameter	Description	Range	Default
`command`	The types of commands that are reported to the TACACS server group.	—	—
`action`	Reports action commands only.	—	—
`all`	Reports all commands.	—	—
`configuration`	Reports configuration commands only.	—	—
`show`	Reports show commands only.	—	—
`no`	Delete command.	—	disabled
`server-group <sg>`	The TACACS server group to which the reporting is sent.	—	—

Usage Guidelines

You must have previously configured the TACACS+ server and server group (see aaa authentication-server tacacs on page 45 and aaa server-group on page 103).

Example

The following command enables accounting and reporting of configuration commands to the server-group “tacacs1”:

```
(host) [mm] (config) #aaa tacacs-accounting
(host) ^[mm] (config-submode) #server-group tacacs1
(host) ^[mm] (config-submode) #command configuration
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa test-server

```
aaa test-server {mschapv2|pap} <server-name> <username> <passwd> {<STRING>} {<verbose>}
```

Description

This command tests a configured authentication server.

Syntax

Parameter	Description
`mschapv2`	Use MSCHAPv2 authentication protocol.
`pap`	Use PAP authentication protocol.
`<server-name>`	Name of the configured authentication server.
`<username>`	Username to use to test the authentication server.
`<passwd>`	Password to use to test the authentication server.
`<STRING>`	MAC address of the user.
`<verbose>`	RADIUS server response for a successful or failed authentication.

Usage Guidelines

This command allows you to check a configured RADIUS authentication server or the internal database. You can use this command to check for an "out of service" RADIUS server.

Example

The following commands add a user in the internal database and verify the configuration:

```
(host) [mynode] #local-userdb add username raduser1 password raduser
(host) [mynode] #aaa test-server mschapv2 internal raduser1 raduser verbose
```

Starting from ArubaOS 8.1.0, the **aaa test-server** command has a new **verbose** option that displays the RADIUS server's response on a successful or failed authentication.

The following command displays the RADIUS server attributes as returned by the server.

```
(host) [mynode] #aaa test-server mschapv2 internal raduser1 raduser verbose
Authentication Successful
Processing time (ms) : 1.397
Attribute value pairs in response
---------------------------------
Vendor  Attribute  Value
------  ---------  -----
        MS-CHAPv2
        Role       guest
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **verbose** option is introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

aaa timers

```
aaa timers
   dead-time <minutes>
   idle-timeout <time> [seconds]
   logon-lifetime <0-255>
   stats-timeout <time> [seconds]
```

Description

This command configures the timers that you can apply to clients and servers.

Syntax

Parameter	Description	Range	Default
`dead-time <minutes>`	Maximum period, in minutes, that the Mobility Master considers an unresponsive authentication server to be out of service. This timer is only applicable if there are two or more authentication servers configured on the Mobility Master. If there is only one authentication server configured, the server is never considered out of service and all requests are sent to the server. If one or more backup servers are configured and a server is unresponsive, it is marked as out of service for the dead time; subsequent requests are sent to the next server on the priority list for the duration of the dead time. If the server is responsive after the dead time has elapsed, it can take over servicing requests from a lower-priority server; if the server continues to be unresponsive, it is marked as down for the dead time.	0-60	10 minutes
`idle-timeout <1-15300>`	Maximum number of minutes after which a client is considered idle if there is no user traffic from the client. The timeout period is reset if there is a user traffic. If there is no IP traffic in the timeout period or there is no 802.11 traffic as indicated in the station ageout time that is set in the wlan ssid profile, the client is aged out. Once the timeout period has expired, the user is removed immediately and no ping request is sent. If the **seconds** parameter is not specified, the value defaults to minutes.	1 to 255 minutes (30 to 15300 seconds)	5 minutes (300 seconds)
`logon-lifetime`	Maximum time, in minutes, that unauthenticated clients are allowed to remain logged on.	0-255	5 minutes
`stats-timeout`	User Interim stats timeout value. If the **seconds** parameter is not specified, the value defaults to minutes.	5-60 minutes(300 to 3600 seconds)	10 minutes (600 seconds)

Usage Guidelines

These parameters can be left at their default values for most implementations.

Example

The following command changes the idle time to 10 minutes:

```
(host) ^[md] (config) aaa timers idle-timeout 10
```

Related Commands

```
(host) ^[md] #show aaa timers
(host) ^[md] #show datapath user table
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	Updated the range of **stats-timeout** parameter.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa trusted-ap

```
aaa trusted-ap <macaddr>
```

Description

This command configures a trusted non-Aruba AP.

Syntax

Parameter	Description
`<macaddr>`	MAC address of the AP

Usage Guidelines

This command configures a non-Aruba AP as a trusted AP.

Example

The following command configures a trusted non-Aruba AP:

```
aaa trusted-ap 00:40:96:4d:07:6e
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

aaa user add

```
aaa user add <ipaddr> [<nusers>] [authentication-method {dot1x|mac|stateful-dot1x|vpn|
 web}] [mac-addr <macaddr>] [name <username>] [profile <aaa_profile>] [role <role>]
```

Description

This command manually assigns a user role or other values to a specified client or device.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the user to be added.
`<nusers>`	Number of users to create starting with <ipaddr>.
`authentication-method`	Authentication method for the user.
`dot1x`	802.1X authentication.
`mac-addr`	MAC authentication.
`stateful-dot1x`	Stateful 802.1X authentication.
`vpn`	VPN authentication.
`web`	Captive portal authentication.
`mac <macaddr>`	MAC address of the user.
`name <username>`	Name for the user.
`profile <aaa_profile>`	AAA profile for the user.
`role <role>`	Role for the user.

Usage Guidelines

This command should only be used for troubleshooting issues with a specific client or device. This command allows you to manually assign a client or device to a role. For example, you can create a role debugging that includes a policy to mirror session packets to a specified destination for further examination, then use this command to assign the debugging role to a specific client. Use the **aaa user delete** command to remove the client or device from the role.

Note that issuing this command does not affect ongoing sessions that the client may already have. For example, if a client is in the employee role when you assign them to the debugging role, the client continues any sessions allowed with the employee role. Use the **aaa user clear-sessions** command to clear ongoing sessions.

Example

The following commands create a role that logs HTTPS traffic, then assign the role to a specific client:

```
(host) [mynode] (config) #ip access-list session log-https
(host) [mynode] (config-submode) #any any svc-https permit log
(host) [mynode] (config-submode) #user-role web-debug
(host) [mynode] (config-submode) #session-acl log-https
```

In enable mode:

```
(host) [mynode] (config) #aaa user add 10.1.1.236 role web-debug
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa user clear-sessions

```
aaa user clear-sessions <ipaddr>
```

Description

This command clears ongoing sessions for the specified client.

Syntax

Parameter	Description
`<ip-addr>`	IP address of the user.

Usage Guidelines

This command clears any ongoing sessions that the client already had before being assigned a role with the **aaa user add** command.

Example

The following command clears ongoing sessions for a client:

```
(host) [mynode] (config) #aaa user clear-sessions 10.1.1.236
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa user delete

```
aaa user delete {|all|<ip-addr>|<ap-ip-addr>|ap-name|mac <macaddr>|name <username>|role
<role>}
```

Description

This command deletes clients, users, or roles.

Syntax

Parameter	Description
`all`	Deletes all connected clients.
`<ip-addr>`	IP address of the client to be deleted.
`<ap-ip-addr>`	IP address of the AP to be deleted.
`ap-name`	Name of the AP to be deleted.
`mac`	MAC address of the client to be deleted.
`name`	Name of the client to be deleted.
`role`	Role of the client to be deleted.

Usage Guidelines

This command allows you to manually delete clients, users, or roles. For example, if you used the **aaa user add** command to assign a user role to a client, you can use this command to remove the role assignment. Note that you must provide either AP name or AP IP address if you want to delete bridge-mode clients.

Example

To delete a user role:

```
(host) [mynode] (config) aaa user delete role web-debug
```

To delete a bridge-mode client:

```
(host) [mynode] (config) aaa user delete ap-name ap303 mac 58:94:6b:31:d0:f0
```

OR

```
(host) [mynode] (config) aaa user delete ap-ip-addr 1.2.3.4 mac 58:94:6b:31:d0:f0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Managed Device.

aaa user fast-age

```
aaa user fast-age
```

Description

This command enables fast aging of user table entries.

Syntax

No parameters.

Usage Guidelines

When this feature is enabled, if a device comes up on the network with a different IP address, the old IP address of the device is immediately deleted. If the user fast-age feature is not configured, the Mobility Master retains up to two IPv4 and two IPv6 addresses per device , and these IPs are aged out only when the device becomes inactive.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master executed on the managed device node.

aaa user logout

```
aaa user logout <ipaddr>
```

Description

This command logs out an authenticated client.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the authenticated client to be logged out.

Usage Guidelines

This command logs out an authenticated client. The client must reauthenticate.

Example

The following command logs out a client:

```
(host) [mynode] #aaa user logout 10.1.1.236
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

aaa user monitor

```
aaa user monitor <ipaddr>|off
```

Description

This command checks to see whether the attributes of an authenticated user differs from those in the SOS.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the user whose attributes are being checked.
`off`	Disable aaa user monitoring.

Usage Guidelines

This command installs a timer that polls the SOS every 60 seconds and checks the following:

- L3 ACLs
- Upstream bandwidth contract
- Downstream bandwidth contract

Example

The following command checks user SOS attributes:

```
(host) [mynode] (config) #aaa user monitor 10.1.1.236
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa user purge-log

```
aaa user purge-log
```

Description

This clear aaa user log files

Syntax

No parameters

Usage Guidelines

Per-user log files for AAA events can be used for troubleshooting issues with a specific client or device. This command clears log information for deleted users.

Example

```
(host) [mynode] (config) #aaa user purge log
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

aaa user stats-poll

```
aaa user stats-poll <secs>
```

Description

This command enables user statistics polling. If enabled, ArubaOS will poll user data verify that user information in the datapath of the Mobility Master is in synchronization with the data in the authentication module of the Mobility Master.

Syntax

Parameter	Description
`<secs>`	This command enables user statistics polling, and defines the time interval between polls. The supported range is 60-600 seconds.

Example

The following command enables user statistics polling with an interval of 10 minutes:

```
(host) ^[md] (config) aaa user stats-poll 600
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

aaa xml-api

```
aaa xml-api server <ipaddr>
   clone <server>
   default-authentication-role <role>
   key <key>
   no ...
```

Description

This command configures an external XML API server.

Syntax

Parameter	Description
`server`	IP address of the external XML API server.
`clone`	Name of an existing XML API server configuration from which parameter values are copied.
`key`	Preshared key to authenticate communication between the Mobility Master and the XML API server.
`default-authentication-role <role>`	Name of the role to be assigned to users after completing XML server authorization.
`no`	Negates any configured parameter.

Usage Guidelines

XML API is used for authentication and subscriber management from external agents. This command configures an external XML API server. For example, an XML API server can send a blacklist request for a client to the managed device. The server configured with this command is referenced in the AAA profile for the WLAN (see aaa profile on page 91).

Example

The following configures an XML API server:

```
(host) ^[md] (config) aaa xml-api server 10.210.1.245
   key qwerTYuiOP
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Config mode on Mobility Master.

activate

```
activate sync
   add-only
   ca-cert <cacert>
   interval <days>
   no ...
   password <password
   provisionurl <provisionurlname>
   sync
   username <username>
   whitelist download
   whitelist-enable
```

Description

This command synchronizes a managed device whitelist or remote AP whitelist on Mobility Master with the Activate whitelist database.

Syntax

Parameter	Description
`add-only`	Allow only addition or modification of entries to the Activate remote AP whitelist database. This parameter is enabled by default. If this setting is disabled, the activate-whitelist-download command can both add and remove entries from the Activate database.
`ca-cert <cacert>`	Use this command to manually upload self signed certificate and establish a trust relationship for a successful IPsec connection between the managed device and Activate server.
`interval <days>`	Number of days between the automatic synchronization of the controller remote AP whitelist entries with the Activate whitelist. The supported range is 1-7 days, and the default value is 1 day.
`no`	Removes or disables an existing parameter.
`password <password>`	Activate user password.
`provisionurl <pro-visionurlname>`	Use this command to provision the controller with the URL of the Activate server **NOTE:** Include the HTTP or HTTPS in the URL.
`sync`	Execute the activate sync command to immediately synchronize the list of managed devices on the Activate server with the managed device whitelist on Mobility Master. By default, this list is synchronized every hour.
`username <username>`	Activate username
`sync`	Issue this command to enable the synchronization the list of managed devices on the Activate server with the switch whitelist on Mobility Master.
`whitelist download`	Issue this command to download and synchronize Mobility Master's remote AP and managed device whitelists from the Activate server.
`whitelist-enable`	Issue this command to enable secure remote AP and managed device whitelist synchronization with the Activate service. This feature is disabled by default.

Parameter	Description
`sync`	Execute the activate sync command to immediately synchronize the list of managed devices on the Activate server with the managed device whitelist on Mobility Master. By default, this list is synchronized every hour.
`whitelist download`	Issue this command to enable the synchronization the list of managed devices on the Activate server with the switch whitelist on Mobility Master.

Usage Guidelines

Use this command to synchronize Mobility Master's remote AP whitelist or managed device whitelist with the cloud-based Activate service. Mobility Master and the Activate server must have layer-3 connectivity to communicate.

Example

The following example synchronizes the Activate whitelist with the remote AP whitelist on the controller:

```
(host)[mynode](config)# activate whitelist download
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master , except for the **whitelist download** and **sync** parameters, which are available in enable mode only.

add ap arm client-match unsupported

```
add ap arm client-match unsupported <mac-addr>
```

Description

This command marks a station as unsupported by ClientMatch .

Syntax

Parameter	Description
`<mac-addr>`	MAC address of the station to be ignored by ClientMatch.

Usage Guidelines

This is an internal command used to diagnose and debug ClientMatch issues, and should be used only under the supervision of customer support.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

adp

```
adp
   discovery
   igmp-join
   igmp-vlan <igmp-vlan-id>
```

Description

This command configures the ADP.

Syntax

Parameter	Description	Range	Default
`discovery`	Enables or disables ADP on the managed device.	—	enabled
`igmp-join`	Enables or disables sending of Internet Group Management Protocol (IGMP) join requests from a managed device.	—	enabled
`igmp-vlan`	VLAN to which IGMP reports are sent.	—	0 (default route VLAN used)

Usage Guidelines

Aruba APs send out periodic multicast and broadcast queries to locate Mobility Master. If the APs are in the same broadcast domain as Mobility Master and ADP is enabled on the managed device, the managed device automatically responds to the queries of APs with its IP address. If the APs are not in the same broadcast domain as Mobility Master, you need to enable multicast on the network. You also need to make sure that all routers are configured to listen for IGMP join requests from the managed device and can route the multicast packets. Use the **show adp config** command to verify that ADP and IGMP join options are enabled on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

airgroup

```
airgroup
   active-domain
   cppm-server
   disallow-vlan
   dlna
   domain
   exclude-switch
   ipv6
   mdns
   policy
   server
   server-refresh
   test-server
```

Description

This command configures AirGroup settings.

Syntax

Parameter	Description
`active-domain <string>`	Configures active domain for AirGroup cluster. **NOTE:** This parameter is available only in Config mode.

`cppm-server`
`aaa`
`rfc-3576-server <rfc3576_server>`
`rfc3576_udp_port <rfc3576_udp_port>`
`server-dead-time <server-dead-time>`
`server-group <server-group>`
`query-interval <1..24>`
	Configures the following in AirGroup AAA profile:
	rfc-3576-server <rfc3576_ server>: Configures RFC 3576 server IP address.
	rfc3576_udp_port <rfc3576_udp_ port>: Configures UDP port number.
	server-dead-time <server-deadtime>: Server dead time in minutes. To disable the server dead time, set the value to 0.
	server-group<server-group>: Name of the server group.
	NOTE: This parameter is available only in Config mode.

`disallow-vlan`
`<1..4094> servers|users`
`string servers|users`
	Configures the following disallowed VLAN.
	<1..4094> {servers|users}: Blocks all AirGroup servers/users on this VLAN ID.
	string {servers|users}: Blocks all AirGroup servers/users on this VLAN name.
	NOTE: This parameter is available only in Config mode.

Parameter	Description
`dlna`	Configures AirGroup DLNA support. **NOTE:** This parameter is available only in Config mode.

`domain <string>`
`description <description>`
`ip-address <ipaddr>`
`no`
	Configures AirGroup domain.
	NOTE: This parameter is only available in Config mode.

`exclude-switch <mac>`	Excludes management of AirGroup on this managed device where: **<mac>**: MAC address of managed device. **NOTE:** This parameter is only available in Config mode.
`ipv6`	Configures IPv6 support for AirGroup. **NOTE:** This parameter is only available in Config mode.
`mdns`	Configure AirGroup mdns support. **NOTE:** This parameter is only available in Config mode.
`policy ap-fqln device-mac <mac>` `{add <string>}|{remove <string>}|{string}`	Configures shared AP-FQLN for this server
`policy ap-group device-mac <mac>` `{add <string>}|{remove <string>}|{<string>}`	Configure shared AP-group for this server
`policy ap-name device-mac <mac>` `{add <string>}|{remove <string>}|{<string>}`	Configure shared AP-name for this server
`policy ap-neighborhood device-mac <mac> number`	Consider neighborhood of configured AP names
`policy autoassociate device-mac <mac>` `{ap-fqln}|{ap-group}|{ap-name}`	Auto associate this wireless server with its AP-name/AP-FQLN/AP-group.
`policy shared-group device-mac <mac>` `{add <string>}|{remove <string>}|{<string>}`	Configure groups shared with this server
`policy shared-role device-mac <mac>` `{add <string>}|{remove <string>}|{<string>}`	Configure shared role-name for this server
`policy shared-user device-mac <mac>` `{add <string>}|{remove <string>}|{<string>}`	Configure users shared with this server
`policy XX:XX:XX:XX:XX:XX`	Server MAC address in XX:XX:XX:XX:XX:XX format.

Parameter	Description
`server enforce-registration`	Configures mDNS devices to be visible only if allowed through ClearPass Policy Manager. **NOTE:** This parameter is only available in Config mode.

`server-refresh`
`service <string> vlan <1..4094>`
 	
`<mac>`
	Sends refresh packet to refresh the cache of AirGroup server.
	<service <string> vlan <1..4094>: AirGroup service.
	<mac>: MAC address of AirGroup server.

`test-server <name> <macaddr>`	Tests AirGroup RADIUS server. **<name>**: Name of RADIUS server. **<macaddr>**: MAC address of RADIUS server.

Usage Guidelines

Starting with ArubaOS 8.0.0.0, AirGroup is disabled by default. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to configure AirGroup command:

```
(host) [mynode] #airgroup policy shared-group device-mac 00:1a:1e:aa:bb:cc add test

(host) [mynode] (config) #airgroup exclude-switch 00:1a:1e:aa:bb:cc
```

Related Commands

Command	Description
show airgroup	This command displays AirGroup settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	Parameter **static** removed.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

airgroupprofile

```
airgroupprofile
   activate {airgroupprofile <airgroup_profile> [<mode> {<centralised>| <distributed>}]}
   cppm <name>
     clone <source>
     query-interval-time <query-interval-time>
     rfc-3576-server <rfc-3576-server>
     rfc3576_udp_port <rfc3576_udp_port>
     server-dead-time <server-dead-time>
     server-group <server-group>
     no
   domain <name>
      clone <source>
      description <description>
      ip-addr <ip-addr>
      no
   ipv6 <name>
     clone <source>
   service <service-name>
      clone <source>
      description
      id <string>
      no
   <profile-name>
      active-domain-profile <airgroup-domain-name>
      autoassociate [apfqln|apgroup|apname]
      clone <source>
      cppm-profile <airgroup-cppm-name>
      disallow-role <role>[type{servers|users}[service]]
      disallow-vlan <vlan>[type{servers|users}[service]]
      enforce-registration
      ipv6-profile <ipv6-profile-name>
      no
```

Description

This command configures an AirGroup profile.

Syntax

Parameter	Description

`activate`
`  airgroupprofile <airgroup_profile>`
`  mode {centralised|distributed}`
	Configures the active AirGroup profile.
	NOTE: This parameter is supported only on the managed devices.
	■ **airgroupprofile**: Configure the AirGroup profile.
	■ **mode**: Configure AirGroup profile in centralised or distributed mode.

Parameter	Description

`cppm <name>`
`clone <source>`
`no`
`query-interval-time <query-interval-time>`
`rfc-3576-server <rfc-3576-server>`
`rfc3576_udp_port <rfc3576_udp_port>`
`server-dead-time <server-dead-time>`
`server-group <server-group>`
	Configures an AirGroup ClearPass Policy Manager profile.
	■ **clone**: Copy profile data from another AirGroup profile.
	■ **no**: Delete the command.
	■ **query-interval-time**: Specify the time interval, in seconds. between general queries.
	■ **rfc-3576-server**: Configure RFC 3576 server IP address.
	■ **rfc3576_udp_port**: Configure UDP port number.
	■ **server-dead-time**: Configure the server dead time, in minutes. To disable the server dead time, set the value to 0. The default value is 10 minutes.
	■ **server-group**: Configure the name of the server group.
	NOTE: This parameter is supported only on the managed devices.

`domain <name>`
`clone <source>`
`description <description>`
`ip-addr <ip-addr>`
`no`
	Configures an AirGroup domain profile.
	■ **clone**: Copy domain profile data from another AirGroup profile.
	■ **description**: Configure the domain name description.
	■ **ip-addr**: Configure the IP address of the controller.
	■ **no**: Delete the command.
	NOTE: This parameter is supported only on the managed devices.

`ipv6 <name>` `clone <source>`	Configures an AirGroup IPv6 profile. **clone**: Copy IPv6 profile data from another AirGroup profile. **NOTE:** This parameter is supported only on the managed devices.

Parameter	Description

`service <service-name>`
`clone <source>`
`description <service_desc>`
`id <service_id>`
`no`
	Configures an AirGroup service profile. By default, the following services are available:
	■ custom
	■ default-airplay
	■ default-airprint
	■ default-allowall
	■ default-amazontv
	■ default-dial
	■ default-dlna-media
	■ default-dlna-print
	■ default-googlecast
	■ default-itunes
	■ default-remotemgmt
	■ default-sharing
	■ DIAL
	Clone: Copy service profile data from another AirGroup service profile.
	Description: Description of AirGroup service profile.
	ID: Identity of AirGroup service profile.
	No: Disable AirGroup service profile.
	NOTE: This parameter is supported only on the managed devices.

Parameter	Description
<profile-name> active-domain-profile <airgroup-domain-name> autoassociate {apfqln | apgroup | apname} clone <source> cppm-profile <airgroup-cppm-name> disallow-role <role>[type{servers|users}[service]] disallow-vlan <vlan>[type{servers|users}[service]] enforce-registration ipv6-profile <ipv6-profile-name> no active-domain-profile autoassociate cppm-profile disallow-role disallow-vlan enforce-registration ipv6-profile <ipv6-profile-name> service <airgroup-service-name>	Configures an AirGroup profile. ■ **active-domain-profile**: Configure an AirGroup domain profile. ■ **autoassociate**: Auto associate servers with the AirGroup profile. Use the following sub-parameters: • **apfqln**: Auto associate with AP FQLN. • **apgroup**: Auto associate with AP Group. • **apname**: Auto associate with AP Name. ■ **clone**: Copy profile data from another AirGroup profile. ■ **cppm-profile**: Configure CPPM profile for the AirGroup profile. ■ **disallow-role**: Configure disallowed roles with AirGroup profile. ■ **disallow-vlan**: Configure disallowed vlans with AirGroup profile. ■ **enforce-registration**: Enforce server registration with AirGroup profile. ■ **ipv6-profile**: Configure an IPv6 profile with AirGroup profile. ■ **service**: Configure AirGroup service profile name. **NOTE:** This parameter is supported only on the managed devices.

Usage Guidelines

Starting with ArubaOS 8.2.0.0, the airgroupprofile command is introduced. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to configure an AirGroup profile for the DIAL service:

```
(host) [md] (config) #airgroupprofile service DIAL
(host) [md] (Airgroup Service Profile "DIAL") #description This is the DIAL service
(host) [md] (Airgroup Service Profile "DIAL") #
```

Related Commands

Command	Description
show airgroupprofile	This command displays AirGroup settings.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

airmatch ap

```
airmatch ap freeze all-aps|[ap-group <ap-group>]|[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-
addr <i6p-addr>] [band <band>] | [channel <channel>]| [eirp <dBm>]| [lms lms-ip <lms-ip>] |
[lms-ipv6 <lms-ipv6>]

airmatch ap unfreeze all-aps|[ap-group <ap-group>]|[ap-name <ap-name>]|[ip-addr <ip-addr>]|
[ip6-addr <i6p-addr>] band <band> | [channel <channel>]| [eirp <dBm>]| [lms lms-ip <lms-ip>] |
[lms-ipv6 <lms-ipv6>]
```

Description

A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Syntax

Parameter	Description
`freeze`	Apply the specified AirMatch settings on the radio, then freeze those settings until they are manually removed. **NOTE:** This parameter supports both single radio and dual-radio APs.
`unfreeze`	Remove AirMatch settings manually applied using the Freeze command. **NOTE:** This parameter supports both single radio and dual-radio APs.
`all-aps`	Freeze or unfreeze AirMatch settings on all APs.
`ap-group <ap-group>`	Freeze or unfreeze AirMatch settings on the specified AP group
`ap-name <ap-name>`	Freeze or unfreeze AirMatch settings on the specified AP
`ip-addr <ip-addr>`	Freeze or unfreeze AirMatch settings on the AP with the specified IPv4 IP address.
`ip6-addr <i6p-addr>`	Freeze or unfreeze AirMatch settings on the AP with the specified IPv6 IP address.
`band <band>`	Set AirMatch settings for the specified radio band. Supported values are **2.4GHz** and **5GHz**. The radio band *must* be specified if you use the **unfreeze** parameter to unfreeze an AP radio. The values, **5GHzu** for upper-band radios and **5GHzl** for lower-band radios are supported by the following APs. ■ AP-344 ■ AP-345
`channel <channel>`	Channel number for the AP 802.11a/b/g, 802.11nor 802.11ac physical layer, (e.g. 36, 36+, 36E). The available channels depend on the regulatory domain (country).

Parameter	Description
`eirp <dBm>`	The transmission power level (in dBm) to be assigned to the AP radio(s). Starting with ArubaOS 8.2, you can specify EIRP values in increments of .1 dBm. 270 Series access points support both positive and negative EIRP values. All other APs support positive EIRP values only. **NOTE:** The following legacy APs do *not* support advanced power controls, and can only be configured in positive EIRP values in increments of .5 dBm. ■ 90 Series ■ 100 Series ■ 110 Series ■ 170 Series ■ RAP-155

`lms`
`lms-ip <lms-ip>`
`lms-ipv6 <lms-ipv6>`
	Include this parameter to freeze or unfreeze AP channels on a local controller. This parameter is only valid if you freeze or unfreeze channels using the **ap-group** or **all-aps** options.

Usage Guidelines

The **airmatch ap freeze** command deploys the specified channel and EIRP values to a radio immediately, then freezes those values, regardless of whether the AirMatch RF planning schedule is enabled or disabled. A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command. This command can be used to freeze either the channel or the EIRP value, or both values. For example, you can freeze the channel on an AP radio, while allowing the EIRP values to be updated by AirMatch.

Example

```
(host)[mynode](config)# airmatch ap freeze {ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{ap-name
<ap-name>}|{ap-group <ap-group>}|{all-aps} {band <band>}|{channel <channel>}|{eirp <eirp>}{lms
{lms-ip <lms-ip>}|{{lms-ipv6 <lms-ipv6>}}
```

Unfreezing a radio configuration with the **airmatch ap unfreeze** command does not mean that there will automatically be an immediate change in the channel and EIRP values for that radio. It does, however, mean that the AirMatch algorithm can assign a new set of values at the next update.

```
(host)[mynode](config)# airmatch ap unfreeze {ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{ap-
name <ap-name>}|{ap-group <ap-group>}|{all-aps} band <band> {channel <channel>}|{eirp <eirp>}
{lms {lms-ip <lms-ip>}|{{lms-ipv6 <lms-ipv6>}}
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.3.0.0	The **freeze** and **unfreeze** parameters support dual 5 GHz radio APs.
ArubaOS 8.2.0.0	The **eirp** parameter supports the configuration of EIRP values in .1 dBm increments. EIRP values for 270 Series access points can be configured as a negative value.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Master	Base operating system	Config mode on Mobility Master.

airmatch db-dump

```
airmatch db-dump
all
collection
```

Description

This command creates a dump of the database used by AirMatch. The dump file can be exported using the **copy** command.

Syntax

Parameter	Description
`all`	Create a dump file of the entire AirMatch database
`collection`	Create a dump file of a specific collection of AirMatch files by specifying the name of a collection type.

Example

The following command creates a dump file of the collection of AirMatch AMON statistics.

```
(host)[mynode]# airmatch db-dump all
```

Related Commands

Command	Description
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.
airmatch profile	This command configures the AirMatch profile.
airmatch runnow	Manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Mobility Master	Base operating system	Enable mode on Mobility Master.

airmatch profile

```
airmatch profile
   deploy-hour <0-23>
   no ...
   noise-event-period-2g <noise-event-period-2g>
   noise-event-period-5g <noise-event-period-5g>
   quality-threshold <quality-threshold>
   radar-event-period-5g <radar-event-period-5g>
   schedule enable|disable
   solver-feas-deploy-threshold <solver-feas-deploy-threshold>
```

Description

This command configures the AirMatch profile.

Syntax

Parameter	Description	Range	Default
`deploy-hour <0-23>`	Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Master, the AirMatch solution will be deployed according to the time zone of the managed device. **NOTE:** If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.	0-23	5
`no ...`	Negates any configured parameter	–	–
`noise-event-period-2g <noise-event-period-2g>`	Use this advanced configuration parameter under the supervision of Aruba support only.	–	–

Parameter	Description	Range	Default
`noise-event-period-5g <noise-event-period-5g>`	Use this advanced configuration parameter under the supervision of Aruba support only.	–	–

Parameter	Description	Range	Default
`quality-threshold <quality-threshold>`	Use the **quality-threshold** parameter to change the percentage of channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change. This setting only applies to scheduled updates. If you manually trigger an update using the **airmatch runnow** command, AirMatch will deploy the new solution regardless of the level of improvement. **NOTE:** If scheduled updates are enabled, the new channel plan is deployed on the specified deployment hour only if it is improved	0-100%	8%

Parameter	Description	Range	Default
	by greater than this threshold value. A new EIRP plan is deployed on the deployment hour every day.		
`radar-event-period-5g <radar-event-period-5g>`	Use this advanced configuration parameter under the supervision of Aruba support only.	–	–

Parameter	Description	Range	Default
`schedule enabled|disabled`	If the AirMatch schedule updates are changed from the default **enabled** setting to **disabled**, the Mobility Master continues to receive RF updates from the APs, but no channel and EIRP changes are executed by Mobility Master at the scheduled time. When AirMatch schedules are disabled, the centralized algorithm stops selecting a new channel, bandwidth, stops EIRP setting. A network operator still can override the previous settings assigned by AirMatch with static channel or EIRP values, and the AP radio can continue to voluntarily change channels to avoid radar interference or high noise levels.	enabled disabled	**enabled**

Parameter	Description	Range	Default
`solver-feas-deploy-threshold <solver-feas-deploy-threshold>`	Use this advanced configuration parameter under the supervision of Aruba support only.	–	–

Usage Guidelines

The AirMatch channel and EIRP optimization features deprecate the channel planning and EIRP optimization features in the legacy ARM feature. AirMatch is supported on Mobility Master only, while legacy ARM channel optimization and EIRP features continue to be supported by stand-alone controllers running ArubaOS 8.x.

AirMatch channel planning evens out channel distributions in any size of network, and in any subset of the contiguous network (as much as allowed by the network configuration, regulatory domain and AP hardware capability). AirMatch also minimizes channel coupling, where adjacent radios are assigned to the same channel. The computing power of Mobility Master impacts channel distribution calculations, so channel coupling may occasionally be allowed in complex networks to keep the computing time practical.

AirMatch EIRP planning automatically considers the local density of the network to manage the APs' coverage and modulation and coding scheme (MCS) operation, and optimizes EIRP changes across neighboring AP radios in order to offer users the best roaming experience.

The AirMatch **schedule disable** setting is different from the ARM setting of **disable** or **maintain**. The ARM **disable** setting changes the AP radio channel and EIRP values back to the default values specified in 802.11a and 802.11g radio profiles for that radio. The ARM **maintain** setting freezes current channel and EIRP settings for that radio. In contrast, the AirMatch **schedule disable** option simply means the centralized algorithm will stop selecting a new channel, bandwidth, or EIRP setting; the network operator still can override the previous settings assigned by AirMatch with static channel or EIRP values, and the AP radio can continue to voluntarily change channels to avoid radar interference or high noise levels.

AirMatch Channel Assignments

Each AP in a Mobility Master deployment measures its RF environment for a five minute period, every 30 minutes, by default. The AP then sends AMON messages about the radio feasibility to the managed device based on thehardware capability for the AP, radio and regulatory domain, and RF neighbors. The managed device forwards these messages to the Mobility Master. The Mobility Master adds this information to a database, computes an optimal solution, and deploys the latest RF plan by sending updated settings to the APs. By default, this configuration update is sent at 5 AM (as per the Mobility Master system clock), but time of this configuration update can be modified via the AirMatch profile.

An exception to this daily update is an automatic channel change due to a radar detection event or high noise interference. If an AP detects a radar event on its current operating channel, that AP automatically changes to another supported channel to avoid radar interference, and does not wait for the daily RF configuration update from the Mobility Master. An AP may also automatically change channels if a very high noise level is detected on the current channel, if at least one other channel is free of noise.

In ArubaOS 8.0, AirMatch moves a radio to a random channel when a radar event is detected, or if a high noise floor is detected on a non-static channel. Starting with ArubaOS 8.0.1, AirMatch uses the criteria described in Table 7 to assign a new channel.

Table 7: *Channel Assignment Logic*

Issue Prompting Channel Change	Channel Selection Criteria
Detected radar	AirMatch selects a channel with a minimum interference index from the channels without high noise or a radar condition.
High channel noise	The channel selection criteria varies between static and non-static channels. ■ If static channel is configured, the channel does not change due to a high noise condition. ■ For a non-static channel, AirMatch selects a channel with a minimum interference index from the channels without high noise or a radar condition.

Channel Quality Improvement Thresholds

ArubaOS 8.0.1 introduces the AirMatch channel quality improvement threshold, which allows you to select the minimum channel improvement that can trigger a new scheduled channel solution. The default threshold value is a 15% improvement. If a proposed channel change will not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.

EIRP settings are not impacted by the channel quality improvement threshold. A new EIRP plan is deployed at the scheduled deployment hour every day, regardless of channel quality improvement levels.

This channel quality setting only applies to scheduled updates. If you manually trigger an update using the **airmatch runnow** command, AirMatch will deploy the new solution regardless of the level of improvement.

Example

To hold the existing AirMatch RF configuration :

```
(host)[mynode](config)# airmatch profile schedule disabled
```

To change the time of the daily AirMatch RF updates from the default 5 AM to 2 AM:

```
(host)[mynode](config)# airmatch profile deploy-hour 2
```

Related Commands

Command	Description
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.
airmatch db-dump	This command creates a dump of the database used by AirMatch. The dump file can be exported using the **copy** command.
airmatch profile	This command configures the AirMatch profile.
airmatch runnow	Manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period.
show airmatch profile	This command displays the configuration settings in the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.2.1.0	The default value of the **quality-threshold** parameter was changed to 8%.
ArubaOS 8.1.0.0	The **eirp-offset** parameter was removed from this command, and was introduced into the rf dot11a-radio-profile and rf dot11g-radio-profile commands.
ArubaOS 8.0.1.0	The **quality-threshold** parameter was introduced.
ArubaOS 8.0.0.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

airmatch runnow

```
airmatch runnow
   eirp
   full
   incremental
   opmode
   quick
```

Description

Manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period.

Syntax

Parameter	Description
`eirp`	Initiates only the EIRP optimization.
`full`	Initiate the process to perform a full optimization of all APs.
`incremental`	Optimize only the new APs that have never been optimized by a previous AirMatch solution.
`opmode`	Generate an AirMatch solution with an opmode update.
`quick`	Quickly generate an AirMatch solution. This option may produce an AirMatch solution that is not as optimal as a full or regularly-scheduled optimization.

Usage Guidelines

Use the Mobility Master CLI to manually initiate AirMatch RF computations and solution deployment instead of waiting for the next scheduled update period. Issue this command to manually initiate AirMatch RF computations any time there is a significant update in the regulatory-domain profile or AirMatch related fields (such as max-channel-bandwidth, eirp-min, and eirp-max) in 802.11g radio profile or 802.11a radio profile.

Example

To initiate a full optimization of all APs, access the Mobility Master CLI in enable mode and issue the following command:

```
(host)[mynode] #airmatch runnow full
```

Related Commands

Command	Description
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.
airmatch profile	This command configures the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.3.0.0	The **eirp** and **opmode** parameters were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

ale-configuration

```
ale-configuration
   ale_sta_associated
   anonymize
   ip <ip-addr> username <uname> password <passwd>
   nbapi_publish
```

Description

This command configures the ALE on the Mobility Master.

Syntax

Parameter	Description	Default
`ale_sta_associated`	Publish ALE_STA channel for associated clients only	False
`anonymize`	Station Mac Anonymization	False
`ip`	VLAN to which IGMP reports are sent.	–
`nbapi_publish`	Enable publishing NB API (zmq and REST)	False

Usage Guidelines

Use this command to enable ALE configuration. After ALE is enabled, you can configure ALE anonymize, STA channel, IP address, and NB API.

Issue **no ale-configuration** to disable ALE on the Mobility Master.

The **nbapi_publish** command enables publishes data available via zmq, including station, virtual AP, AP, radio, RSSI, visability_rec, destination, application; and REST API including details about floor, campus, building, Virtual AP, AP, station, radio.

Example

To enable ALE configuration:

```
(host) [mynode] (config) #ale-configuration
```

To enable anonymize in ALE:

```
(host) [mynode] (config) #ale-configuration
(host) [mynode] (config-submode)#anonymize
```

Related Commands

Command	Description
show ale-configuration	This command displays ALE configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

allow-sso

```
allow-sso <username> <role>
```

Description

This command configures the AMP SSO for a user name.

Syntax

Parameter	Description
`username`	Enter the user name
`role`	Enter the role of the user

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

am

```
scan ip-addr <ipaddr> <channel> [bssid <bssid>]
test ip-addr <ip-addr>
   auto-device-creation
      start interval <interval> phy-type {80211a|80211g}
      stop
   create-device
      ap phy-type {80211a|80211g} [bssid <bssid>] [mac <mac_address>]
      client phy-type {80211a|80211g} [bssid <bssid>] [mac <mac_address>]
   ev-gen event_id <event_id> trap_id <trap_id> [ADDITIONAL_INFO <ADDITIONAL_INFO> |
   ADDRESS_TYPE <ADDRESS_TYPE> |
      AP_CHANNEL <AP_CHANNEL> | AP_LOCATION <AP_LOCATION> |
      AP_MAC_ADDRESS <AP_MAC_ADDRESS> | AP_RADIO_NUM <AP_RADIO_NUM> |
      ASSOCIATION_TYPE <ASSOCIATION_TYPE> | CONF_LEVEL <CONF_LEVEL> |
      FRAME_TYPE <FRAME_TYPE> | INTERFERING_AP_INFO_URL <INTERFERING_AP_INFO_URL> | MATCHED_
      IP <MATCHED_IP> | MATCHED_MAC <MATCHED_MAC> |
      NODE_MAC <NODE_MAC> | RECEIVER_MAC <RECEIVER_MAC> | ROGUE_INFO_URL <ROGUE_INFO_URL> |
      SIGNATURE_NAME <SIGNATURE_NAME> | SNR <SNR>
      SOURCE_MAC <SOURCE_MAC> | SPOOFED_FRAME_TYPE <SPOOFED_FRAME_TYPE> | TARGET_AP_BSSID
      <TARGET_AP_BSSID> | TARGET_AP_SSID <TARGET_AP_SSID> | TRANSMITTER_MAC <TRANSMITTER_
      MAC>]
   suspect-rap bssid <bssid> match-type <match-type> match-method <match-method>
   wired-mac
      add {bssid <bssid> mac <mac>|enet-mac <enet-mac> mac <mac>|prop-wm mac <mac-addr>|sys-
      tem-gw-wm mac <mac>|system-wm mac <mac>}
      remove {bssid <bssid> mac <mac>|enet-mac <enet-mac> mac <mac>|prop-wm mac <mac>|sys-
      tem-gw-wm mac <mac>|system-wm mac <mac>}
```

Description

The **scan** sub-command enables channel scanning for the specified air monitor. In addition, the **test** sub-command enables the client to test an air monitor.

Syntax

Parameter	Description	Range
`scan`	Enable or disable channel scan.	—
`ip-addr <ip-addr>`	IP address of the air monitor to be scanned.	
`<channel>`	Channel to which the scanning is tuned. Set to 0 to enable scanning of all channels.	—
`bssid <bssid>`	BSSID of the air monitor.	—
`test`	Enables the client to test an air monitor.	—
`ip-addr <ip-addr>`	IP address of the air monitor.	—

Parameter	Description	Range
auto-device-creation	Sets the AP mode to add a monitored device and client at every interval. ■ start ■ stop Intervals are written as time in seconds.	—
interval <interval>	Sets the interval in seconds at which the new AP and client devices are added.	
phy-type {80211a|80211g}	Sets the band of the device. ■ 80211a for *a* band ■ 80211g for *g* band	
create-device {ap | client}	Creates an AP or client device. ■ ap ■ client	—
phy-type {80211a | 80211g}	Specifies the band for the device. ■ 80211a ■ 80211g	
bssid <bssid>	Specifies the bssid of the new device	
mac <mac>	Specifies the wired-mac address of the new device	
ev-gen	Create an IDS event from the AP.	—
event_id <event-id>	Specifies the event id to generate for the event.	

Parameter	Description	Range
trap_id <trap_id>	Specifies the trap id to generate or use 65535 if there are no traps. The various trap IDs are explained here: ■ ADDITIONAL_INFO—Additional information for syslog ■ ADDRESS_TYPE—Address type (an integer because it is enum) ■ AP_CHANNEL—Detecting AP channel or target channel ■ AP_LOCATION—Detecting AP Name ■ AP_MAC_ADDRESS—Detecting AP MAC ■ AP_RADIO_NUM—Detecting AP Radio ■ ASSOCIATION_TYPE—Association Type ex. Association To Rogue ■ CONF_LEVEL—Confidence level of suspected rogue (5-100) ■ FRAME_TYPE—Frame type (an integer because it is enum) ■ INTERFERING_AP_INFO_URL—URL ■ MATCHED_IP—Matched IP for classification ■ MATCHED_MAC—Matched MAC for classification ■ NODE_MAC—Node MAC ■ RECEIVER_MAC—Receiver MAC ■ ROGUE_INFO_URL—URL ■ SIGNATURE_NAME—Name of signature matched ■ SNR—Signal-to-Noise Ratio ■ SOURCE_MAC—Source MAC ■ SPOOFED_FRAME_TYPE—Spoofed Frame type (EAP Success) ■ TARGET_AP_BSSID—Target AP BSSID ■ TARGET_AP_SSID—Target AP SSID ■ TRANSMITTER_MAC—Transmitter MAC	
suspect-rap	Test the suspect remote AP feature.	—
bssid <bssid>	Specifies the BSSID of monitored AP.	—
match-type <match-type>	Specifies the match type.	—
match-method <match-method>	Specifies the match method.	—
wired-mac {add | remove}	Tests the rogue AP classification feature. Specifies the wired MAC table.	—
bssid <BSSID> mac <mac>	Specifies BSSID of monitored AP and wired-MAC address.	—
enet-mac <enet-mac> mac <mac>	MAC address of ENET interface of AP and wired-MAC address.	—
prop-wm mac <mac>	Specifies the propagate wired-MAC	—

Parameter	Description	Range
`system-gw-wm mac <mac>`	Specifies the system gateway MAC.	—
`system-wm mac <mac>`	Specifies the system wired-MAC.	—

Usage Guidelines

These commands are intended to be used with an AP that is configured as an air monitor.

Example

The following command sets the air monitor to scan all channels:

```
(host) (config) #am scan 10.1.1.244 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

amon msg-buffer-size

```
amon msg-buffer-size <msg-buffer-size>
```

Description

This command modifies the size of AMON packets on the managed device.

Syntax

Parameter	Description	Range	Default
`<msg-buffer-size>`	The size of AMON packets on the managed device.	1152-40000 bytes	1264 bytes

Example

The following command caps the AMON message size at 1500 bytes:

```
(host)[mynode](config) #amon msg-buffer-size 1500
```

Related Commands

Release	Modification
show amon msg-buffer-size	Displays the size of AMON packets on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **msg-buffer-size** range was modified.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

amon source-interface

```
amon source-interface <vlan-num>
```

Description

This command specifies the IPv4 address of the VLAN as the source IP address.

Syntax

Parameter	Description
`<vlan-num>`	The IPv4 address of the VLAN.

Example

The following example sets the VLAN number.

```
(host) [mynode] (config) #amon source-interface <vlan-num>
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

amon udp

```
[no] amon udp
```

Description

Enable the AirWave server to allow traffic on UDP port 8211.

Syntax

No parameters.

Usage Guidelines

Issue the **no amon udp** command to disable AMON UDP and re-enable it again using the command **amon udp**.

Example

The example below enables AMON UDP.

```
(host) [mynode] (config) #amon udp
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

ap am-filter-profile

```
ap am-filter-profile {default | <profile-name>}
   allow-ap-group
   allow-self
   ap-group <ap-group>
   ap-name <ap-name>
   clone
   filter-enable
   no
```

Description

This command configures an AM filter.

Syntax

Parameter	Description	Default
`am-filter-profile <profile-name>`	Name of this instance of the profile	default
`allow-ap-group`	Allows all APs in the same group as the AP	
`allow-self`	Allows AP to hear its own frames	
`ap-group <ap-group>`	Allows all APs in the group	
`ap-name <ap-name>`	Name of AP to allow	
`clone {default | <source>}`	Copy data from another AM filter	
`filter-enable`	Enable AM filtering	
`no`	Delete command	

Example

The following command allows AM filtering for all APs in the test1 group:

```
(host) [mynode] (config) #ap am-filter-profile test
(host) [mynode] (AM Filter "test") #ap-group test1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

ap ap-blacklist-time

```
ap ap-blacklist-time <ap-blacklist-time>
```

Description

This command determines the time in seconds an AP is blacklisted.

Syntax

Parameter	Description
`<ap-blacklist-time>`	The time in seconds that the AP will remain blacklisted.

Example

The following is an example of the **ap-blacklist-time** command:

```
(host) [mynode] (config) #ap ap-blacklist-time 55
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on the Mobility Master

ap authorization-profile

```
ap authorization-profile {default | <profile-name>}
   ap-authorization-group <profile-name>
   clone {default | <source>}
   no
```

Description

This command defines a temporary configuration profile for remote APs that are not yet authorized on the network.

Syntax

Parameter	Description	Range	Default
`ap authorization-profile <profile-name>`	Name of this instance of the profile.	1–63 characters	default
`ap-authorization-group <profile-name>`	Name of a configuration profile to be assigned to the group unauthorized remote APs.	—	—
`clone {default | <source>}`	Copy data from another authorization profile.	—	default
`no`	Delete command.	—	—

Usage Guidelines

The AP authorization-profile specifies which configuration should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. By default, these yet-unauthorized APs are put into the temporary AP group **authorization-group** and assigned the predefined profile **NoAuthApGroup**. This configuration allows a user to connect to an unauthorized remote AP through a wired port and then enter a corporate username and password. Once a valid user has authorized the remote AP, the AP will be permanently marked as authorized on the network and will then download the configuration assigned to that AP by its permanent AP group.

Example

The following command creates a new authorization profile with a non-default configuration for unauthorized remote APs:

```
(host) [mynode] (config) #ap authorization-profile default2
   (host) [mynode] ((AP Authorization profile "default2") #authorization-group NoAuthApGroup2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap arm client-match

```
ap arm client-match
   activate rules file-name <file-name>
   restore rules
```

Description

This command allows the managed device to use a newer set of ClientMatch rules without updating the entire operating system, reducing network downtime.

Syntax

Parameter	Description	Default
`activate rules file-name <file-name>`	File name of the client-match rules update package.	N/A
`restore rules`	Issue this command to remove an imported client-match rules udpate package and restore the default ClientMatch vaules.	N/A

Usage Guidelines

The ClientMatch rules that manage client associations are primarily based upon the client RF environment, and apply uniformly to all types of clients, regardless of device type or operating system. ArubaOS supports incremental updates to ClientMatch rules to support network devices running newer operating systems that may be incompatible with the existing ClientMatch client association rules. This feature allows the managed deviceto use a newer set of ClientMatch rules without updating the entire operating system, reducing network downtime.

Example

Use the WebUI or CLI to upload an custom update file of client -match rules to the /flash/config folder on Mobility Master. This feature is not available for stand-alone controller deployments.

```
(host)[mm](config)# copy tftp: <tftphost> <filename> flash: <destname>
(host)[mm](config)# copy ftp: <ftphost> <user> <password> flash: <destname>
(host)[mm](config)# copy scp: <scphost> <username> <password> flash: <destname>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
Mobility Master	Base operating system	Config mode on Mobility Master.

ap clarity-synthetic

```
ap clarity-synthetic {ap-name <ap-name> | wired-mac <wired-mac>}
   amsip-addr <amsip-addr> forward-mode
      gre test-id <test-id> | web-sockets test-id <test-id>
         mixed-mode band <a|g> | station-mode
   reset
```

Description

This command allows configuration of the Clarity-Synthetic feature. Clarity Synthetic enables the controller to select and convert a supported AP to client mode. The converted AP acts like a Wi-Fi client and starts synthetic data transaction within the network to monitor and detect the network health.

Syntax

Parameter	Description	Default
`ap clarity-synthetic {ap-name <ap-name>|wired-mac <wired-mac>}`	Specifies the name of the AP or the AP wired MAC address.	
`amsip-addr <amsip-addr> forward-mode`	IP address of Clarity synthetic Server with the forward mode specified for test	
`gre test-id <test-id> | web-sockets test-id <test-id>`	GRE mode of forwarding or the web sockets mode of forwarding with unique test id string	
`mixed-mode band <a|g> | station-mode`	Specifies if AP operates in mixed mode (for either the a or g band) or in only station mode	
`reset`	Resets the AP from Clarity Synthetic mode.	

Usage Guidelines

The Clarity Synthetic feature is supported on 200 Series, 210 Series, and 220 Series access points. This feature helps in detecting network health by using synthetic transaction from a Wi-Fi client. This feature converts the radios of a supported AP to change from AP mode to station mode.

Example

The following command configures the IP address of the Clarity-Synthetic server (in the forward mode used for test) and specifies the GRE mode of forwarding for an AP working in the *a* band :

```
(host) [mynode] #ap clarity-synthetic wired-mac ac:a3:1e:d6:30:f0 amsip-addr 5.6.7.5 forward-mode gre test-id 5 mixed-mode band a
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Mobility Master	Base operating system	Enable or Config mode on Mobility Master.

ap debug advanced-stats

```
ap debug advanced-stats {ap-name <ap-name>}|{ ip-addr <ip-addr>}|{ ip6-addr <ip-addr>}
```

Description

Issue this command under the supervision of Aruba technical support to enable the collection and display of advanced AP debugging information.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP for which you want to record advanced debugging information.
`ip-addr <ip-addr>`	IP address of the AP for which you want to record advanced debugging information.
`ip6-addr <ip6-addr>`	IPv6 address of the AP for which you want to record advanced debugging information.

Usage Guidelines

The additional information collected when advanced net80211 or radio statistics are enabled on an AP appears in the output of the show ap debug radio-stats command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

ap debug client-trace start

```
ap debug client-trace start
   {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>}
```

Description

Use this command to trace management packets from a client MAC address.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IPv4 address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.

Usage Guidelines

This command should only be used under the guidance of Aruba technical support.

Related Commands

Command	Description
ap debug client-trace stop	Use this command to stop tracing management packets from a client MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system.	Enable mode on Mobility Master.

ap debug client-trace stop

```
ap debug client-trace stop
   {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>}
```

Description

Use this command to stop tracing management packets from a client MAC address.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IPv4 address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.

Usage Guidelines

This command should only be used under the guidance of Aruba technical support.

Related Commands

Command	Description
ap debug client-trace start	Use this command to trace management packets from a client MAC address.
show ap debug client-trace	Use this command to show counts of different types of management data frames traced from a client MAC address

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Enable mode on Mobility Master.

ap debug dot 11r remove-key

```
ap debug dot 11r remove-key <mac>
   [ap-name <ap-name> | ip-addr <ip-addr>| ip6-addr <ip6-addr]
```

Description

This command removes the r1 key from an AP.

Syntax

Parameter	Description
`<mac>`	MAC address of the client.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IP address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.

Usage Guideline

Use this command to remove an r1 key from an AP when the AP does not have a cached r1 key during Fast BSS Transition roaming.

Examples

You can use the following command to remove an r1 key from an AP when the AP does not have a cached r1 key during Fast BSS Transition roaming.

```
(host) [mynode] #ap debug dot11r remove-key <mac> ap-name <ap-name> | ip-addr <ip-addr>
(host) [mynode] #ap debug dot11r remove-key 00:50:43:21:01:b8 ap-name MAcage-105-GL
```

Execute the following command to check if the r1 key is removed from the AP:

```
(host) [mynode] #show ap debug dot11r state ap-name MAcage-105-GL
Stored R1 Keys
--------------
Station MAC  Mobility Domain ID  Validity Duration  R1 Key
-----------  ------------------  -----------------  ------
```

Related Commands

Command	Description
show ap debug dot11r	Use this command to check if the r1 key is removed from an AP.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

ap debug openflow

```
ap debug openflow flows
   delete-all {ap-name|ip-addr <ip-addr>|ip6-addr}
```

Description

This command deletes all the OpenFlow flows.

Syntax

Parameter	Description
`flows`	A list of OpenFlow flows.
`delete all`	Deletes all OpenFLow flows. ■ ap-name - name of the AP to be deleted. ■ ip-addr - IPv4 address of the AP. ■ ip6-addr - IPv6 address of the AP.

Usage Guidelines

This command should only be used under the guidance of Aruba technical support.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Enable mode on Mobility Master.

ap debug radio-event-log

```
ap debug radio-event log [start|stop] [ap-name <name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
radio <0|1> events [all|ani|hex|rcfind|rcupdate|rx|size|text|tx]>]
```

Description

Start and stops packet log capture of radio events for debugging purposes, and sends a log file of the events to a dump server when logging stops.

Syntax

Parameter	Description
`start`	Start Wi-Fi packet log capture.
`ap-name <ap-name>`	Name of the AP for which you want to capture packet log events.
`radio 0|1`	Include this parameter to start or stop packet log capture for the specified radio.
`events`	Classification the event type to capture, can be hex and multiple, default all. ■ all: Capture all of the following types of radio events ■ ani : Adaptive Noise Immunity control events ■ hex: Hex format of event tx=0x1|rx=0x2|rcfind=0x4|rcupdate=0x8|ani=0x10|text=0x20 ■ rcfind: Transmission (Tx) control event ■ rcupdate: Transmission (Tx) rate update event ■ rx: Received (Rx) status register event ■ size: radio log size,range 1024-10485760 bytes(1KB-10MB), Default:3145728 bytes(3MB) ■ text: Text record event ■ tx: Transmission (Tx) control and Tx status register event
`ip-addr <ip-addr>`	IPv4 address of the AP for which you want to capture packet log events.
`ip6-addr <ip6-addr>`	IPv6 address of the for which you want to capture packet log events.
`stop`	Stop Wi-Fi packet log capture and send a log file of the events to a dump server.

Example

The following commands starts and stops a Wi-Fi radio event log:

```
(host) [mynode] #ap debug radio-event-log start ap-name 6c:f3:7f:c6:71:90 radio 0 events all
(host) [mynode] #ap debug radio-event-log stop ap-name 6c:f3:7f:c6:71:90 radio 0
```

Related Commands

Command	Description
show ap debug dot11r	Use this command to display the Radio log capture status.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

allap debug radio-registers dump

```
ap debug radio-registers dump [[filename <filename> {all|interrupt|qcu |radio}]ap-name
<name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
```

Description

This command allows you to collect all or specific radio register information into a separate file.

Syntax

Parameter	Description
`ap-name`	Name of the access point.
`filename`	Name of file where information is collected.
`all`	All registers interrupted.
`interrupt`	Interrupt related registers.
`qcu`	Collect QCU information.
`radio`	Radio ID (0 or 1).
`ip-addr`	Collect radio register information for this specific AP radio.
`ip6-addr`	Collect radio register information for the AP assigned to this ipv6 address.

Usage Guidelines

This command collects specified radio-register information for debugging purposes, dumps the registers into a local file, and will automatically transfer the file to the dump-server that is configured in ap-system-profile.

Example

The following command collects all radio registers from **myap1** into a file called **myradioregfile**:

```
(host) [mynode] #ap debug radio-registers dump ap-name myap1 filename myradioregfile all
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
802.11n-capable APs	Base operating system.	Enable mode on Mobility Master.

ap debug stm-trace

```
ap debug stm-trace category
   [ip-addr <ip-addr> | loglevel | mac <mac>]
```

Description

This command enables / disables stm-trace categories.

Syntax

Parameter	Description
`category`	The trace category to be enabled or disbaled. ■ all - Traces all categories ■ amon - Traces in the category of AMON ■ auth - Traces in the category of authentication ■ bss - Traces in the category of BSSIDs ■ cluster - Traces in the category of cluster ■ config - Traces in the category of configuration ■ enet - Traces in the category of AP Enet port management ■ gsm - Traces in the category of GSM ■ radio - Traces in the category of radio ■ sapm - Traces in the category of cluster ■ sos - Traces in the category of SOS ■ station - Traces in the category of stations ■ syslog - Traces in the category of syslog ■ system - Traces in the category of general system
`ip-addr <ip-addr>`	Trace events related to the AP IP address.
`loglevel`	The loglevel of the syslogs to be included in the trace. ■ alert - Trace all logs equal or higher than LOG_ALERT ■ critical - Trace all logs equal or higher than LOG_CRIT ■ debug - Trace all logs equal or higher than LOG_DEBUG ■ emergency - Trace all logs equal or higher than LOG_EMERG ■ error - Trace all logs equal or higher than LOG_ERR ■ info - Trace all logs equal or higher than LOG_INFO ■ notice - Trace all logs equal or higher than LOG_NOTICE ■ warn - Trace all logs equal or higher than LOG_WARN
`mac <mac>`	Trace events related to the client MAC address.

Examples

You can use the following command to trace all events related to the IP address.

```
(host) [mynode]  #ap debug stm-trace category all ip-addr <ip-addr>
(host) [mynode]  #ap debug stm-trace category all 10.20.10.20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

ap deploy-profile

```
ap deploy-profile
   blacklist
   default-ap-group
   enable
   ip-range <start> <end>
   ipv6-range <start> <end>
   no
```

Description

This command applies the AP deployment policy to the default AP group, and/or to the list of AP MAC addresses included in the UAP blacklist table, and/or to the specified IP address range. The AP deployment policy redirects the applicable APs to the Instant discovery process, ensuring that the APs run only in controller-less mode.

Syntax

Parameter	Description	Range	Default
`blacklist`	Enables the blacklist policy. Applies the AP deployment policy to the APs whose MAC addresses are included in the UAP blacklist table.	—	disabled
`default-ap-group`	Applies the AP deployment policy to the default AP group.	—	disabled
`enable`	Enables the AP deploy profile. The policies configured are enforced only if this is enabled.	—	disabled
`ip-range`	Applies the AP deployment policy to the specified IPv4 address range. You can define up to 128 IPv4 address ranges.	—	—
`<start>`	Starting IPv4 address of the range.	—	—
`<end>`	Ending IPv4 address of the range.	—	—
`ipv6-range`	Applies the AP deployment policy to the specified IPv6 address range. You can define up to 128 IPv6 address ranges.	—	—
`<start>`	Starting IPv6 address of the range.	—	—
`<end>`	Ending IPv6 address of the range.	—	—
`no`	Removes the AP deploy profile configuration.	—	—

Example

The following set of commands enable the AP deployment policy :

```
(host) [mynode] (config) #ap deploy-profile
(host) [mynode] (ap deploy-profile) #enable
```

The following command applies the AP deployment policy to an IPv4 address range with a starting IP address of 1.1.1.1 and ending IP address of 1.1.1.10:

```
(host) [mynode] (ap deploy-profile) #ip-range <1.1.1.1> <1.1.1.10>
```

The following command enables the blacklist policy in the AP deploy profile:

```
(host) [mynode] (ap deploy-profile) #blacklist
```

The following command removes the AP deployment policy configuration:

```
(host) [mynode] (config) #no ap deploy-profile
```

Related Commands

Command	Description
show ap deploy-profile	The **show ap deploy-profile** command displays the complete list of IP address ranges to which the AP deployment policy is applied.
uap-blacklist	This command adds AP MAC addresses to the UAP blacklist database. When the blacklist policy is enabled in the AP deploy profile, it is applied to this blacklist database entries.

Command History

Release	Modification
ArubaOS8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on master Mobility Master

ap enet-link-profile

```
ap enet-link-profile {default | <profile>}
   clone {default | <source>}
   dot3az
   dot3bz
   duplex {auto | full | half}
   no ...
   poe
   speed {10 | 100 | 1000 | 2500 | 5000 | auto}
```

Description

This command configures an AP Ethernet link profile.

Syntax

Parameter	Description	Range	Default
`ap enet-link-profile <profile>`	Name of this instance of the profile. The name must be 1-63 characters long.	—	default
`clone <source>`	Name of an existing Ethernet Link profile from which parameter values are copied.	—	default
`dot3az`	Enable support for the 803.az Energy Efficient Ethernet standard, which allows the APs to consume less power during periods of low data activity. If this feature is enabled for an AP group, any APs in the group that do not support 803.az will ignore this setting.	—	disabled
`dot3bz`	Enable support for IEEE 802.3bz standard. Only 330 Series access points are compliant with this standard.	—	enabled
`duplex`	The duplex mode of the Ethernet interface, either full, half, or auto-negotiated.	full half auto	auto
`no`	Negates any configured parameter.	—	—
`poe`	Enables PoE for APs that support PoE.	—	—
`speed`	The speed of the Ethernet interface, either 10 Mbps, 100 Mbps, 1000 Mbps (1 Gbps), or auto-negotiated.	10 100 1000 2500 5000 auto	auto

Usage Guidelines

This command configures the duplex and speed of the Ethernet port on the AP. The configurable speed is dependent on the port type.

Example

The following command configures the Ethernet link profile for full-duplex and 100 Mbps:

```
(host) [mynode] (config) #ap enet-link-profile enet
   (host) [mynode] (AP Ethernet Link profile "enet") #duplex full
   (host) [mynode] (AP Ethernet Link profile "enet") #speed 100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master.

ap flush-r1-on-new-r0

```
ap flush-r1-on-new-r0
```

Description

Use this command to enable or disable flushing of R1 keys, when R0 is updated for d-tunnel or bridge mode.

Example

The following example enables flushing of R1 keys:

```
(host) [mynode] (config) #ap flush-r1-on-new-r0
```

The following command displays the status of flushing of R1 keys:

```
(host) [mynode] (config) #show flush-r1-on-new-r0
Fast Roaming flush-r1-on-new-r0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode or Config mode on the Mobility Master or the managed device

ap image-preload

```
ap image-preload
   activate all-aps|specific-aps
   add {ap-group <ap-group> | ap-name <ap-name>}
   cancel
   clear-all
   delete {ap-group <ap-group> | ap-name <ap-name>}
   [partition <part-num>]
   [max-downloads <max-downloads>]
```

Description

Configure APs to preload a new software image from a managed device before it starts actively running the new image.

Syntax

Parameter	Description
`activate`	Issue the **ap image-preload activate** command to activate this feature, allowing APs in the preload list to start downloading their new image from the managed device.
`all-aps`	All APs will be allowed to pre-download the image.
`specific-aps`	Only APs in the preload list will be allowed to preload the image.
`add`	Add individual APs or AP groups to the list of APs allowed to preload the image.
`ap-group <group>`	Add a group of APs to the preload list.
`ap-name <name>`	Add an individual AP to the preload list.
`cancel`	Cancel the AP preload and clear the preload list. Any APs downloading a new image at the time this command is issued will continue to download the file.
`clear-all`	Clear all APs from the preload list.
`delete`	Delete an individual AP or AP group from the preload list. **NOTE:** This command may be issued before or after preloading is activated. If it is executed after preloading has already been activated, any APs downloading a new image at the time this command is issued will continue to download the file. APs that are still waiting to preload will be removed from the preload list.
`ap-group <group>`	Remove the specified group of APs from the preload list
`ap-name <name>`	Remove an individual AP from the preload list
`partition <partition-num>`	Specify the partition from which the APs should download their images. By default, the APs will preload images from the default boot partition of the managed device.
`max-downloads <max-downloads>`	Specify the maximum number of APs that can simultaneously download their image from the managed device. The default value is ten APs.

Usage Guidelines

The AP image preload feature minimizes the downtime required for a Mobility Master upgrade by allowing the APs to download the new images before the Mobility Master actually starts running the new version.

This feature allows you to select the maximum number of APs that are allowed to preload the new software image at any one time, thereby reducing the possibility that the Mobility Master may get overloaded or that network traffic may be impacted by all APs on the Mobility Master attempting to download a new image at once.

APs can continue normal operation while they are downloading their new software version. When the download completes, the AP sends a message to the Mobility Master, informing it that the AP has either successfully downloaded the new software version, or that the preload has failed for some reason. If the download fails, the AP will retry the download after a brief waiting period.

You can allow every AP on a managed device to preload a new software version, or also create a custom list of AP groups or individual APs that can use this feature. If a new AP associates to the managed device while the AP image download feature is active, the managed device will check the name and group of that AP to see if it appears in the preload list. If an AP is on the list, (and does not already have the specified image in its Flash memory) that AP will start preloading its image.

Once a software version has been downloaded by an AP, another version cannot be downloaded until the AP reboots.

Example

The following command enables the image preload feature and adds the APs in the AP groups corp1 and corp2 to the preload list.

```
(host)[mynode](config)#ap image-preload activate specific-aps
(host)[mynode](config)#add ap-group corp1
(host)[mynode](config)#add ap-group corp2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Enable mode on Mobility Master.

ap gap-db

```
ap gap-db
[reinit-
resync lms {lms-ip <lms-ip>}|{lms-ip6 <lms-ip6>} [{ap-name <ap-name>|{wired-mac <wired-mac>}]
```

Description

Resynchronize an AP status on a managed device and Mobility Master

Syntax

Parameter	Description
`reinit-db`	Re-initialize GAP DB.
`resync`	Trigger a re-sync.

`lms-ip <lms-ip>`
 	
`lms-ip6 <lms-ip6>`
	Synchronize the status of all APs terminating on the specified Managed device. Specify either the IPv4 address or the IPv6 address of the managed device.

`ap-name <ap-name>`	Synchronize only the AP with the specified AP name.
`wired-mac <wired-mac>`	Synchronize only the AP with the specified MAC address.

Usage Guidelines

A managed device sends AP status messages about the APs terminating on that managed device to Mobility Master. In the event that an AP state appears to be different between Mobility Master and the managed device, this command will resynchronize the AP status information by allowing the managed device and Mobility Master to exchange a list of APs.

Example

The following command triggers a resynchronization for an IPv4 address of the managed device.

```
(host)[mynode]#ap gap-db resync lms lms-ip 10.20.10.20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

ap general-profile

```
ap general-profile
   periodic-sync
```

Description

This command configures the general profile of an AP.

Syntax

Parameter	Description	Range
`ap general-profile`	Configures the AP general profile.	—
`periodic-sync`	Enables AP State periodic sync.	—
`sync-interval <sync-interval>`	Specifies AP State sync interval in minutes.	55–1440 minutes (24 hours)
`no`	Negates any previous configuration.	—

Usage Guidelines

This command configures the general profile of an AP.

Example

The following example enables the AP state periodic sync of an AP:

```
(host) [mynode] (config) #ap general-profile
(host) [mynode] (ap general-profile) #periodic-sync
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

ap-lacp-striping-ip

```
ap-lacp-striping-ip
   aplacp-enable
   no
   striping-ip <ip-addr> lms <LMS>
```

Description

Define an AP LACP LMS map information profile that maps a GRE striping IP address to an existing LMS-IP address.

Syntax

Parameter	Description
`ap-lacp-striping-ip`	Configures the AP LACP LMS map information.
`aplacp-enable`	Enables LACP IP striping. This feature is disabled by default.
`no ...`	Negate any setting or return a configured parameter it to its default value.
`striping-ip <ip-addr>`	Specify an IPv4 address for the 802.11g radio of the controller to allow LACP-enabled switches to send traffic for the two controller radios on different links. Recommended value for this parameter is **lms <ip-addr>**+1.
`lms <LMS>`	Enter the LMS IP address currently defined in the device's AP system profile to map the existing LMS IP to the GRE striping IP address.

Usage Guidelines

The **AP LACP LMS map information** profile is a local profile that maps a LMS IP address (defined in the AP system profile) to a GRE striping IP address. If 220 Series or 270 Series access points fail over to a standby or backup controller, the AP LACP LMS map information profile on the new controller defines the IP address that the APs use to terminate 802.11.g radio tunnels on the new controller. This feature allows 220 Series, 270 Series, and 320 Series access points to continue to support link aggregation to a backup controller in the event of a controller failure even if the backup controller is in a different L3 network.

If your topology includes a backup controller you must define GRE striping IP settings in the active and the backup controller.

Example

On Mobility Master

```
(host)[node] (config) #ap system-profile LACP
(host)[node] (AP system-profile "LACP") #lms-ip 192.0.2.1
(host)[node] (AP system-profile "LACP") #bkup-lms-ip 192.0.77.1
(host)[node] (AP system-profile "LACP") #exit
(host)[node] (config) #ap-lacp-striping-ip
(host)[node] (AP LACP LMS map information) #striping-ip 192.0.2.2 lms 192.0.2.1
(host)[node] (AP LACP LMS map information) #aplacp-enable
```

On an L2-connected High Avability (HA) standby or HA+VRRP controller:

```
(bkup-host)[node] (config) #ap-lacp-striping-ip
(bkup-host)[node] (config) (AP LACP LMS map information) #striping-ip
  192.0.2.16 lms 192.0.2.1
(bkup-host) [node] (config)(AP LACP LMS map information) #aplacp-enable
```

On L3-connected High Availability (HA) standby controllers, or HA controllers in dual HA mode, where each dual-mode controller acts as standby for the APs served by the other dual-mode controller:

```
(bkup-host)[node] (config) #ap-lacp-striping-ip
(bkup-host)[node] (config) (AP LACP LMS map information) #striping-ip
  10.1.1.14 lms 192.0.2.1
(bkup-host)[node] (config) (AP LACP LMS map information) #striping-ip
  192.0.2.2 lms 192.0.2.1
(bkup-host) [node] (config)(AP LACP LMS map information) #aplacp-enable
```

If you are using High Availability between L3-connected or dual-mode controllers, you must configure **two** different striping IPs (one for each subnet) to ensure that both controllers will have striping IPs mapped to the corresponding LMS IP address.

Important Points to Remember

- In the upstream direction when the AP transmits GRE frames to the Mobility Master the bonding driver must be in active-active mode and not in the default active-standby mode to allow link aggregation.
- If an AP's uplink access switch ports are configured in static port-channel mode, then the AP will set the Ethernet bonding mode to static port-channel (xor mode) only if **gre-striping-ip** is configured. If **gre-striping-ip** is not configured, then the AP goes back to **active-standby** mode. In this scenario, the AP may go down depending on the behavior of the upstream switch.
- If an AP's uplink access switch ports are configured in dynamic LACP mode, the AP detects LACP-PDUs and automatically sets the Ethernet bonding mode to LACP. If **gre-striping-ip** is not configured, then the AP's Ethernet bonding mode will continue to be in LACP mode, but the AP will send GRE traffic only through one Ethernet port.
- In 320 Series and 330 Series access points, if AP uplink packet capture is taken, the downstream traffic will have sequence number in GRE header. Wireshark Aruba wlan decoder will not be able to decode these packets correctly since it looks for known Aruba GRE tunnel IDs.
- Ensure that the **gre-striping-ip** is unique and not used by any other host on the subnet.
- LACP support is limited to a use case where Enet 0 and Enet 1 ports of the AP are connected to a switch, and LACP is enabled on the two corresponding switch ports.
- The port priority is not applicable to the AP as both ports need to be used. This value is always set to the maximum numerical priority (0xFF), which is the lowest priority.
- The system priority is not configurable. It is set to the maximum numerical value (0xFFFF), which is the lowest priority. This leaves control of the aggregate to the upstream switch.
- The timeout value is not configurable.
- The key is not configurable and the default key value is 1.
- LACP cannot be enabled if wired AP functionality is enabled on the second port. You cannot enable LACP if the Enet 1 port is shutdown.

Troubleshooting Link Aggregation

The following show commands in the CLI can be used to troubleshoot Link Aggregation on 220 Series , 270 Series, 320 Series and 330 Series access points:

- **show ap debug lacp ap-name <ap-name>**—Using this command, you can view if LACP is active on an AP. It displays the number of GRE packets sent and received on the two Ethernet ports. Using this command with verbose option on 320 Series and 330 Seriesaccess points displays packet re-ordering statistics of each wlan client.
- **show ap database**—The output of this command includes an **LACP Striping** flags to indicate of the AP is configured with a LACP striping IP address,

- **show datapath tunnel**—Using this command on 220 Series/270 Series access points, you can verify if the 2.4GHz tunnels are anchored on the **gre-striping-ip** (The GRE IDs for these tunnels are in a range between 0x8300 and 0x83F0) . On 320 Series and 330 Series access points, use the verbose option to verify that 5 Ghz tunnels have striping IP set in the column **StripIP** (The GRE IDs for these tunnels are in a range between 0x8200 and 0x82F0).
- **show datapath station**—On 320 Series and 330 Series access points, using this command displays the LACP sequence number sent in the GRE header of the last packet to the client. This information is displayed under **Seq** column.
- **show ap remote debug anul-sta-entries**—On 320 Series and 330 Series access points, using this command displays LAG enabled/disabled per station and data drops due to LAG packet reordering.
- **show datapath user**—Using this command, you can verify if the **gre-striping-ip** has an entry with the 'L' (local) flag
- **show datapath route-cache**—Using this command, you can verify if the **gre-striping-ip** has an entry with the LC MAC.

Related Commands

The following show commands display information about the settings defined in the AP LACP LMS map information profile:

Command	Description
show ap-lacp-striping-ip	Displays all settings defined in AP LACP LMS map information profile.
show ap database	The output of this command displays an **s** flag to indicate that the AP is enabled with a striping IP address.
show ap debug lacp	The output of this command displays the striping IP address of the AP, as defined in the AP LACP LMS map information profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

ap lldp med-network-policy-profile

```
ap lldp med-network-policy-profile {default | <profile-name>}
   application-type
   guest-voice
   guest-voice-signaling
   softphone-voice
   streaming-video
   video-conferencing
   video-signaling
   voice
   voice-signaling
   clone {default | <source>}
   dscp <dscp>
   l2-priority <l2-priority>
   no ...
   tagged
   vlan <vlan>
```

Description

Define an LLDP MED network policy profile that defines DSCP values and L2 priority levels for a voice or video application.

Syntax

Parameter	Description	Default
`ap lldp med-network-policy-profile <profile-name>`	Configures an AP LLDP-MED Network Policy Profile	Default
`application-type`	Specifies the type of application that this profile manages.	—
`guest-voice`	Use this application type if the AP services a separate voice network for guest users and visitors.	—
`guest-voice-signaling`	Use this application type if the AP is part of a network that requires a different policy for guest voice signaling than for guest voice media. Do not use this application type if both the same network policies apply to both guest voice and guest voice signaling traffic.	—
`softphone-voice`	Use this application type if the AP supports voice services using soft phone software applications on devices such as PCs or laptops.	—

Parameter	Description	Default
`streaming-video`	Use this application type if the AP supports broadcast or multicast video or other streaming video services that require specific network policy treatment. This application type is not recommended for video applications that rely on TCP with buffering.	—
`video-conferencing`	Use this application type of the AP supports video conferencing equipment that provides real-time, interactive video and audio services.	—
`video-signaling`	Use this application type if the AP is part of a network that requires a different policy for video signaling than for the video media. Do not use this application type if both the same network policies apply to both video and video signaling traffic.	—
`voice`	Use this application type if the AP services IP telephones and other appliances that support interactive voice services. **NOTE:** This is the default application type.	—
`voice-signaling`	Use this application type if the AP is part of a network that requires a different policy for voice signaling than for the voice media. Do not use this application type if both the same network policies apply to both voice and voice signaling traffic.	—
`clone {default | <source>}`	Makes a copy of an existing profile by specifying that profile name.	—
`dscp <dscp>`	Selects a DSCP priority value for the specified application type by specifying a value from 0-63, where 0 is the lowest priority level and 63 is the highest priority.	0–63 Default is 0

Parameter	Description	Default
`l2-priority <L2-priority>`	Select a 802.1p priority level for the specified application type, by specifying a value from 0–7, where 0 is the lowest priority level and 7 is the highest priority.	0–7 Default is 0
`no`	Negates any setting or return a configured parameter it to its default value.	—
`tagged`	Specifies if the policy applies to a to a VLAN that is tagged with a VLAN ID or untagged. The default value is untagged. **NOTE:** When an LLDP-MED network policy is defined for use with an untagged VLAN, then the L2 priority field is ignored and only the DSCP value is used.	Default is untagged
`vlan <vlan>`	Specifies a VLAN by VLAN ID (0–4094) or VLAN name.	Default is 0

Usage Guidelines

LLDP-MED (media endpoint devices) is an extension to LLDP that supports interoperability between VoIP devices and other networking clients. LLDP-MED network policy discovery lets endpoints and network devices advertise their VLAN IDs (for example, voice VLAN), priority levels, and DSCP values. ArubaOS supports a maximum of eight LLDP -MED Network Policy profiles.

Creating an LLDP MED network policy profile does not apply the configuration to any AP or AP interface or interface group. To apply the LLDP-MED network policy profile, you must associate it to an LLDP profile, then apply that LLDP profile to an AP wired port profile.

Example

The following commands create a LLDP MED network policy profile for streaming video applications and marks streaming video as high-priority traffic.

```
(host) [mynode] (config) #ap lldp med-network-policy-profile vid-stream
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #dscp 48
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #l2-priority 6
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #tagged
(host) [mynode] (AP LLDP-MED Network Policy Profile "vid-stream") #vlan 10
```

Next, the LLDP MED network policy profile is assigned to an LLDP profile, and the LLDP profile is associated with an AP wired-port profile.

```
(host) [mynode] (config) #ap lldp profile video1
(host) [mynode] (AP LLDP Profile "video1") #ap lldp-med-network-policy-profile vid-stream
(host) [mynode] (AP LLDP Profile "video1") #
(host) [mynode] (config) #ap wired-port-profile corp2
(host) [mynode] (AP wired port profile "corp2") #lldp-profile video1
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap lldp profile

```
ap lldp profile {default | <profile-name>}
   clone {default | <source>}
   dot1-tlvs [port-vlan | vlan-name]
   dot3-tlvs [link-aggregation | mac| mfs| power]
   lldp-med-network-policy-profile {default | <lldp-med-network-policy-profile>}
   lldp-med-tlvs [capabilities | inventory | network-policy]
   no ...
   optional-tlvs [capabilities | management-address | port-description | system-description |
   system-name]
   receive
   transmit
   transmit-hold <transmit-hold [1-100>
   transmit-interval <transmit-interval[1-3600]>
```

Description

Define an LLDP profile that specifies the TLV elements to be sent in LLDP PDUs.

Syntax

Parameter	Description	Range	Default
`ap lldp profile <profile-name>`	Configures an AP LLDP profile.		default
`clone <profile>`	Make a copy of an existing LLDP profile.		default
`dot1-tlvs`	Specify the 802.1 TLV that the AP will send in LLDP PDUs. By default, the AP will send every 802.1 TLV.		
`port-vlan`	Transmit the LLDP 802.1 port VLAN TLV. If the native VLAN is configured on the port, the port-vlan TLV will send that value, otherwise it will send a value of 0.		
`vlan-name`	Transmit the LLDP 802.1 VLAN name TLV. The AP sends a value of "Unknown" for VLAN 0, or "VLAN <number>" for non-zero VLAN numbers.		

Parameter	Description	Range	Default
dot3-tlvs	Specify the 802.3 TLV that the AP will send in LLDP PDUs. By default, the AP will send every 802.3 TLV.		
link-aggregation	Transmit the 802.3 link aggregation TLV to indicate that link aggregation is not supported.		
mac	Transmit the 802.3 MAC or PHY Configuration or Status TLV to indicate the duplex and bit rate capacity, and current duplex and bit rate settings of the AP interface.		
mfs	Transmit the 802.3 Maximum Frame Size TLV to show the maximum frame size capability of the AP.		
power	Transmit the 802.3 Power via media dependent interface (MDI) TLV to show the power support capabilities of the AP interface. **NOTE:** This parameter is supported by the RAP-3WNP and 130 Series only.		
lldp-med-network-policy-profile <profile>	Specify the LLDP MED Network Policy profile to be associated with this LLDP profile.		
lldp-med-tlvs	Specify the LLDP-MED TLV that the AP will send in LLDP PDUs. By default, the AP will not send any LLDP-MED TLV.		

Parameter	Description	Range	Default
capabilities	Transmit the LLDP-MED capabilities TLV. The AP will automatically send this TLV if any other LLDP-MED TLV is enabled.		
inventory	Transmit the LLDP-MED inventory TLV. **NOTE:** An AP cannot send this TLV unless it also sends the LLDP-MED capabilities TLV.		
network-policy	Transmit the LLDP-MED network-policy TLV. **NOTE:** An AP cannot send this TLV unless it also sends the LLDP-MED capabilities TLV.		
optional-tlvs	Specify the optional TLV that the AP will send in LLDP PDUs.		
capabilities	Transmit the system capabilities TLV to indicate which capabilities are supported by the AP.		
management-address	Transmit a TLV that indicates the management IP address of the AP, in either IPv4 or IPv6 format.		
port-description	Transmit a TLV that gives a description of the wired port of an AP in an alphanumeric format.		
system-description	Transmit a TLV that describes the model number and software version of the AP.		

Parameter	Description	Range	Default
system-name	Transmit a TLV that sends the AP name or wired MAC address.		
receive	Issue this command to enable LLDP PDU reception. This parameter is enabled by default.		
transmit	Issue this command to enable LLDP PDU transmission. This parameter is enabled by default.		
transmit-hold <transmit-hold>	Enter a value from 1–100. This value is multiplied by the transmit interval to determine the number of seconds to cache learned LLDP information before that information is cleared. If the transmit-hold value is at the default value of 4, and the transmit interval is at its default value of 30 seconds, then learned LLDP information will be cached for 4 x 30 seconds, or 120 seconds.	1–100	4
transmit-interval <transmit-interval>	The interval between LLDP TLV transmission seconds. The supported range is 1–3600 seconds and the default value is 30 seconds.	1–3600 seconds	30 seconds

Usage Guidelines

LLDP is a Layer-2 protocol that allows network devices to advertise their identity and capabilities on a LAN. Wired interfaces on Aruba APs support LLDP by periodically transmitting LLDP PDUs consisting of TLV elements. Use this command to specify the TLV that should be sent by the AP interface associated with the LLDP profile.

Example

The following command configures an LLDP profile, allows the AP interface to send the port-vlan and vlan-name TLV.

```
(host) [mynode] (config)#ap lldp profile 8021TLVs
(host) [mynode] (AP LLDP Profile "8021TLVs") #dot1-tlvs port-vlan
(host) [mynode] (AP LLDP Profile "8021TLVs") #dot1-tlvs vlan-name
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap mesh-cluster-profile

```
ap mesh-cluster-profile <profile-name>
   clone <source>
   cluster <cluster>
   no
   opmode {opensystem|wpa2-psk-aes}
   rf-band {a|g}
   wpa-hexkey <wpa-hexkey>
   wpa-passphrase <wpa-passphrase>
```

Description

This command configures a mesh cluster profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`ap mesh-cluster-profile <profile-name>`	Configures a mesh cluster profile. Give a name to the mesh cluster profile. The name must be 1–63 characters long.	—	default
`clone <source>`	Copies parameter values from an existing mesh cluster profile.	—	—
`cluster <cluster>`	Indicates the mesh cluster name. The name can have a maximum of 32 characters and is used as the MSSID for the mesh cluster. When you first create a new mesh cluster profile, the profile uses the default cluster name “Aruba-mesh”. Use the **cluster** parameter to define a new, unique MSSID before you assign APs or AP groups to the mesh cluster profile. **NOTE:** If you want a mesh cluster to use WPA2-PSK-AES encryption, *do not use spaces in the mesh cluster name*, as this may cause errors in mesh points associated with that mesh cluster. To view existing mesh cluster profiles, use the CLI command show ap mesh-cluster-profile.	—	Aruba-mesh
`no`	Negates any configured parameter.	—	—

Parameter	Description	Range	Default
`opmode`	Configures one of the following data encryption types: ■ **opensystem**: No encryption. ■ **wpa2-psk-aes**: WPA2 with AES encryption using a pre-shared key. Best practices are to select wpa2-psk-aes and use the **wpa-passphrase** parameter to select a passphrase. Keep the passphrase in a safe place.	opensystem wpa2-psk-aes	opensystem
`rf-band`	Configures the RF band in which multiband mesh nodes must operate: ■ **a**: 802.11a ■ **g**: 802.11g Best practices are to use 802.11a radios for mesh deployments.	a g	a
`wpa-hexkey <wpa-hexkey>`	Configures a WPA PSK.	—	—
`wpa-passphrase <wpa-passphrase>`	Sets the WPA password that generates the PSK.	—	—

Usage Guidelines

Mesh cluster profiles are specific to mesh nodes (APs configured for mesh) and provide the framework of the mesh network. You must define and configure the mesh cluster profile before configuring an AP to operate as a mesh node.

You can configure multiple mesh cluster profiles to be used within a mesh cluster. You must configure different priority levels for each mesh cluster profile. See ap-group or ap-name for more information about priorities.

Cluster profiles, including the “default” profile, are not applied until you provision your APs for mesh.

Example

The following command configures a mesh cluster profile named “cluster1” for the mesh cluster “headquarters:”

```
(host) [mynode] (config) #ap mesh-cluster-profile cluster1
(host) [mynode] (Mesh Cluster profile "cluster1")cluster headquarters
```

Related Commands

Command	Description
show ap mesh-cluster-profile	Displays the complete list of cluster profiles and their profile status. Include the **<profile-name>** parameter to view the settings for a specific mesh cluster profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap mesh-ht-ssid-profile

```
ap mesh-ht-ssid-profile {default | <profile-name>}
   40MHz-enable
   80MHz-enable
   ba-amsdu-enable
   clone {default | <source>}
   high-throughput-enable
   ldpc
   legacy-stations
   max-rx-a-mpdu-size {8191 | 16383 | 32767 | 65535}
   max-tx-a-mpdu-size <max-tx-a-mpdu-size>
   max-tx-a-msdu-count-be <max-tx-a-msdu-count-be>
   max-tx-a-msdu-count-bk <max-tx-a-msdu-count-bk>
   max-tx-a-msdu-count-vi <max-tx-a-msdu-count-vi>
   max-tx-a-msdu-count-vo <max-tx-a-msdu-count-vo>
   max-vht-mpdu-size {3895 | 7991 | 11454}
   min-mpdu-start-spacing {0.25 | 0.5 | 0 | 1 | 2 | 4 | 8 | 16}
   mpdu-agg
   no
   short-guard-intvl-20MHz
   short-guard-intvl-40MHz
   short-guard-intvl-80MHz
   stbc-rx-streams {0 | 1}
   stbc-tx-streams
   supported-mcs-set
   temporal-diversity
   very-high-throughput-enable
   vht-supported-mcs-map <supported-mcs-set>
   vht-txbf-explicit-enable
```

Description

This command configures a mesh HT SSID profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`ap mesh-ht-ssid-profile <profile-name>`	Configures a Mesh HT SSID profile. Enter the name of an existing mesh high-throughput SSID profile to modify that profile, or enter a new name or create a new mesh HT profile. The mesh HT profile can have a maximum of 32 characters. To view existing HT SSID radio profiles, use the command **show ap mesh-radio-profile**.		default
`40MHz-enable`	Enable or disable the use of 40 MHz channels. This parameter is enabled by default.		enabled
`80MHz-enable`	Enable or disable the use of 80 MHz channels.		enabled

Parameter	Description	Range	Default
`ba-amsdu-enable`	Enable or Disable Receive AMSDU in BA negotiation.		enabled
`clone <source>`	Copy configuration information from a source profile into the currently selected profile.		
`high-throughput-enable`	Enable or disable HT (802.11n) features on this SSID. This parameter is enabled by default.		enabled
`ldpc`	If enabled, the AP will advertise Low-density Parity Check (LDPC) support. LDPC improves data transmission over radio channels with high levels of background noise.		enabled
`legacy-stations`	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).		enabled
`max-rx-a-mpdu-size`	Maximum size of a received aggregate MPDU, in bytes.	8191, 16383, 32767, 65535	
`max-tx-a-mpdu-size <max-tx-a-mpdu-size>`	Maximum size of a transmitted aggregate MPDU, in bytes.	1576–65535	
`max-tx-a-msdu-count-be <max-tx-a-msdu-count-be>`	Maximum number of MSDUs in a TX A-MSDU on best-effort AC. TX-AMSDU disabled if 0.	0–15	2
`max-tx-a-msdu-count-bk <max-tx-a-msdu-count-bk>`	Maximum number of MSDUs in a TX A-MSDU on background AC. TX-AMSDU disabled if 0.	0–15	2
`max-tx-a-msdu-count-vi <max-tx-a-msdu-count-vi>`	Maximum number of MSDUs in a TX A-MSDU on video AC. TX-AMSDU disabled if 0.	0–15	2
`max-tx-a-msdu-count-vo <max-tx-a-msdu-count-vo>`	Maximum number of MSDUs in a TX A-MSDU on voice AC. TX-AMSDU disabled if 0.	0–15	0
`max-vht-mpdu-size`	Maximum size of a VHT MPDU.	3895, 7991, 11454	11454

Parameter	Description	Range	Default
`min-mpdu-start-spacing`	Minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.	0 (No restriction on MDPU start spacing), .25 µsec, .5 µsec, 1 µsec, 2 µsec, 4 µsec, 8 µsec, 16 µsec	0 µs
`mpdu-agg`	Enable or disable MPDU aggregation. HT mesh APs are able to send aggregated MDPUs, which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU.		enabled
`no`	Delete command.		
`short-guard-intvl-20Mhz`	Enable or disable use of short (400 ns) guard interval for 130 Series APs in 20 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput. This parameter is enabled by default.		enabled

Parameter	Description	Range	Default
`short-guard-intvl-40Mhz`	Enable or disable use of short (400 ns) guard interval in 40 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput. This parameter is enabled by default.		enabled
`short-guard-intvl-80Mhz`	Enable or disable use of short (400 ns) guard interval in 80 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput. This parameter is enabled by default.		enabled

Parameter	Description	Range	Default
`stbc-rx-streams`	Controls the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0–7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)	0–1	1
`stbc-tx-streams`	Controls the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0–7. Higher MCS values are not supported. (Supported on 170 Series, 130 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)	0–1	1
`supported-mcs-set <supported-mcs-set>`	A list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20 MHz vs. 40 MHz) and the number of spatial streams used by the mesh node. The default value is 0–31—16–23 are supported on 130 Series/RAP-15x/802.11ac APs only; 24–31 are supported on 320 Series/330 Series only. To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma. Examples: 2-10 1,3,6,9,12 Range: 0–15.	0–31	0–31
`temporal-diversity`	Shows if temporal diversity has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries.		disabled
`very-high-throughput-enable`	Shows if very-high-throughput (820.11ac) features are enabled or disabled.		enabled

Parameter	Description	Range	Default
`vht-supported-mcs-map <supported-mcs-set>`	Comma-separated list of max supported MCS for spatial streams 1 through 4. Valid values for max MCS are 7, 8, 9, and - (if spatial stream is not supported). Max MCS of a spatial stream cannot be higher than the MCS of the previous stream. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx.		9,9,9,9
`vht-txbf-explicit-enable`	Enable or Disable use of VHT Explicit Transmit Beamforming.		enabled

Guidelines

The mesh HT profile defines settings unique to 802.11n-capable, high-throughput APs. If none of the APs in your mesh deployment are 802.11n-capable APs, you do not need to configure a HT SSID profile.

If you modify a currently provisioned and running high-throughput SSID profile, your changes take effect immediately. You do not reboot the Mobility Master or the AP.

Example

The following command configures a mesh HT SSID profile named “HT1” and sets some non-default settings for MPDU aggregation:

```
(host) [mynode] (config) #ap mesh-ht-ssid-profile HT1
(host) [mynode] (Mesh High-throughput SSID profile "HT1") #max-rx-a-mpdu-size 32767
(host) [mynode] (Mesh High-throughput SSID profile "HT1") #max-tx-a-mpdu-size 32767
(host) [mynode] (Mesh High-throughput SSID profile "HT1") #min-mpdu-start-spacing .25
```

Related Commands

Command	Description
show ap mesh-ht-ssid-profile	View a complete list of mesh HT SSID profiles and their status.
show ap mesh-ht-ssid-profile	View the settings of a specific mesh radio profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap mesh-radio-profile

```
ap mesh-radio-profile {default | <profile-name>
   a-tx rates [6 | 9 | 12 | 18 | 24 | 36 | 48 | 54]
   allowed-vlans <vlan-list>
   children <children>
   clone {default | <source>}
   eapol-rate-opt
   g-tx rates [1| 2 | 5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54]
   heartbeat-threshold <heartbeat-threshold>
   hop-count <hop-count>
   link-threshold <link-threshold>
   max-retries <max-retries>
   mesh-ht-ssid-profile {default | <profile-name>}
   mesh-mcast-opt
   mesh-survivability
   metric-algorithm {best-link-rssi | distributed-tree-rssi}
   mpv <mpv>
   no ...
   reselection-mode {reselect-anytime | reselect-never | startup-subthreshold | subthreshold-
   only}
   rts-threshold <rts-threshold>
```

Description

This command configures a mesh radio profile used by mesh nodes.

Syntax

Parameter	Description	Range	Default
`ap mesh-radio-profile <profile>`	Configures a Mesh Radio profile. Give a name to this instance of the profile. The name must be 1–63 characters long.	—	default
`a-tx rates`	Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	

Parameter	Description	Range	Default
`allowed-vlans`	Specifies a list of VLAN IDs that can be used by a mesh link on APs associated with this mesh radio profile		
`<vlan-list>`	A comma-separated list of VLAN IDs. You can also specify a range of VLAN IDs using a dash (for example, 1–4095)		
`children <children>`	Indicates the maximum number of children a mesh node can accept.	1–64	64
`clone <source>`	Name of an existing mesh radio profile from which parameter values are copied.		default
`eapol-rate-opt`	Use a more conservative rate for more reliable delivery of EAPOL frames.		disabled
`g-tx rates`	Indicates the transmit rates for the 802.11b or 802.11g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54	
`heartbeat-threshold <heartbeat-threshold>`	Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes.	1–255	30

Parameter	Description	Range	Default
`hop-count <hop-count>`	Indicates the maximum hop count from the mesh portal.	1–32	8
`link-threshold <link-threshold>`	Indicates the minimal RSSI value. If the RSSI value is below this threshold, the link may be considered a sub-threshold link. A sub-threshold link is a link whose average RSSI value falls below the configured threshold. If this occurs, the mesh node may try to find a better link on the same channel and cluster (only neighbors on the same channel are considered). The supported threshold is hardware dependent, with a practical range of 10–90.	hardware-dependent	12
`max-retries <max-retries>`	Maximum number of times a mesh node can re-send a packet.	0–15	4
`mesh-ht-ssid-profile <profile-name>`	HT SSID Profile for the mesh feature.		default

Parameter	Description	Range	Default
`mesh-mcast-opt`	Enables or disables scanning of all active stations currently associated to a mesh point to select the lowest transmission rate based on the slowest connected mesh child. When enabled, this setting dynamically adjusts the multicast rate to that of the slowest connected mesh child. Multicast frames are not sent if there are no mesh children. Best practices are to use the default value.		enabled
`mesh-survivability`	Allow mesh points and portals to become active even if the Mobility Master cannot be reached by bridging LAN traffic. This is a beta feature that is disabled by default; it should not be enabled unless you are instructed to do so by Aruba technical suppport.	—	distributed-tree-rssi
`metric-algorithm`	Specifies the algorithm used by a mesh node to select its parent. Best practices are to use the default value distributed-tree-rssi.	—	distributed-tree-rssi

Parameter	Description	Range	Default
`best-link-rssi`	Selects the parent with the strongest RSSI, regardless of the number of children a potential parent has.	—	—
`distributed-tree-rssi`	Selects the parent based on link-RSSI and node cost based on the number of children. This option evenly distributes the mesh points over high quality uplinks. Low quality uplinks are selected as a last resort.	—	—
`mpv <mpv>`	This parameter is experimental and reserved for future use.	0–4094	0 (disabled)
`no`	Negates any configured parameter.	—	—
`reselection-mode`	Specifies the method used to find a better mesh link. Best practices are to use the default value startup-subthreshold.	(see below)	startup-sub threshold

Parameter	Description	Range	Default
`reselect-anytime`	Mesh points using the **reselect-anytime** reselection mode perform a single topology readjustment scan within 9 minutes of startup and 4 minutes after a link is formed. If no better parent is found, the mesh point returns to its original parent. This initial scan evaluates more distant mesh points before closer mesh points, and incurs a dropout of 5-8 seconds for each mesh point. After the initial startup scan is completed, connected mesh nodes evaluate mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal.	—	—
`reselect-never`	Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal.	—	—

Parameter	Description	Range	Default
`startup-subthreshold`	Mesh points using the **startup-subthreshold** reselection mode perform a single topology readjustment scan within 9 minutes of startup and 4 minutes after a link is formed. If no better parent is found, the mesh point returns to its original parent. This initial startup scan evaluates more distant mesh points before closer mesh points, and incurs a dropout of 5–8 seconds for each mesh point. After that time, each mesh node evaluates alternative links if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). Best practices are to use the default **startup-subthreshold** value.	—	—

Parameter	Description	Range	Default
	If a mesh point using the **startup-subthreshold** mode reselects a more distant parent because its original, closer parent falls below the acceptable threshold, then as long as that mesh point is connected to that more distant parent, it will seek to reselect a parent at the earlier distance (or less) with good link quality. For example, if a mesh point disconnects from a mesh parent 2 hops away and subsequently reconnects to a mesh parent 3 hops away, then the mesh point will continue to seek a connection to a mesh parent with both an acceptable link quality and a distance of two hops or less, even if the more distant parent also has an acceptable link quality.		
`subthreshold-only`	Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link.	—	—

Parameter	Description	Range	Default
`rts-threshold <rts-threshold>`	Defines the packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue RTS and wait for other mesh nodes to respond with CTS to begin transmission. This helps prevent mid-air collisions.	256–2346	2333 bytes

Usage Guidelines

Mesh radio profiles are specific to mesh nodes (APs configured for mesh) and determine the RF or channel used by mesh nodes to establish mesh links and the path to the mesh portal. You can configure multiple radio profiles; however, you select and deploy only one radio profile per mesh cluster.

Radio profiles, including the “default” profile, are not active until you provision your APs for mesh. If you modify a currently provisioned and running radio profile, your changes take place immediately. You do not reboot the Mobility Master or the AP.

Example

The following command creates a mesh radio profile named “radio2” and associates a mesh HT profile named meshHT1:

```
(host) [mynode] (config) #ap mesh-radio-profile radio2
(host) [mynode] (Mesh Radio profile "radio2") #mesh-ht-ssid-profile meshHT1
```

Related Commands

Command	Description
show ap mesh-radio-profile	To view the settings of a specific mesh radio profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap multizone-profile

```
ap multizone-profile <profile-name>
   clone <source>
   datazone <zone>
   controller-ip <ipv>
   num-nodes <num_nodes>
   num-vaps <num_nodes>
   multizone-enable
   no
   primaryzone
```

Description

MultiZone feature allows AP to terminate to multiple managed devices that reside in different zones. A zone is a collection of managed devices under a single administration domain. The zone can have a single managed device or a cluster. This command allows you to create an AP multizone profile, set the data zone index, and controller-ip.

Syntax

Parameter	Description
`<profile-name>`	Name of the profile.
`clone`	Copy data from one AP multizone profile to another.
`datazone`	Datazone zone Index [1 - 4].
`controller-ip <ip>`	Managed device to be configured on one of the datazones.
`num-nodes <num_nodes>`	(Optional) The maximum number of managed devices for the zone should be set between 1 - 11, as the primary zone must have at least one managed device. Default value is 1.
`num-vaps <num_vaps>`	(Optional) The maximum number of essids for the zone should be set between 1 - 16. Default value is 3.
`multizone-enable`	If enabled, AP enters multizone mode. Default value is disabled.
`no`	Delete command.
`primaryzone`	This parameter is used to configure the primary zone.
`controller-ip <ip>`	Managed device to be configured on one of the primary zones.
`num-nodes <num_nodes>`	(Optional) The maximum number of managed devices for the zone should be set between 1 - 11, as the primary zone must have at least one managed device. Default value is 1.
`num-vaps <num_vaps>`	(Optional) The maximum number of essids for the zone should be set between 1 - 16. Default value is 3.

Example

The following command enables AP multizone.

```
(host) [mm] (config) #ap multizone-profile <default> multizone-enable
```

Command History

Release	Modification
ArubaOS 8.1.0.0	The **primaryzone** parameter was introduced.
ArubaOS 8.0.1.0	The **num-nodes** sub-parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master

ap provisioning-profile

```
ap provisioning-profile <profile>
   ap-poe-power-optimization
   apdot1x-passwd
   apdot1x-username
   cellular_nw_preference 3g-only|4g-only|advanced|auto
   clone
   link-priority-cellular
   link-priority-ethernet
   master clear|set
   no
   pppoe-passwd
   pppoe-service-name
   pppoe-user
   remote-ap
   uplink-vlan <uplink-vlan>
   usb-csr
   usb-dev
   usb-dial
   usb-init
   usb-modeswitch -v <default_vendor> -p <default_product> -V <target_vendor> -P <target_
   product> -M <message_content>
   usb-passwd
   usb-power-mode auto| enable|disable
   usb-tty
   usb-tty-control
   usb-type
   usb-user
```

Description

This command defines a provisioning profile for an AP or group of APs.

Syntax

Parameter	Description	Default	Range
`ap-poe-power-optimization`	Enabling optimization minimizes the POE draw of the AP. Enabling optimization may disable some parts of the AP. Disabling ensures all features are enabled. ■ **enabled**: AP operates in normal mode. ■ **disabled**: USB and Ethernet port (eth1) are shut down on AP.	disabled	—
`apdot1x-passwd`	Password of the AP to authenticate to 802.1X using PEAP	—	—
`apdot1x-username`	Username of the AP to authenticate to 802.1X using PEAP	—	—

Parameter	Description	Default	Range
`cellular_nw_preference g-only|4g-only| advanced|auto`	The cellular network preference setting allows you to select how the modem should operate. ■ auto (default): In this mode, modem firmware will control the cellular network service selection; so the cellular network service failover and fallback is not interrupted by the remote AP (RAP). ■ 3g_only: Locks the modem to operate only in 3G. ■ 4g_only: Locks the modem to operate only in 4G. advanced: The RAP controls the cellular network service selection based on an Received Signal Strength Indication (RSSI) threshold-based approach. Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network. The RAP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the RAP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The RAP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode. The RAP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the RAP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The RAP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.	auto	—
`clone <source>`	Clone an existing ap provisioning profile.	—	—
`link-priority-cellular <link-priority-cellular>`	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary controller link.	0-255	0
`link-priority-ethernet <link-priority-ethernet>`	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.	0-255	0
`master`	Change the FQDN or IP address for the Mobility Master.	—	—
`set <masterstr>`	Specify the or IP address or FQDN for the Mobility Master.	—	—
`clear`	Clear the definition for the Mobility Master in this profile.	—	—
`no`	Negates any configured parameter.	—	—
`pppoe-passwd`	Point-to-Point Protocol over Ethernet (PPPoE) password for the AP.	—	—

Parameter	Description	Default	Range
`pppoe-service-name`	PPPoE service name for the AP.	—	—
`pppoe-user`	PPPoE username for the AP.	—	—
`remote-ap`	Specifies that the profile is to be associated with a remote AP using certificates.	—	—
`reset-bootinfo`	Restores factory default provisioning parameters to the specified AP. **NOTE:** This parameter can only be used on the Mobility Master.	—	—
`uplink-vlan <uplink-vlan>`	If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature. **NOTE:** If an AP is provisioned with an uplink VLAN, it must be connected to a trunk mode port or the AP's frames will be dropped.	0 (disabled) to 4095	0
`usb-dev`	The USB device identifier.	—	—
`usb-dial`	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.	—	—
`usb-init`	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.	—	—
`usb-modeswitch -v <default_vendor> -p <default_product> -V <target_vendor> -P <target_product> -M <message_content>`	USB cellular devices on remote APs typically register as modems, but may occasionally register as a mass-storage device. If a remote AP cannot recognize its USB cellular modem, use the usb-modeswitch command to specify the parameters for the hardware model of the USB cellular data-card. **NOTE:** You must enclose the entire modeswitch parameter string in quotation marks.	—	—
`usb-passwd`	A PPP password, if provided by the cellular service provider.	—	—
`usb-power-mode auto|enable|disable`	Set the USB power mode to control the power to the USB port.	—	—
`usb-tty`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.	—	—
`usb-tty-control`	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.	—	—

Parameter	Description	Default	Range
usb-type	Specify the USB driver type. ■ **acm**: Use ACM driver ■ **airprime**: Use Airprime driver ■ **ether**: Use CDC Ether driver for direct IP 4G device ■ **hso**: Use HSO driver for newer Option ■ **huawei-cdc**: Use Huawei driver for 4G device ■ **netgear-gobi**: Use Gobi driver for Netgear 340U/341U 4G device ■ **none**: Disable 3G or 2G network on USB ■ **option**: Use Option driver ■ **option-novatel-u620**: Use Option driver for Novatel U620L 4G device ■ **pantech-3g**: Same as "pantech-uml290" - to support upgrade ■ **pantech-auto**: Use Pantech driver for Automatic modem mode ■ **pantech-uml290**: Use Pantech USB driver for UML290 device ■ **ptumlusbnet**: Use Pantech USB driver for 4G device ■ **rndis**: Use a RNDIS driver for a 4G device ■ **rndis-pantech-uml295:** Use RNDIS driver for Pantech UML 295 4G device ■ **sierra-evdo**: Use EVDO Sierra Wireless driver ■ **sierra-gsm**: Use GSM Sierra Wireless driver ■ **sierrausbnet**:Use SIERRA Direct IP driver for 4G device ■ **storage**: Use USB flash as storage device for storing RAP certificates	—	none
usb-user	The PPP username provided by the cellular service provider.	—	—

Usage Guidelines

The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group via the command **ap-group <group> provisioning-profile <profile>**.

In order to enable cellular uplink for a remote AP (RAP), the RAP must have the device driver for the USB data card and the correct configuration parameters. ArubaOS includes device drivers for the most common hardware types, but you can use the **usb** commands in this profile to configure a RAP to recognize and use an unknown USB modem type.

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Example

The following commands create a provisioning profile named **profile_branch**, in which the cellular link is the primary uplink because it has a higher priority than the Ethernet link:

```
(host) [mynode] (config) #ap provision-profile profile_branch
   link-priority-cellular 2
```

```
link-priority-ethernet 1
usb-type acm
usb-modeswitch "-v 0x106c -p 0x3b06 -V 0x106c -P 0x3717 -M
5534243b82e238c240000008000008ff020000000000000000000000000000000"
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

ap packet-capture

```
ap packet-capture
   clear <ap-name|ip-addr|ip6-addr>] <pcap-id> radio <0|1>
   close-port <port>
   interactive <ap-name|ip-addr|ip6-addr> <filter-spec> <target-ip> <target-port> radio <0|1>
channel <channel>
   open-port <port>
   pause <ap-name|ip-addr|ip6-addr> <pcap-id> radio <0|1>
   raw-start [<ap-name|ip-addr|ip6-addr>] <target-ip> <target-port> <format> radio <0|1>
channel <channel> maxlen <maxlen>
   resume [<ap-name|ip-addr|ip6-addr>] <pcap-id> radio <0|1>
   stop <ap-name|ip-addr|ip6-addr>  <pcap-id> radio <0|1>
   wired-start <ap-name|ip-addr|ip6-addr> <target-ip> <target-port>
   wired-stop <ap-name|ip-addr|ip6-addr> <target-ip> <target-port>
```

Description

These commands manage WiFi packet capture (PCAP) on Aruba APs. The WiFi packets are encapsulated in a UDP header and sent to a client running a packet analyzer like Wildpacket's Airopeek, Omnipeek, or Wireshark.

Syntax

Parameter	Description
`clear`	Clears the packet capture session.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IP address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.
`<pcap-id>`	ID of the PCAP session.
`radio <0-1>`	ID of the radio sending the packets
`close-port <port>`	(CPsec Campus APs and Remote APs only) Close or disallow access to this UDP port on the AP for packet capture purposes.
`interactive`	Start an interactive packet capture session between an AP and a client running a packet analyzer.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IP address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.
`<filter-spec>`	Packet Capture filter specification. See **Usage Guidelines** for details.
`<target-ip>`	IP address of the client running the packet analyzer.
`<target-port>`	UDP port number on the client station where the captured packets are sent.
`radio <0-1>`	ID of the radio sending the packets

Parameter	Description
channel <channel>	(Optional or Applicable only in AM mode) Number of a radio channel to tune into to capture packets.
open-port <port>	(CPsec Campus APs and Remote APs only) Enable or allow access to this UDP port on the AP for packet capture purposes.
pause	Pause a packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.
radio <0-1>	ID of the radio sending the packets
raw-start	Stream packets from the driver to a client running the packet analyzer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.
radio <0-1>	ID of the radio sending the packets
channel <channel>	(Optional or Applicable only in AM mode) Number of a radio channel to tune into to capture packets.
maxlen <maxlen>	(Optional) Limit the length of 802.11 frames to include in the capture to a specified maximum.
resume	Resume a packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.
radio <0-1>	ID of the radio sending the packets.
stop	Stop a packet capture session.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.

Parameter	Description
ip6-addr <ip6-addr>	IPv6 address of the AP.
<pcap-id>	ID of the PCAP session.
radio <0-1>	ID of the radio sending the packets
wired-start	Start a wired ethernet packet stream to an external viewer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.
wired-stop	Halt a wired ethernet packet stream currently being sent to an external viewer.
ap-name <ap-name>	Name of the AP.
ip-addr <ip-addr>	IP address of the AP.
ip6-addr <ip6-addr>	IPv6 address of the AP.
<target-ip>	IP address of the client running the packet analyzer.
<target-port>	UDP port number on the client station where the captured packets are sent.

Usage Guidelines

These commands direct an AP to send Wi-Fi packet captures to a client packet analyzer utility such as Airmagnet, Wireshark and so on, on a remote client.

Before using these commands, you need to start the packet analyzer utility on the client and open a capture window for the port from which you are capturing packets. The packet analyzer cannot be used to control the flow or type of packets sent from APs.

The packet analyzer processes all packets. However, you can apply display filters on the capture window to control the number and type of packets being displayed. In the capture window, the time stamp displayed corresponds to the time that the packet is received by the client and is not synchronized with the time on the AP.

Filter specification (used in ap packet-capture interactive) supports the following:

- type (beacon/rts/cts/data/ack/ctrl/mgmt/all)
- sta (mac address)
- bss (mac address)
- da (mac address)
- sa (mac address)
- dir (tods, fromds)
- retry (1, 0)
- frag (1, 0)
- wep (1, 0)

Filter spec examples:

(type eq beacon) or ((sta eq 000000010203) and (dir eq tods))

(type == data) && ((sta = 000000010203) || (sta == 000000010203))

(type != beacon)

(wep nq 1)

(type eq all)

Examples

The following command starts a raw packet capture session for the AP **ly115** on radio **0**, and sends the packets to the client at **10.64.102.4** on port **5000**.

```
(host) [mynode] (config) #ap packet-capture raw-start ap-name ly115 10.64.102.4  5000 0 radio
0
Packet capture has started for pcap-id:1
```

The following commands start an interactive packet capture session for the AP **ap1**.

```
#ap packet-capture open-port 5555
#ap packet-capture interactive ap-name ap1 "type eq all" 192.168.0.3 5555 radio 0
```

The output of the command in the example below displays packet capture session statistics for the AP **ap1**. In this example, the output has been divided into multiple sections to better fit on the pages of this document. In the actual CLI, it will appear in a single, long table.

```
#show ap packet-capture status ap-name ap1

Packet Capture Sessions at ap1, IP 10.3.44.167
----------------------------------------------
pcap-id  filter       type         intf               channel max-pkts
-------  ------       ----         ----               ------- --------
1        type eq all  interactive  6c:f3:7f:ba:65:70  153     0


max-pkt-size  num-pkts  status       url target       Radio ID
------------  --------  ------       ------           ------
65536         3759      in-progress  192.168.0.3/5555 0
```

Related Commands

To view the status of outstanding packet capture sessions, use show ap packet capture.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Works in Access Point, AM, and Spectrum Monitor modes on all AP models in enable mode.

ap process restart

```
ap process restart
   {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>}
```

Description

Use this command to restart the AP process of a particular AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IPv4 address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.

Usage Guidelines

This command should only be used under the guidance of Aruba technical support.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Enable mode on Mobility Master or managed devices.

ap provisioning-profile

```
ap provisioning-profile {default | <profile-name>}
   ap-lldp-pse-detect {disabled | enabled}
   ap-poe-power-optimization
   ap2xx-prestandard-poe-detection
   apdot1x-factory-cert
   apdot1x-passwd <apdot1x-passwd>
   apdot1x-tls
   apdot1x-username <apdot1x-username>
   cellular_nw_preference {3g-only | 4g-only | advanced | auto}
   clone {default | <source>}
   link-priority-cellular <link-priority-cellular>
   link-priority-ethernet <link-priority-ethernet>
   master {clear | set <masterstr>}
   no
   pppoe-passwd <pppoe-passwd>
   pppoe-service-name <pppoe-service-name>
   pppoe-user <pppoe-user>
   remote-ap
   uplink-vlan <uplink-vlan>
   usb-csr
   usb-dev <usb-dev>
   usb-dial <usb-dial>
   usb-init <usb-init>
   usb-modeswitch <usb-modeswitch [-v | -p | -V | -P | -M]>
   usb-passwd <usb-passwd>
   usb-power-mode {auto | enable | disable}
   usb-tty <usb-tty>
   usb-tty-control <usb-tty-control>
   usb-type
   usb-user <usb-user>
```

Description

This command defines a provisioning profile for an AP or group of APs.

Syntax

Parameter	Description	Range	Default
`ap provisioning-profile <profile-name>`	Configures a provisioning profile for an AP or a group of APs. Give a name for the profile.		default
`ap-lldp-pse-detect`	Enabling causes the AP to detect the POE type via LLDP POE TLV. Use one of the following parameters: ■ **enabled**: The AP uses PSE TYPE in the POE TLV to detect the PSE type. ■ **disabled**: The AP detects the POE using the HW classification.		

Parameter	Description	Range	Default
ap-poe-power-optimization	Enabling optimization minimizes the POE draw of the AP. Enabling optimization may disable some parts of the AP. Disabling optimization ensures all features are enabled. Use one of the following parameters: ■ **enabled:** USB and Ethernet port (eth1) are shut down on AP. ■ **disabled:** AP operates in normal mode.		disabled
ap2xx-prestandard-poe-detection	Configures the prestandard PoE detection on 200 Series APs. The POE+ pre-standard detection is only available on 200 Series APs. It consists of a basic voltage comparator. If the line voltage is equal to or greater than 51 V, the PSE is assumed to be 802.3at compatible.	—	—
apdot1x-factory-cert	Enable AP to use factory certificates when doing 802.1x EAP-TLS.Custom cert available.		
apdot1x-passwd	Sets the password of the AP to authenticate to 802.1X using PEAP.	—	—
apdot1x-tls	Enable AP to perform 802.1x authentication using EAP-TLS.		
apdot1x-username	Sets the username of the AP to authenticate to 802.1X using PEAP.	—	—

Parameter	Description	Range	Default
`cellular_nw_preference {3g-only | 4g-only | advanced | auto}`	The cellular network preference setting allows you to select how the modem should operate. ■ **auto (default)** ■ **3g_only:** Locks the modem to operate only in 3G. ■ **4g_only:** Locks the modem to operate only in 4G. ■ **advanced:** The Remote AP controls the cellular network service selection based on an Received Signal Strength Indication (RSSI) threshold-based approach. Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network. The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode. The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.	—	auto
`clone <source>`	Clones an existing AP provisioning profile.	—	default

Parameter	Description	Range	Default
link-priority-cellular <link-priority-cellular>	Sets the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary controller link.	0–255	0
link-priority-ethernet <link-priority-ethernet>	Sets the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.		
master	Changes the FQDN or IP address for the Mobility Master.	—	—
set <masterstr>	Specifies the IP address or FQDN for the Mobility Master.	—	—
clear	Clear the definition for the Mobility Master in this profile.	—	—
no	Negates any configured parameter.	—	—
pppoe-passwd <pppoe-passwd>	PPPoE password for the AP.	—	—
pppoe-servicename <pppoe-service-name>	PPPoE service name for the AP.	—	—
pppoe-user <pppoe-user>	PPPoE username for the AP.	—	—
remote-ap	Specifies that the profile is to be associated with a remote AP using certificates.	—	—
uplink-vlan <uplink-vlan>	If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature. **NOTE:** If an AP is provisioned with an uplink VLAN, it must be connected to a trunk mode port or the frames of the AP will be dropped.	0–4095	0 (disabled)
usb-csr	Configures the USB storage for CSR and private Key file		

Parameter	Description	Range	Default
`usb-dev <usb-dev>`	Configures the USB device identifier.	—	—
`usb-dial <usb-dial>`	Configures the dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.	—	—
`usb-init <usb-init>`	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.	—	—

`usb-modeswitch <usb-modeswitch>`
`-v for default_vendor`
`-p for default_product`
`-V for target_vendor`
`-P for target_product`
`-M for message_content`
	USB cellular devices on remote APs typically register as modems, but may occasionally register as a mass-storage device. If a remote AP cannot recognize its USB cellular modem, use the usb-modeswitch command to specify the parameters for the hardware model of the USB cellular data-card.
	NOTE: You must enclose the entire modeswitch parameter string in quotation marks.
		—	—

`usb-passwd <usb-passwd>`	A PPP password, if provided by the cellular service provider.	—	—
`usb-power-mode` `{auto| enable|disable}`	Set the USB power mode to control the power to the USB port.	—	—
`usb-tty <usb-tty>`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.	—	—
`usb-tty-control` `<usb-tty-control>`	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.	—	—

Parameter	Description	Range	Default
`usb-type`	Specify the USB driver type. **acm:** Use ACM driver **airprime:** Use Airprime driver **ether:** Use CDC Ether driver for direct IP 4G device **hso:** Use HSO driver for newer Option **huawei-cdc:** Use Huawei driver for 4G device ■ **lnetgear-gobi:** Use Gobi driver for Netgear 340U or 341U 4G device ■ **none:** Disable 3G or 2G network on USB ■ **option:** Use Option driver ■ **option-novatel-u620:** Use Option driver for Novatel U620L 4G device ■ **pantech-3g:** Same as "pantech-uml290" - to support upgrade ■ **pantech-auto:** Use Pantech driver for Automatic modem mode ■ **pantech-uml290:** Use Pantech USB driver for UML290 device ■ **ptumlusbnet:** Use Pantech USB driver for 4G device ■ **rndis:** Use a RNDIS driver for a 4G device ■ **rndis-1800:** Same as RNDIS - to use for L800 4G device ■ **rndis-pantech-uml295:** Use RNDIS driver for Pantech UML 295 4G device ■ **sierra-evdo:** Use EVDO Sierra Wireless driver ■ **sierra-gsm:** Use GSM Sierra Wireless driver ■ **sierrausbnet:** Use SIERRA Direct IP driver for 4G device ■ **storage:** Use USB flash as storage device for storing Remote AP certificates	—	none
`usb-user <usb-user>`	The PPP username provided by the cellular service provider.	—	—

Usage Guidelines

The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group by using the **ap-group <group> provisioning-profile <profile>** command.
In order to enable cellular uplink for a Remote AP it must have the device driver for the USB data card and the correct configuration parameters. ArubaOS includes device drivers for the most common hardware types, but you can use the usb commands in this profile to configure a Remote AP to recognize and use an unknown USB modem type.

Examples

The following commands create a provisioning profile named profile_branch, in which the cellular link is the primary uplink because it has a higher priority than the Ethernet link:

```
(host) [mynode] (config) #ap provision-profile profile_branch
```

```
(host) [mynode] (Provisioning profile "profile_branch") #link-priority-cellular 2
(host) [mynode] (Provisioning profile "profile_branch") #link-priority-ethernet 1
(host) [mynode] (Provisioning profile "profile_branch") #usb-type acm
(host) [mynode] (Provisioning profile "profile_branch") #usb-modeswitch "-v 0x106c -p 0x3b06 -
V 0x106c -P 0x3717 -M 5534243b82e238c240000008000008ff020000000000000000000000000000000"
```

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **apdot1x-factory-cert** , **apdot1x-tls**, and **ap-lldp-pse-detect** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap redeploy controller-less

```
ap redeploy controller-less
   all
   ap-group <ap-group>
   ap-name <ap-name>
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
   wired-mac <wired-mac>
```

Description

This command sets the AP preference role to controller-less, allowing the AP to bypass controller discovery and immediately initiate Instant discovery during AP image upgrade. APs with the controller-less preference role are deployed as controller-less APs.

Syntax

Parameter	Description
`all`	Deploys all APs as controller-less APs.
`ap-group <ap-group>`	Deploys all APs in the specified AP group as controller-less APs.
`ap-name <ap-name>`	Deploys a specific AP as a controller-less AP.
`ip-addr <ip-addr>`	Deploys the AP with a specific IP address as a controller-less AP.
`ip6-addr <ip6-addr>`	Deploys the AP with a specific IPv6 address as a controller-less AP.
`wired-mac <wired-mac>`	Deploys the AP with a specific MAC address as a controller-less AP.

Example

The following command deploys all APs as controller-less APs:

```
(host) [mynode] #ap redeploy controller-less all
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on master Mobility Master

ap regulatory activate

```
ap regulatory activate <filename>
```

Description

This command activates the specified regulatory certificate

Syntax

Parameter	Description
<filename>	Name of the regulatory certificate to be activated.

Usage Guidelines

Use this command to activate a new regulatory certificate to your configuration.

Related Commands

To view the current regulatory certificate, use the **show ap regulatory** command.

To view the supported channels, use the **show ap allowed-channels country-code** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

ap regulatory-domain-profile

```
ap regulatory-domain-profile {default | <profile-name>
   clone {default | <source>}
   country-code <country-code>
   no
   valid-11a-40mhz-channel-pair <valid-11a-40mhz-channel-pair>
   valid-11a-80mhz-channel-group <valid-11a-80mhz-channel-group>
   valid-11a-160mhz-channel-group <valid-11a-160mhz-channel-group>
   valid-11a-channel <valid-11a-channel>
   valid-11g-40mhz-channel-pair <valid-11g-40mhz-channel-pair>
   valid-11g-channel <valid-11g-channel>
```

Description

This command configures an AP regulatory domain profile.

Syntax

Parameter	Description	Default
`ap regulatory-domain-profile <profile>`	Configures a Regulatory Domain profile. Give a name to this instance of the profile. The name must be 1–63 characters long.	default
`clone <source>`	Name of an existing regulatory domain profile from which parameter values are copied.	default
`country-code <country-code>`	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.	Country code configured on the Mobility Master during initial setup
`no`	Negates any configured parameter.	—

Parameter	Description	Default
`valid-11a-40mhz-channel-pair <valid-11a-40mhz-channel-pair>`	Specify a channel pair valid for 40 MHz operation in the 802.11a frequency band for the specified regulatory domain. The two channels must be separated by a dash. Example: 36–40 44–48 52–56	Country code determines supported channel pairs **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11a-80mhz-channel-group <valid-11a-80mhz-channel-group>`	This parameter defines which 80 MHz channels on the *a* band are available for assignment by ARM and for Mobility Master to randomly assign if the user has not specified a channel. The channel numbers below correspond to channel center frequency. Example: 36-48 52-64	Country code determines supported channels. **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11a-160mhz-channel-group <valid-11a-160mhz-channel-group>`	Specifies a valid 802.11a channel group for 160 MHz channel on the *a* band. The channel numbers below correspond to channel center frequency. Example: 36-64	Country code determines supported channels. **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11a-channel <valid-11a-channel>`	Enter a single 802.11a channel number for 20 MHz operation within the specified regulatory domain.	
`valid-11g-40mhz-channel-pair <valid-11g-40mhz-channel-pair>`	Specify a channel pair valid for 40 MHz operation in the 802.11g frequency band for the specified regulatory domain. The two channels must be separated by a dash. Example: 36–48	country code determines supported channel pairs **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11g-channel <valid-11g-channel>`	Enter a single 802.11g channel number for 20 MHz operation within the specified regulatory domain.	country code determines supported channels **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.

Usage Guidelines

This profile configures the country code and valid channels for operation of APs. The list of valid channels only affects the channels that may be selected by ARM or by the Mobility Master when no channel is configured. Channels that are specifically configured in the AP radio settings profile (see rf dot11a-radio-profile or rf dot11g-radio-profile) must be valid for the country and the AP model.

A Mobility Master shipped to certain countries, such as the U.S. and Israel, cannot terminate APs with regulatory domain profiles that specify different country codes from the Mobility Master. For example, if a controller is designated for the U.S., then only a regulatory domain profile with the "US" country code is valid; setting APs to a regulatory domain profile with a different country code will result in the radios not coming up. For controllers in other countries, you can mix regulatory domain profiles on the same controller; for example, one controller can support APs in Japan, Taiwan, China, and Singapore.

In order for an AP to boot correctly, the country code configured in the AP regulatory domain profile must match the country code of the LMS. If none of the channels supported by the AP have received regulatory approval by the country whose country code you selected, the AP will revert to Air Monitor mode.

This command is used to override available channels in the list of channels allowed for use in that country. If you do not add any channels to the AP regulatory domain profile, it means the AP can use any of the available channels. If you want to disable use of an entire band, best practices is to use the **rf-dot11a-radio-profile** or **rf-dot11g-radio-profile** commands to disable the radio. Alternatively, if you want to disable a specific bandwidth, use the **Max Channel Bandwidth** and **Min Channel Bandwidth** settings in the radio profiles, and AirMatch will enforce this setting.

Examples

The following command configures the regulatory domain profile for APs in Japan:

```
(host) [mynode](config) #ap regulatory-domain-profile rd1
(host) [mynode] (Regulatory Domain profile "rd1") #country-code JP
```

The following command configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 36 and 40, is allowed for 40 MHz mode of operation on the 5 GHz frequency band:

```
(host)[mynode] (config) #ap regulatory-domain-profile usa1
(host) [mynode] (Regulatory Domain profile "usa1") #country-code US
(host) [mynode] (Regulatory Domain profile "usa1") #valid-11a-40mhz-channel-pair 36-40
```

The following command configures a regulatory domain profile for APs in the United States and specifies that the channel pair of 5 and 1, is allowed for 40 MHz mode of operation on the 2.4 GHz frequency band:

```
(host) [mynode](config) #ap regulatory-domain-profile usa1
host) [mynode] (Regulatory Domain profile "usa1") #country-code US
host) [mynode] (Regulatory Domain profile "usa1") #valid-11g-40mhz-channel-pair 1-5
```

Related Commands

Command	Description
show ap allowed-channels	To view the supported channels.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master

ap regulatory reset

```
ap regulatory-domain-profile <profile>
   clone <profile>
   country-code <code>
   no ...
   valid-11a-40mhz-channel-pair <valid-11a-40mhz-channel-pair>
   valid-11a-80mhz-channel-group <valid-11a-80mhz-channel-group>
   valid-11a-channel <num>
   valid-11g-40mhz-channel-pair <valid-11g-40mhz-channel-pair>
   valid-11g-channel <num>
```

Description

This command returns the Mobility Master to the factory default Regulatory-Cert.

Syntax

Parameter	Description	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—
`clone`	Name of an existing regulatory domain profile from which parameter values are copied.	—
`country-code`	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.	Country code configured on the Mobility Master during initial setup.
`no`	Negates any configured parameter.	—
`valid-11a-40mhz-channel-pair`	Specify a channel pair valid for 40 MHz operation in the 802.11a frequency band for the specified regulatory domain. The two channels must be separated by a dash. Example: 36-40 44-48 52-56	Country code determines supported channel pairs **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
valid-11a-80mhz-channel-group	This parameter defines which 80 MHz channels on the “a” band are available for assignment by ARM and for Mobility Master to randomly assign if the user has not specified a channel. The channel numbers below correspond to channel center frequency.	—

Parameter	Description	Default
`valid-11a-channel`	Enter a single 802.11a channel number for 20 MHz operation within the specified regulatory domain.	Country code determines supported channels **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11g-40mhz-channel-pair`	Specify a channel pair valid for 40 MHz operation in the 802.11g frequency band for the specified regulatory domain. The two channels must be separated by a dash. Example: 1-5 2-6 7-11	Country code determines supported channel pairs **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.
`valid-11g-channel`	Enter a single 802.11g channel number for 20 MHz operation within the specified regulatory domain.	Country code determines supported channels **NOTE:** Changing the country code causes the valid channel lists to be reset to the defaults for the country.

Usage Guidelines

Use this command to return the Mobility Master to the factory default regulatory information.

Related Commands

To view the current Regulatory-Cert, use the **show ap regulatory** command.

To view the supported channels, use the **show ap allowed-channels country-code** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

ap spectrum clear-webui-view-settings

```
ap spectrum clear-webui-view-settings
```

Description

Clear a saved spectrum dashboard view.

Syntax

No parameters

Usage Guidelines

Saved spectrum view preferences may not be backwards compatible with the spectrum analysis dashboard in earlier versions of ArubaOS. If you downgrade to an earlier version of ArubaOS and your client is unable to load a saved spectrum view in the spectrum dashboard, access the CLI in enable mode and issue this command to delete the saved spectrum views and display default view settings in the spectrum dashboard.

Example

The following command removes the WEBUI spectrum view settings file of an user:

```
(host) [mynode] ##ap spectrum clear-webui-view-settings
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	RF Protect license.	Enable mode on Mobility Master.

ap spectrum local-override

```
no
override ap-name <ap-name> spectrum-band <2.4ghz | 5ghz>
```

Description

Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.

Syntax

Parameter	Description	Range	Default
`no`	Negates any previous AP spectrum local-override configuration	—	—
`override ap-name <ap-name>`	Specifies the name of an AP whose radio should be converted to a spectrum monitor radio.	—	—
`spectrum band`	Specifies the spectrum band or portion of the band to be monitored by the spectrum monitor radio	**2GHz** (channels 1–14) **5GHz** (channels 36–64, 100–140 and 149–165).	2GHz

Usage Guidelines

There are two ways to change an AP that supports the spectrum monitor feature into a spectrum monitor. You can assign that AP to a 802.11a and 802.11g radio profile that is already set to spectrum mode, or you can temporarily change the AP into a spectrum monitor using a local spectrum override profile. When you use a local spectrum override profile to override the mode setting of an AP, that AP will begin to operate as a spectrum monitor, but will remain associated with its previous 802.11a and 802.11g radio profiles. If you change any parameter (other than the overridden mode parameter) in the spectrum monitor's 802.11a or 802.11g radio profiles, the spectrum monitor will immediately update with the change. When you remove the local spectrum override, the spectrum monitor will revert back to its previous mode, and remain assigned to the same 802.11a and 802.11g radio profiles as before.

For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.3.0.x User Guide.

Related Commands

Command	Description
show ap spectrum local-override	This command shows a list of AP radios currently converted to spectrum monitors via the spectrum local-override list.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	RF Protect license	Config mode on Mobility Master

ap system-profile

```
ap system-profile <profile-name>
   aeroscout-rtls-server ip-or-dns <ipaddr-or-dns> port <port> include-unassoc-sta
   {disable|enable}
   airmatch-measure-duration <airmatch-measure-duration>
   airmatch-report-enabled
   airmatch-report-period <airmatch-report-period>
   am-scan-rf-band {a | all | g}
   ap-arp-attack-protection
   ap-console-password <ap-console-password>
   ap-console-protection
   ap-deploy-hour
   ap-usb-power-override
   bkup-band {a | all | g}
   bkup-lms-ip <ipaddr>
   bkup-lms-ipv6 <ipaddr>
   bkup-mode {static | dynamic | off}
   bkup-password <password>
   ble-op-mode {Beaconing | Disabled | DynamicConsole | PersistentConsole}
   ble-token <string>
   ble-url <url>
   bootstrap-threshold <number>
   clone {default | <source>}
   console-enable
   console-log-lvl
   disable-tftp-image-upgrade
   dns-domain <domain>
   double-encrypt
   driver-log-level <severity-level>
   dscp-to-dot1p-priority-mapping <dscp-to-dot1p-priority-mapping>
   dual-5ghz-mode {automatic | disabled | enabled}
   dump-server <dump-server>
   flex-radio-mode {2.4GHz|2.4GHz-and-5GHz|5GHz}
   gre-offload
   health-check [burst size <burst-size> | frequency <frequency> | mode <mode> | packet-size
   <packet-size>| report <report>| retries <retries>}
   health-check-option
   heartbeat-dscp <heartbeat-dscp>
   heartbeat-interval <heartbeat-interval>
   image-url <image-url>
   ipm-enable
   ipm-power-reduction-step-prio {all | ipm-step {cpu_throttle_25 | cpu_throttle_50 | cpu_
   throttle_75 | disable_alt_eth | disable_pse | disable_usb | radio_2ghz_chain_1x1 | radio_
   2ghz_chain_2x2 | radio_2ghz_chain_3x3 | radio_2ghz_power_3dB | radio_2ghz_power_6dB |
   radio_5ghz_chain_1x1 | radio_5ghz_chain_2x2 | radio_5ghz_chain_3x3 | radio_5ghz_power_3dB |
   radio_5ghz_power_6dB} priority <priority>}
   led-mode {normal | off}
   led-override
   lms-hold-down-period <lms-hold-down-period>
   lms-ip <lms-ip>
   lms-ipv6 <lms-ipv6>
   lms-ping-interval <lms-ping-interval>
   lms-preemption
   maintenance-mode
   max-request-retries <max-request-retries>
   mcast-aggr
   mcast-aggr-allowed-vlan <vlan-list>
   mgmt-dscp <mgmt-dscp>
   mtu <mtu>
   native-vlan-id <native-vlan-id>
```

```
no
number_ipsec_retries <number_ipsec_retries>
rap-bw-resv-1 acl <aclname> <bw-value> [priority <priority>]
rap-bw-resv-2 acl <acl-name> <bw-value> [priority <priority>]
rap-bw-resv-3 acl <acl-name> <bw-value> [priority <priority>]
rap-bw-total <rap-bw-total>
rap-dhcp-default-router <rap-dhcp-default-router>
rap-dhcp-dns-server <rap-dhcp-dns-server>
rap-dhcp-lease <rap-dhcp-lease>
rap-dhcp-pool-end <rap-dhcp-pool-end>
rap-dhcp-pool-netmask <rap-dhcp-pool-netmask>
rap-dhcp-pool-start <rap-dhcp-pool-start>
rap-dhcp-server-id <rap-dhcp-server-id>
rap-dhcp-server-vlan <rap-dhcp-server-vlan>
rap-gre-mtu <rap-gre-mtu>
rap-local-network-access
recovery-mode {auto | legacy}
request-retry-interval <request-retry-interval>
rf-band <a | g>
rtls-server ip-or-dns <ip-or-dns> port <port> key <key> station-message-frequency <seconds>
[include-unassoc-sta {enable | disable}]
rtls-server-compat_mode
secondary-master <secondary-master>
session-acl <session-acl>
slow_timer_recovery
spanning-tree
syscontact <syscontact>
telnet
```

Description

This command configures an AP system profile.

Syntax

Parameter	Description	Range	Default
`ap system-profile <profile>`	Configures AP system profile. Give a name for this instance of the profile. The name must be 1–63 characters long.	—	default
`aeroscout-rtls-server`	Enables the AP to send RFID tag information to an AeroScout RTLS server. RTLS station reporting includes information for APs and the clients that the AP has detected.	—	—
`ip-or-dns <ip-or-dns>`	IP address or the DNS of the AeroScout server to which location reports are sent.	—	—

Parameter	Description	Range	Default
`port <port>`	Port number on the AeroScout server to which location reports are sent.	—	—
`include-unassoc-sta enable|disable`	If you select the **include-unassoc-sta enable** option, the station reports will also include information about clients not associated to any AP. By default, unassociated clients are not included in station reports.	—	disabled
`airmatch-measure-duration <airmatch-measure-duration>`	Change the AirMatch RF measurement duration from the default value of 5 minutes to any value in the range 5–60 minutes. A value of 0 disables AirMatch RF environment measurements.	5–60 minutes, or 0 minutes to disable measurements	5 minutes
`airmatch-report-enabled`	Each AP in a Mobility Master deployment measures its RF environment for a duration specified by **airmatch-measure-duration**, every 30 minutes by default. Mobility Master uses this information to compute an optimal solution.	—	enabled
`airmatch-report-period <airmatch-report-period>`	Change the frequency period which AirMatch starts measuring the RF environment. The default value is 30 minutes and the supported range of values is 5–180 minutes.	5–180 minutes	30 minutes
`am-scan-rf-band`	Scanning band for multiple RF radios.	a, g, all	all
`a`	Sets the scanning band to 802.11a only.	—	—

Parameter	Description	Range	Default
g	Sets the scanning band to 802.11g only.	—	—
all	Sets the scanning band to apply to all bands.	—	—
ap-arp-attack-protection	Drop ARP packets coming from wired or wireless clients with AP gateway IP address. In other words, disallow ARP attack from untrusted ports.	—	enabled
ap-console-password <ap-console-password>	Set the AP console password on the managed device. If the user does not set any password, the managed device generates a default random password which can be viewed by executing the **encrypt disable** command followed by the **show ap system-profile <profile-name>** command.	6–32 characters	default random password
ap-console-protection	Enable the AP console password.	—	enabled
ap-deploy-hour	Configure hour-of-day for solution deployment for all radios of an AP. Overrides Airmatch profile if a valid hour is specified.	0–23	—
ap-usb-power-override	Enabling override enables the USB port of the AP with PoE AT power. **NOTE:** This parameter is applicable for AP-205H access point only.	—	disabled
bkup-band a | all | g	Band on which the Mobility Master broadcasts the backup ESSID.	802.11a, all bands, or 802.11g	all

Parameter	Description	Range	Default
`bkup-lms-ip <bkup-lms-ip>`	In multi-controller) networks, specifies the IP address of a *backup* to the IP address specified with the lms-ip parameter.	—	—
`bkup-lms-ipv6 <bkup-lms-ipv6>`	In multi-controller IPv6 networks, specifies the IPv6 address of a *backup* to the IPv6 address specified with the lms-ipv6 parameter.	—	—
`bkup-mode dynamic|off|static`	This parameter allows AP console access using a backup ESSID, allowing users to access an AP console after the AP has disconnected from the Mobility Master. When the AP advertises a backup ESSID in either static or dynamic mode, a user is able to access and debug the AP remotely through a virtual AP. Select **dynamic** or **static** to enable this feature and select the mode by which the Mobility Master broadcasts the backup ESSID. This feature is disabled by default.	dynamic, off, or static	off
`bkup-passwords <bkup-passwords>`	Allows client access to adjust the band and mode settings for the backup ESSID.	—	—

Parameter	Description	Range	Default

`ble-op-mode`
`Beaconing |`
`Disabled |`
`DynamicConsole |`
`PersistentConsole`
	Determines how the built-in BLE chip in the AP functions. BLE chip can be in one of the following four modes:
	■ **Beaconing**: The built-in BLE chip of the AP functions as an iBeacon combined with beacon management functionality.
	■ **Disabled**: The built-in BLE chip of the AP is turned off. This is the default setting.
	■ **DynamicConsole**: The built-in chip of the AP functions as a regular iBeacon combined with beacon management functionality. However, when the link to the Mobility Master is lost, the built-in chip temporarily enables access to the AP console over BLE. This state of the BLE device may be rolled back to any of the other modes if the AP receives a different configuration setting for the **ble-op-mode** parameter from the new LMS.
	■ **PersistentConsole**: The built-in chip of the AP provides access to the AP console over BLE using a mobile application. This functionality is the superset of the **Beaconing** mode.
	NOTE: BLE is disabled on ArubaOS FIPS build.
		—	Disabled

Parameter	Description	Range	Default
`ble-token <ble-token>`	The BLE endpoint authorization token is a text string of 1–255 characters used by the BLE to authorize to and securely communicate with the BMC. This token is unique for each deployment.	1–255 characters	—
`ble-url <ble-url>`	URL of the Meridian server to which the BLE sends monitoring data.	—	—
`bootstrap-threshold <bootstrap-threshold>`	Configures number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the Mobility Master, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.	1–65535	8
`clone <source>`	Name of an existing AP system profile from which parameter values are copied.	—	—
`console-enable`	Enables console port on the AP.	—	enabled

Parameter	Description	Range	Default
`console-log-lvl {alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}`	Specifies the level of driver log prints sent to AP console. The description of different log levels are as follows: ■ **alerts:** To send driver log prints when Immediate action is needed ■ **critical:** To send driver log prints when critical conditions exist ■ **debugging:** To send driver log prints for debugging messages ■ **emergencies:** To send driver log prints when system is unusable ■ **errors:** To send driver log prints when there are error conditions ■ **informational:** To send driver log prints for informational messages ■ **notifications**: To send driver log prints when a normal, but significant condition occurs ■ **warnings:** To send driver log prints for warning conditions	—	—
`dscp-to-dot1p-priority-mapping`	Configures semicolon- separated mapping between IP DSCP value and VLAN 802.1p priority. Format: <DSCP range/list (0-63) >:<802.1p value (0-7) > Format Example: 24:4;32,34:3;45-56:1;57-60,62:7	—	—

Parameter	Description	Range	Default
`dns-domain <dns-domain>`	Name of domain that is resolved by corporate DNS servers. Use this parameter when configuring split tunnel.	—	—
`double-encrypt`	This parameter applies only to remote APs. Use double encryption for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel. All other types of data traffic between the Mobility Master and the AP (wired traffic and traffic from a split-tunneled SSID) are always encrypted in the IPsec tunnel.	—	disabled

Parameter	Description	Range	Default
`driver-log-level {alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}`	Configures the level of driver log prints sent to syslog server. The description of different log levels are as follows: ■ **alerts:** To send driver log prints when Immediate action is needed ■ **critical:** To send driver log prints when critical conditions exist ■ **debugging:** To send driver log prints for debugging messages ■ **emergencies:** To send driver log prints when system is unusable ■ **errors:** To send driver log prints when ther are error conditions ■ **informational:** To send driver log prints for informational messages ■ **notifications**: To send driver log prints when a normal, but significant condition occurs ■ **warnings:** To send driver log prints for warning conditions	—	

Parameter	Description	Range	Default
`dual-5ghz-mode {automatic|disabled|enabled}`	Mode for Dual 5GHz APs: ■ **automatic**: Dual 5GHz Mode is enabled or disabled automatically. ■ **disabled**: Dual 5GHz mode is disabled. ■ **enabled**: both radios operate on 5GHz band. **NOTE:** The **dual-5ghz-mode** parameter is supported only on 340 Series (AP-344 and AP-345) access points. However, the **automatic** mode is not supported on AP-344 access points. For example, if the configuration for **dual-5ghz-mode** is set to **automatic**, AP-344 access points do not support a dynamic mode change. Users must manually set **dual-5ghz-mode** to **Enabled** if they require AP-344 access points to operate in the dual 5GHz mode. Additionally, users must purchase the required dual 5GHz external antenna.	—	**automatic** **NOTE:** ■ In a master-local or a stand-alone controller mode, **automatic** is treated as **disabled**. ■ In a Mobility Master-Managed Device mode, **automatic** indicates that AirMatch determines when to modify the operating mode from dual band to the dual 5GHz mode.
`dump-server <dump-server>`	(For debugging purposes.) Specifies the server to receive a core dump generated when an AP process crashes.	—	—

Parameter	Description	Range	Default
`flex-radio-mode {2.4GHz|2.4GHz-and-5GHz|5GHz}`	The mode for flexible Radios. Use the following parameters: ■ **2.4GHz**: The radio operates on 2.4GHz. ■ **2.4GHz-and-5GHz**: The radio operates on both 2.4GHz and 5GHz. ■ **5GHz**: The radio operates on 5GHz.	–	–
`gre-offload`	HW acceleration of GRE traffic (for test purpose only)	—	Disabled
`health-check`	The AP Health check feature configured via the **health-check** parameters uses ping probes to check reachablility and latency levels for the connection between the AP and the managed device. Recorded latency information appears in the output of the **show ap ip health-check** command. If the managed device IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file (tmp or ap_hcm_log) on the AP.	—	—
`burst-size <size>`	Number of probes to be sent during the probe frequency interval defined by the **frequency** health-check parameter.	1–16 probes	5 probes

Parameter	Description	Range	Default
`frequency <frequency>`	Probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the **burst-size** parameter during each frequency interval defined by this **frequency** parameter.	10–300 seconds	10 seconds
`mode <mode>`	Ping probe mode is the only mode currently supported by this feature.	—	ping
`packet-size <packet-size>`	The size, in bytes, of a ping datagram.	10–2000 bytes	32 bytes
`report <report>`	Number of seconds between health check reports sent from the AP to the controller. usage reports.	60–3600 seconds	60 seconds
`retries <retries>`	Number of times the attempts to resend a probe.	1–10 retries	3 retries
`health-check-option`	Issue the **ap system-profile <profile> health-check-option** command to enable the AP Health check feature.	—	disabled
`heartbeat-dscp <heartbeat-dscp>`	Define the DSCP value of AP heartbeats. Use this feature to prioritize AP heartbeats and prevent the AP from losing connectivity with the Mobility Master over high-latency or low-bandwidth WAN connections.	0–63	0

Parameter	Description	Range	Default
heartbeat-in <heartbeat-interval>	Set the interval between heartbeat messages between a remote or campus AP and its associated Mobility Master. An increase in the heartbeat interval increases the time it will take for an AP to detect the loss in connectivity to the Mobility Master, but can reduce internet bandwidth consumed by a remote AP.	1–60 seconds	1 second
image-url <image-url>	Provide the image URL for an alternate AP image.	—	—
ipm-enable	Enables the IPM system.	—	disabled
ipm-power-reduction-step-prio all	Sets up all the IPM power reduction steps.	—	—
ipm-power-reduction-step-prio ipm-step	Sets IPM power reduction steps.	—	—
cpu_throttle_25	Configure this option to reduce the CPU frequency to 25%.		
cpu_throttle_50	Configure this option to reduce the CPU frequency to 50%.		
cpu_throttle_75	Configure this option to reduce the CPU frequency to 75%.		
disable_alt_eth	Disables the 2nd Ethernet port.		
disable_pse	Disables PSE.		
disable_usb	Disables the USB.		
radio_2ghz_chain_1x1	Configure this option to reduce 2 GHz chains to 1x1.		
radio_2ghz_chain_2x2	Configure this option to reduce 2 GHz chains to 2x2.		

Parameter	Description	Range	Default
radio_2ghz_chain_3x3	Configure this option to reduce 2 GHz chains to 3x3.		
radio_2ghz_power_3dB	Configure this option to reduce the 2 GHz radio power by 3 dB from maximum.		
radio_2ghz_power_6dB	Configure this option to reduce the 2 GHz radio power by 6 dB from maximum.		
radio_5ghz_chain_1x1	Configure this option to reduce 5 GHz chains to 1x1.		
radio_5ghz_chain_2x2	Configure this option to reduce 5 GHz chains to 2x2.		
radio_5ghz_chain_3x3	Configure this option to reduce 5 GHz chains to 3x3.		
radio_5ghz_power_3dB	Configure this option to reduce the 5 GHz radio power by 3 dB from maximum.		
radio_5ghz_power_6dB	Configure this option to reduce the 5 GHz radio power by 6 dB from maximum.		
priority <priority>	Sets the priorities for IPM power reduction steps.		
led-mode	The operating mode for the AP LEDs. This option is available on all 802.11n indoor AP platforms.	—	normal
normal	Display LEDs in normal mode.	—	—
off	Turn off all LEDs.	—	—
led-override	Override the LED action for single-LED APs in normal LED operating mode. If enabled, this feature disables the LED auto-turn-off function.	—	disabled

Parameter	Description	Range	Default
`lms-hold-down-period`	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.	1–3600 seconds	600 seconds
`lms-ip <lms-ip>`	In multi-controller networks, this parameter specifies the IP address of the LMS —the Mobility Master—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the managed device or Mobility Master. When using redundant managed device as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions. **NOTE:** If the LMS-IP is blank, the access point will remain on the managed device that it finds using methods like DNS or DHCP. If an IP address is configured for the LMS IP parameter, the AP will be immediately redirected to the managed device at that address.	—	—

Parameter	Description	Range	Default
`lms-ipv6 <lms-ipv6>`	In multi-controller IPv6 networks, specify the IPv6 address of the LMS—the Mobility Master—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the managed device or Mobility Master. When using redundant managed device as the LMS, set this parameter to be the VRRP IP address to ensure that APs always have an active IP address with which to terminate sessions.	—	—
`lms-ping-interval <lms-ping-interval>`	Specifies the interval at which application level ping needs to be sent to Mobility Master to check the reachability. Applicable only for Remote AP. **NOTE:** If this parameter is changed, UDP session timeout on an intermediate router which performs the NAT function should be set accordingly. The preferred timeout value is (lms-ping-interval + 30 seconds).	10–60 seconds	20 seconds
`lms-preemption`	Automatically reverts to the primary LMS IP address when it becomes available.	—	disabled

Parameter	Description	Range	Default
`maintenance-mode`	Enable or disable AP maintenance mode. This setting is useful when deploying, maintaining, or upgrading the network. If enabled, APs stop flooding unnecessary traps and syslog messages to NMS systems or network operations centers when deploying, maintaining, or upgrading the network. The Mobility Master still generates debug syslog messages if debug logging is enabled.	—	disabled
`max-request-retries <max-request-retries>`	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either tries the IP address specified by the bkup-lms-ip (if configured) or reboots.	1–65535	10
`mcast-aggr`	Enable multicast aggregation at AP.	—	disabled
`mcast-aggr-allowed-vlan <vlan-list>`	Enable list of VLANs where AP multicast aggregation is allowed.	—	disabled
`mgmt-dscp <mgmt-dscp>`	Sets the DSCP value of AP management packets.	0–63	—
`mtu`	MTU, in bytes, on the wired link for the AP.	1024–1578	—
`native-vlan-id <native-vlan-id>`	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).	—	1
`no`	Negates any configured parameter.	—	—

Parameter	Description	Range	Default
`number-ipsec-retries <number_ipsec_retries>`	The number of times the AP will attempt to recreate an IPsec tunnel with the Mobility Master before the AP will reboot. A value of 0 disables the reboot.	1–1000	85
`rap-bw-resv-1 acl <aclname> [priority <priority>]`	Session ACLs with uplink bandwidth reservation in Kbps. You can specify up to three session ACLs to reserve uplink bandwidth. The sum of the three uplink bandwidths should not exceed the **rap-bw-total** value. BW value is in Kbps. Optionally, you can specify the priority for class 1, class 2, and class 3 traffic.	—	—
`rap-bw-resv-2 acl <aclname> <bwvalue> [priority <priority>]`			
`rap-bw-resv-3 acl <aclname> [priority <priority>]`			
`rap-bw-total <rap-bw-total>`	This is the total reserved uplink bandwidth (in Kbps).	—	—
`rap-dhcp-default-router <rap-dhcp-default-router>`	IP address for the default DHCP router.	—	192.168.11.1
`rap-dhcp-dns-server <rap-dhcp-dns-server>`	IP address of the DNS server.	—	192.168.11.1
`rap-dhcp-lease <rap-dhcp-lease>`	The amount of days that the assigned IP address is valid for the client. Specify the lease in <days>. 0 indicates the IP address is always valid; the lease does not expire.	0–30	0
`rap-dhcp-pool-end <rap-dhcp-pool-end>`	Configures a DHCP pool for remote APs. This is the last IP address of the DHCP pool.	—	192.168.11.254
`rap-dhcp-pool-netmask <rap-dhcp-pool-netmask>`	Configures a DHCP pool for remote APs. This is the netmask used for the DHCP pool.	—	255.255.255.0

Parameter	Description	Range	Default
`rap-dhcp-pool-start <rap-dhcp-pool-start>`	Configures a DHCP pool for remote APs. This is the first IP address of the DHCP pool.	—	192.168.11.2
`rap-dhcp-server-id <rap-dhcp-server-id>`	IP address used as the DHCP server identifier.	—	192.168.11.1
`rap-dhcp-server-vlan <rap-dhcp-server-vlan>`	VLAN ID of the remote AP DHCP server used if the Mobility Master is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is unavailable.	—	—
`rap-gre-mtu <rap-gre-mtu>`	Configures the maximum size of the GRE packets exchanged between a Remote AP and the Mobility Master.	1024–1578 bytes	1200 bytes
`rap-local-network -access`	Enable or disable local network access across VLANs in a Remote AP.	—	disabled

Parameter	Description	Range	Default
`recovery-mode {legacy | auto}`	Select either the legacy recovery mode or the auto mode (fast recovery). ■ **legacy**— On detecting a firmware assert, the AP transfers the core-dump to the managed device and executes an AP reboot. ■ **auto**—On detecting a firmware assert, the AP executes the fast recovery process in the radio affected instead of rebooting the AP. This reduces the downtime of the AP in the network. If the AP detects a coredump with a valuable information during a firmware assert, then it transfers the core dump to the managed device and the AP reboots.	—	legacy
`request-retry-interval <request-retry-interval>`	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.	1–65535 seconds	10 seconds
`rf-band {a | g}`	For APs that support both *a* and *b/g* RF bands, RF band in which the AP should operate: ■ g = 2.4 GHz ■ a = 5 GHz	–	g
`rtls-server`	Enables the AP to send RFID tag information to an RTLS server.	—	—

Parameter	Description	Range	Default
`ip-or-dns`	IP address or the DNS of the RTLS server to which location reports are sent.	—	—
`port`	Port number on the server to which location reports are sent.	—	—
`key`	Shared secret key.	—	—
`station-message-frequency`	Indicates how often packets are sent to the server.	1–3600 seconds	30 seconds
`[include-unassoc-sta {enable | disable}]`	RTLS station reporting includes information for APs and the clients that the AP has detected. If you include the **include-unassoc-sta** parameter, the station reports will also include information about clients not associated to any AP. By default, unassociated clients are not included in station reports.	—	disabled
`rtls-server-compat_mode`	The compatibility mode controls the format of tag frames forwarded to the RTLS server. Enabling this mode will enable legacy format (includes a 2 byte padding), and disabling this mode will remove the padding. The tag frame format will be the same across all AP models.	—	—
`secondary-master <secondary-master>`	Assigns a remote AP as a secondary Mobility Master in the event the primary Mobility Master can not be reached.	—	—

Parameter	Description	Range	Default
`session-acl <session-acl>`	Session ACL configured with the ip access-list session command. **NOTE:** This parameter requires the PEFNG license.	—	—
`slow_timer_recovery`	If you enable this option, ArubaOS checks for a slow CPU timer, and if it detects an issue, it restarts the AP without logging a reason for the reboot. This feature is supported on AP-103H, and RAP-108 or RAP-109 access points.	—	disabled
`spanning-tree`	Enables the spanning-tree protocol.	—	disabled
`syscontact`	SNMP system contact information.	—	—
`telnet`	Enables or disables telnet to the AP.	—	disabled

Usage Guidelines

The AP system profile configures AP administrative operations, such as AirMatch and AP health check options and logging levels.

By default, each AP in a Mobility Master deployment measures its RF environment for a 5-minute duration, every 30 minutes. Mobility Master uses this information to compute an optimal solution, then deploys the latest RF plan by sending updated settings to the APs. Use the **airmatch** settings in the ap system profile to modify these default report intervals, or to disable or reenable AirMatch reports to the APs.

The AP Health check feature configured via the **health-check** parameters uses ping probes to check reachablility and latency levels for the connection between the AP and the managed devices. Recorded latency information appears in the output of the **show ap ip health-check** command. If the managed device IP address becomes unreachable from the AP uplink, this feature records the time that the connection failed, and saves that information in a log file (tmp or ap_hcm_log) on the AP.

Starting from ArubaOS 8.2.0.0, the **no ipm-power-reduction-step-prio ipm-step <ipm-step> priority <priority number>** subcommand for the **ap system-profile <profile>** command set is simplified. If you want to remove one step or priority, you only need to specify the step and not the priority. For example: **no ipm-power-reduction-step-prio ipm-step <ipm-step>**.

Example

To set the Dual 5GHz mode option for 340 Series access points through the CLI, use the following commands:

```
(host) [mynode] (config) #ap system profile <profile-name>
(host) [mynode] (AP system profile "<profile-name>") #dual-5ghz-mode enabled
```

Execute the following commands to configure LACP and AP LACP LMS map information settings.

```
(host) [mynode] (config) #ap system-profile LACP
(host) [mynode] (AP system profile "LACP") #lms-ip 192.0.2.1
(host) [mynode] (AP system profile "LACP") #exit
(host) [mynode] (config) #ap-lacp-striping-ip
(host) [mynode] (AP LACP LMS map information) #striping-ip 192.0.2.2 lms 192.0.2.1
(host) [mynode] (AP LACP LMS map information) #aplacp-enable
```

For more information on configuring LACP support, including important pre-deployment considerations and troubleshooting information, refer to the *ArubaOS User Guide*.

Execute the following command to remove one IPM step or priotity from the AP system profile, "default":

```
(host) [mynode] (config) #ap system-profile default
(host) [mynode] (AP system profile "default") #no ipm-power-reduction-step-prio ipm-step cpu_
throttle_50
```

Execute the following command to remove all IPM priorities set for an AP system profile:

```
(host) [mynode] (AP system profile "default") #no ipm-power-reduction-step-prio all
```

Use the following commands to configure the recovery mode parameter for 300 Series access points:

```
(host)  [mynode]  (config) #ap system-profile <profile-name>
(host) [mynode] (AP system profile "<profile-name>") #recovery-mode auto
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The following new parameters were added: ■ **dual-5ghz-mode** ■ **recovery-mode** ■ **ap-deploy-hour**
ArubaOS 8.2.0.0	■ A new parameter, **all**, was added to the **ipm-power-reduction-step-prio** subcommand. ■ The **no ipm-power-reduction-step-prio ipm-step <ipm-step> priority <priority number>** subcommand was changed to **no ipm-power-reduction-step-prio ipm-step <ipm-step>**. ■ A new parameter, **flex-radio-mode**, was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

ap test

```
ap test
   ap-name
   dot11k-force-beacon-request
   dot11k-force-link-measurement-request
   dot11k-force-tsm-request
   dot11v-force-bss-transition
   force_send_delts
   ip-addr
   ip6-addr
   rebootstrap
   wan
```

Description

Execute this command to get the test results in an AP.

Syntax

Parameter	Description	Range	Default
`ap test`	Run test command on AP.	—	—
`ap-name|bar-retries|bar-times`	Name of the access point.	—	—
`dot11k-force-beacon-request|sta|<sta_mac>`	Test force sending 802.11 Beacon Report Request frame.	—	—
`dot11k-force-link-measurement-request|sta|<sta_mac>`	Test force sending 802.11 Link Measurement Request frame.	—	—
`dot11k-force-tsm-request|sta|<sta_mac>`	Test force sending TSM Report Request frame.	—	—
`dot11v-force-bss-transition|sta|<sta_mac>`	Test force sending BSS Transition Mgmt Request frame.	—	—
`force_send_delts`	Force sending DELTS to the client.	—	—
`ip-addr`	IP Address of Access Point.	—	—

Parameter	Description	Range	Default
`ip6-addr`	IPv6 address of Access Point.	—	—
`rebootstrap|ap-name|ip-addr|ip6-addr`	Rebootstrap AP.	—	—
`wan|down|up`	Wan link test command. ■ **down** — Trigger wan down event. ■ **up** — Trigger wan up event.	—	—

Example

The following command displays different results of AP-related tests:

```
(host) [mynode] #ap test
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

ap wipe out flash

```
ap wipe out flash
   ap-name <ap-name>
   ip-addr <ip-addr>
```

Description

Overwrite the entire AP compact flash, destroying its contents (including the current image file).

Syntax

Parameter	Description	Range	Default
`ap-name`	Wipe out the flash of the AP with the specified name.	—	—
`ip-addr`	Wipe out the flash of the AP with the specified IP address.	—	—

Usage Guidelines

Use this command only under the supervision of Aruba technical support. If you delete the current image in the AP's flash memory, the AP will not function until you reload another image.

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

ap wired-ap-profile

```
ap wired-ap-profile {default | <profile-name>}
   broadcast
   clone {default | <source>
   forward-mode {bridge|split-tunnel|tunnel}
   no
   switchport {access vlan <vlan> | mode {access|trunk} | trunk {allowed vlan <vlan-list>| add
   <vlan-list> | except <vlan-list> | remove <vlan-list>}} | {native vlan <vlan>}
   trusted
   wired-ap-enable
```

Description

This command configures a wired AP profile.

Syntax

Parameter	Description	Default
`ap wired-ap-profile <profile-name>`	Name of this instance of the profile. The name must be 1–63 characters.	default
`broadcast`	Forward broadcast traffic to this tunnel.	
`clone <source>`	Name of an existing wired AP profile from which parameter values are copied.	default
`forward-mode`	In this default forwarding mode, the AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual. This parameter controls whether data is tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). All forwarding modes support band steering, TSPEC or TCLAS enforcement, 802.11k and station blacklisting.	

Parameter	Description	Default
bridge	802.11 frames are bridged into the local Ethernet LAN. When a remote AP or campus AP is in bridge mode, the AP handles all 802.11 association requests and responses, encryption or decryption processes, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in bridge mode supports only the 802.1X authentication type. **NOTE:** Virtual APs in bridge mode using static WEP should use key slots 2–4 on the managed device. Key slot 1 should only be used with Virtual APs in tunnel mode.	
split-tunnel	802.11 frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). An AP in split-tunnel mode supports only the 802.1X authentication type. An AP in split-tunnel forwarding mode handles all 802.11 association requests and responses, encryption or decryption, and firewall enforcement. The 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. **NOTE:** Virtual APs in split-tunnel mode using static WEP should use key slots 2–4 on the managed device. Key slot 1 should only be used with Virtual APs in tunnel mode.	
tunnel	In this default forwarding mode, the AP handles all 802.11 association requests and responses, but sends all 802.11 data packets, action frames, and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual.	
no	Negates any configured parameter.	
switchport	Configures the switching mode characteristics for the port.	
access vlan <vlan>	The VLAN to which the port belongs. The default is VLAN 1.	
mode {access|trunk}	The mode for the port, either access or trunk mode. The default is access mode.	
trunk allowed vlan {add <vlan-list> | except <vlan-list>| remove <vlan-list>| <vlan-list}	Allows multiple VLANs on the port interface. You must define this parameter using VLAN IDs or VLAN names VLAN IDs and VLAN names cannot be listed together.	

Parameter	Description	Default
`trunk native vlan <vlan>`	The native VLAN for the port (frames on the native VLAN are not tagged with 802.1q tags).	
`trusted`	Sets port as either trusted or untrusted. The default setting is untrusted.	
`wired-ap-enable`	Enables the wired AP. The wired AP is disabled by default.	

Usage Guidelines

This command is only applicable to Aruba APs that support a second Ethernet port. The wired AP profile configures the second Ethernet port (enet1) on the AP.

For mesh deployments, this command is applicable to all Aruba APs configured as mesh nodes. If you are using mesh to join multiple Ethernet LANs, configure and enable bridging on the mesh point Ethernet port.

Mesh nodes only support bridge mode and tunnel mode on their wired ports (enet0 or enet1). Split tunnel mode is not supported.

Use the bridge mode to configure bridging on the mesh point Ethernet port. Use tunnel mode to configure secure jack operation on the mesh node Ethernet port.

When configuring the Ethernet ports on APs with multiple Ethernet ports, note the following requirements:

- If configured as a mesh portal, connect enet0 to the managed device to obtain an IP address. The wired AP profile controls enet1.Only enet1 supports secure jack operation.
- If configured as a mesh point, the same wired AP profile will control both enet0 and enet1.

Example

The following command configures the enet1 port on a multi-port AP as a trunk port:

```
(host) [mynode] (config) #ap wired-ap-profile wiredap1
(host) [mynode] (Wired AP profile "wiredap1") #switchport mode trunk
(host) [mynode] (Wired AP profile "wiredap1") #switchport trunk allowed 4,5
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode Mobility Master.

ap wired-port-profile

```
ap wired-port-profile {default | <profile-name>}
   aaa-profile {default | <profile-name>}
   authentication-timeout <timeout>
   auto-recovery-enable
   auto-recovery-interval <auto-recovery-interval>
   bridge-role
   clone {default | <source>}
   enet-link-profile <profile-name>
   lldp-profile {default | <profile-name>}
   loop-detection-interval <loop-detection-interval>
   loop-protect-enable
   no
   portfast
   portfast-trunk
   rap-backup
   shutdown
   spanning-tree
   storm-control-broadcast
   storm-control-broadcast-threshold
   wired-ap-profile <profile-name>
```

Description

This command configures a wired port profile.

Syntax

Parameter	Description	Range	Default
`ap wired-port-profile <profile-name>`	Name of this instance of the profile. The name must be 1–63 characters.		default
`aaa-profile <profile-name>`	Name of a AAA profile to be used by devices connecting to the wired port of the AP.		
`authentication-timeout <timeout>`	Authentication timeout value, in seconds, for devices connecting the wired port of the AP. The supported range is 1–65535 seconds, and the default value is 20 seconds.	1–65535 seconds	5 seconds

Parameter	Description	Range	Default
`auto-recovery-enable`	Enables automatic recovery of the port in the AP that is shut down because of loop protection. After the automatic recovery, if the loop re-occurs, then the port is shutdown again		Disabled
`auto-recovery-interval <auto-recovery-interval>`	Specify the time, in seconds, to automatically recover the port in the AP that is shut down because of loop protection.	30-43200 seconds	300 seconds
`bridge-role <role>`	Role that is assigned to a user if split-tunnel authentication fails.		
`clone <source>`	Create a new AP wired port profile based upon the values of an existing profile.		default
`enet-link-profile <profile-name>`	Specify an Ethernet link profile to be used by devices associated with this wired port profile. The Ethernet link profile defines the duplex value and speed to be used by the port.		
`lldp-profile <profile-name>`	Specify an LLDP profile to be used by devices associated with this wired port profile. The LLDP profile specifies the type-length-value (TLV) elements to be sent in LLDP PDUs.		
`loop-detection-interval <loop-detection-interval>`	Specify the time, in seconds, to send loop detection packets on the ports of an AP.	1-10 seconds	2 seconds
`loop-protect-enable`	Enables loop protection on the ports of an AP.		Disabled
`no`	Negates any defined parameter		
`portfast`	Enables portfast for AP wired ports. Spanning tree must be enabled before this command can be used.		

Parameter	Description	Range	Default
`portfast-trunk`	Spanning tree must be enabled before this command can be used.		
`rap-backup`	Use the **rap-backup** parameter to use the wired port on a Remote AP for local connectivity and troubleshooting when the AP cannot reach the managed device. If the AP is not connected to the managed device, no firewall policies will be applied when this option is enabled. (The AAA profile will be applied when the AP is connected to managed device).		
`shutdown`	Disable the wired AP port.		
`spanning-tree`	Enables the spanning-tree protocol.		
`storm-control-broadcast`	Enables the broadcast storm control. When this parameter is enabled, if the AP detects a loop on one of its Ethernet port, it shuts down the Ethernet port. This prevents the AP from receiving or sending any frames.		
`storm-control-broadcast-threshold`	Specify the broadcast packets per second on each Ethernet port of an AP before the Ethernet port is shut down.		2000
`wired-ap-profile <profile-name>`	Name of a wired AP profile to be used by devices connecting the wired port of the AP. The wired AP profile defines the forwarding mode and switchport values used by the port.		

Usage Guidelines

This command is only applicable to APs with Ethernet ports. Issue this command to enable or disable the wired port, define an AAA profile for wired port devices, and associate the port with an ethernet link profile that defines its speed and duplex values.

Example

The following command defines a AAA profile for wired port devices:

```
(host)[mynode] (config) #ap wired-port-profile wiredport1
(host)[mynode] (AP wired port profile"wiredport1") #aaa-profile default-open
(host)[mynode] (AP wired port profile"wiredport1") #authentication-timeout 30
(host)[mynode] (AP wired port profile"wiredport1") #wired-ap-profile wiredap1
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The following parameters were introduced: ■ auto-recovery-enable ■ auto-recovery-interval ■ loop-detection-interval ■ loop-protect-enable ■ storm-control-broadcast ■ storm-control-broadcast-threshold
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

apboot

```
apboot {all [global|local]|ap-group <ap-group> |ap-name <ap-name>|ip-addr <ipaddr>|ip6-addr
<ip6addr>|wired-mac <macaddr>}
```

Description

This command reboots the specified APs.

Syntax

Parameter	Description	Default
`all`	Reboot all APs.	all
`global`	Reboot APs on all controllers.	global
`local`	Reboot only APs registered on this controller. This is the default.	local
`ap-group`	Reboot APs in a specified group.	ap-group
`ap-name`	Reboot the AP with the specified name.	ap-name
`ip-addr`	Reboot the AP at the specified IP address.	ip-addr
`ip6-addr`	Reboot the AP at the specified IPv6 address.	ip6-addr
`wired-mac`	Reboot the AP at the specified MAC address.	wired-mac

Usage Guidelines

You should not normally need to use this command as APs automatically reboot when you reprovision them. Use this command only when directed to do so by your Aruba representative.

Example

The following command reboots a specific AP:

```
(host) [mynode] (config)# apboot ap-name Building3-Lobby
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Master.

apconnect

```
apconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>}
```

Description

This command instructs a mesh point to disconnect from its current parent and connect to a new parent.

Syntax

Parameter	Description
`ap-name <name>`	Specify the name of the mesh point to be connected to a new parent.
`bssid <bssid>`	Specify the BSSID of the mesh point to be connected to a new parent.
`ip-addr <ipaddr>`	Specify the IP address of the mesh point to be connected to a new parent.

Usage Guidelines

To maintain a mesh topology created using the **apconnect** command, Aruba suggests setting the mesh reselection-mode to **reselect-never**, otherwise the normal mesh reselection mechanisms could break up the selected topology.

Example

The following command connects the mesh point "meshpoint1" to a new parent with the specified BSSID.

```
(host) [mynode] (config) #apconnect ap-name meshpoint1 parent-bssid 00:12:6d:03:1c:f1
```

Related Commands

Command	Description	Mode
ap mesh-radio-profilereselection-modereselect-never	Use this command to prevent the AP from re-selecting a new parent.	Enable or Config mode.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Master.

ap-crash-transfer

```
ap-crash-transfer
```

Description

This command allows AP coredump files to be transferred to the controller flash memory if no dumpserver is configured.

Syntax

No Parameters

Usage Guidelines

The command **ap system-profile <profile> dump-server <server>** specifies a server to receive a core dump generated when an AP process crashes. If no dump server is configured, issue the **ap-crash-transfer** command to save dump files to the controller flash memory.

If you define a dump server and issue the ap-crash-server command, the dump server configuration takes precedence, and coredump files are sent to the dump server.

Example

```
(host)[mynode] (config) #ap-crash-transfer
```

Related Commands

Command	Description
show ap-crash-transfer	This command shows if AP coredump files can be transferred to controller flash memory if no dumpserver is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

apdisconnect

```
apdisconnect {ap-name <name>|bssid <bssid>|ip-addr <ipaddr>}
```

Description

This command disconnects a mesh point from its parent.

Syntax

Parameter	Description
`ap-name`	Specifies the name of the parent AP.
`bssid`	Specifies the BSSID of the parent AP.
`ip-addr`	Specifies the IP address of the parent AP.

Usage Guidelines

Each mesh point learns about the mesh portal from its parent (a mesh node that is part of the path to the mesh portal). This command directs a mesh point to disassociate from its parent. The mesh point will attempt to associate with another neighboring mesh node, if available. The old parent is not eligible for re-association for 60 seconds after disconnection.

Example

The following command disconnects a specific mesh point from its parent:

```
(host) [mynode] (config) #apdisconnect ap-name meshpoint1
```

Related Commands

Command	Description	Mode
apconnect	This command connects a mesh point to a new specified parent.	Enable or Config mode.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Master.

apflash

```
apflash
   all {global|local}
   ap-group <ap-group>
   ap-name <ap-name>
   ip-addr <ip-addr>
   wired-mac <wired-mac>
```

Description

This command re-flashes the specified AP.

Syntax

Parameter	Description
`all`	Re-flash all APs.
`global`	Re-flash all APs on all managed devices.
`local`	Re-flash all APs registered on this device. This is the default setting.
`ap-group`	Re-flash all APs in this group.
`ap-name`	Re-flash AP with this name.
`ip-addr`	Re-flash AP with this IP address.
`wired-mac`	Re-flash AP with this MAC address.

Usage Guidelines

Execute this command under the guidance of Aruba technical support.

Examples

The following commands re-flashes an AP with an AP name *ap-corp-325*:

```
(host) [mynode] #apflash ap-name ap-corp-325
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master.

ap-group

```
ap-group {default | <profile-name>}
   am-filter-profile {default | <profile-name>}
   ap-multizone-profile {default | <profile-name>}
   ap-system-profile {default | <profile-name>}
   authorization-profile {default | <profile-name>}
   clone {default | <source>}
   dot11a-radio-profile {default | <profile-name>}
   dot11a-traffic-mgmt-profile {default | <profile-name>}
   dot11g-radio-profile {default | <profile-name>}
   dot11g-traffic-mgmt-profile {default | <profile-name>}
   enet0-port-profile {default | <profile-name>}
   enet1-port-profile {default | <profile-name>}
   enet2-port-profile {default | <profile-name>}
   enet3-port-profile {default | <profile-name>}
   enet4-port-profile {default | <profile-name>}
   event-thresholds-profile {default | <profile-name>}
   ids-profile {default | <profile-name>}
   mesh-cluster-profile {default | <profile-name>} [priority <1-16>]
   mesh-radio-profile {default | <profile-name>}
   no ...
   provisioning profile {default | <profile-name>}
   regulatory-domain-profile {default | <profile-name>}
   rf-optimization-profile {default | <profile-name>}
   virtual-ap {default | <profile-name>}
```

Description

This command configures an AP group.

Syntax

Parameter	Description	Range	Default
`ap-group <profile-name>`	Profile name that identifies the AP group. The name must be 1–63 characters long. **NOTE:** You cannot use quotes (“) in the AP group name.	—	default
`am-filter-profile <profile-name>`	Configures the AM filter profile.	—	default
`ap-multizone-profile <profile-name>`	Configures the AP multizone profile.	—	default
`ap-system-profile <profile-name>`	Configures AP administrative operations, such as logging levels. See ap system-profile on page 249.	—	default
`authorization-profile <profile-name>`	Restrictive group for unauthorized AP.	—	default

Parameter	Description	Range	Default
`clone <source>`	Name of an existing AP group from which profile names are copied.	—	—
`dot11a-radio-profile <profile-name>`	Configures 802.11a radio settings and load balancing for the AP group; contains the ARM profile. See rf dot11a-radio-profile on page 843.	—	default
`dot11a-traffic-mgmt-profile <profile-name>`	Configures bandwidth allocation. See wlan traffic-management-profile on page 2646.	—	default
`dot11g-radio-profile <profile-name>`	Configures 802.11g radio settings and load balancing for the AP group; contains the ARM profile. See rf dot11a-radio-profile on page 843.	—	default
`dot11g-traffic-mgmt-profile <profile-name>`	Configures bandwidth allocation. See wlan traffic-management-profile on page 2646.	—	default
`enet0-port-profile <profile-name>`	Configures the duplex and speed of the Ethernet interface 0 on the AP. For information on how these profiles are defined, see ap wired-port-profile on page 279.	—	default
`enet1-port-profile <profile-name>`	Configures the duplex and speed of the Ethernet interface 1 on the AP. For information on how these profiles are defined, see ap wired-port-profile on page 279.	—	default
`enet2-port-profile <profile-name>`	Configures the duplex and speed of an Ethernet interface 2 on the AP. These profiles are defined using the command ap wired-port-profile on page 279.	—	default
`enet3-port-profile <profile-name>`	Configures the duplex and speed of an Ethernet interface 3 on the AP. These profiles are defined using the command ap wired-port-profile on page 279.	—	default

Parameter	Description	Range	Default
`enet4-port-profile <profile-name>`	Configures the duplex and speed of an Ethernet 4 interface on the AP. For information on how these profiles are defined, see ap wired-port-profile on page 279.	—	default
`event-thresholds-profile <profile-name>`	Configures Received Signal Strength Indication (RSSI) metrics. See rf event-thresholds-profile on page 872.	—	default
`ids-profile <profile-name>`	Configures Aruba's IDS. See ids profile on page 507.	—	default
`mesh-cluster-profile <profile-name>`	Configures the mesh cluster profile for mesh nodes that are members of the AP group. There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See ap mesh-cluster-profile on page 200.	—	default
`priority <1-16>`	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The lower the number, the higher the priority.	1–16	1
`mesh-radio-profile <profile-name>`	Configures the 802.11g and 802.11a radio settings for mesh nodes that are members of the AP group. See ap mesh-ht-ssid-profile on page 203. Commands to configure mesh for outdoor APs require the Outdoor Mesh license.	—	default
`no`	Negates any configured parameter.	—	—
`provisioning profile <profile-name>`	Configures the provisioning profile.	—	default
`regulatory-domain-profile <profile-name>`	Configures the country code and valid channels. See ap regulatory-domain-profile on page 239.	—	default

Parameter	Description	Range	Default
`rf-optimization-profile <profile-name>`	Configure coverage hole and interference detection. See rf optimization-profile on page 877.	—	default
`virtual-ap <profile-name>`	One or more profiles, each of which configures a specified WLAN. See wlan virtual-ap on page 2652.	—	default

Usage Guidelines

AP groups are at the top of the configuration hierarchy. An AP group collects virtual AP definitions and configuration profiles, which are applied to APs in the group.

Example

The following command configures a virtual AP profile to the “default” AP group:

```
(host)[mynode](config) #ap-group test1
(host)[mynode] (AP group "test1") #virtual-ap corpnet
```

Related Commands

Command	Description
show ap-group	Shows configuration for an AP group.

You can view AP group settings using the command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

ap-leds

```
ap-leds
   {all | ap-group <ap-group> | ap-name <ap-name> | ip-addr <ip address> | wired-mac <mac
   address>}
```

Description

This command allows you to set the behavior of an AP's LEDs.

Syntax

Parameter	Description
`all`	Controls the LED behavior for all APs
`global`	Selects all APs on all controllers. ■ **blink**: Make LEDs blink for identification. ■ **normal**: Restore LEDs to their normal behavior.
`local`	Selects all APs registered on this controller.
`ap-group <ap-group>`	Controls the LED behavior for APs in the specified group.
`ap-name <ap-name>`	Controls the LED behavior for the AP with the specified name.
`ip-addr <ip-addr>`	Controls the LED behavior for the AP with the specified IP address.
`wired-mac <mac-addr>`	Controls the LED behavior for the AP with the specified MAC address.

Usage Guidelines

Use the **ap-leds** command to make the LEDs on a defined set of APs either blink or display in the currently configured LED operating mode. Note that if the LED operating mode defined in the AP's system profile is set to "off", then the **normal** parameter in the **ap-leds** command will disable the LEDs. If the LED operating mode in the AP system profile is set to "normal" then the **normal** parameter in this command will allow the LEDs light as usual.

Example

The following command causes all local APs to blink their LEDs for identification purposes:

```
(host) [mynode] (config) #ap-leds
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

ap-move

```
ap-move
   all
   ap-group <ap-group>
   ap-name <ap-name>
```

Description

When HA is enabled, use this command to move an AP or group of APs to their managed devices.

Syntax

Parameter	Description
`all`	Move all APs.
`ap-group <ap-group>`	Move all APs belonging to the specified AP group.
`ap-mac <ap-mac>`	Move all APs belonging to the MAC of the specified AP.
`target-v4`	Target managed device IPv4 address.
`target-v6`	Target managed device IPv6 address.

Usage Guidelines

When HA is enabled on a pair of managed devices, this command should be used when it is necessary to move a single AP, all APs in an ap-group, or all APs to switchover to their standby managed device without an actual failure of the active managed device. For example, this allows the network admin to manually move one or more APs to their managed device and perform a planned upgrade or maintenance on the active managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms.	Base operating system.	Config mode on Mobility Master.

ap-name

```
ap-name <profile-name>
   am-filter-profile {default | <profile-name>}
   ap-multizone-profile {default | <profile-name>}
   ap-system-profile {default | <profile-name>}
   authorization-profile {default | <profile-name>}
   clone {default | <source>}
   dot11a-radio-profile {default | <profile-name>}
   dot11a-traffic-mgmt-profile {default | <profile-name>}
   dot11g-radio-profile {default | <profile-name>}
   dot11g-traffic-mgmt-profile {default | <profile-name>}
   enet0-profile {default | <profile-name>}
   enet1-profile {default | <profile-name>}
   enet2-profile {default | <profile-name>}
   enet3-profile {default | <profile-name>}
   enet4-profile {default | <profile-name>}
   event-thresholds-profile {default | <profile-name>}
   exclude-mesh-cluster-profile-ap {default | <profile-name>}
   exclude-virtual-ap {default | <profile-name>}
   ids-profile {default | <profile-name>}
   mesh-cluster-profile {default | <mesh-cluster-profile>} priority <priority>
   mesh-radio-profile {default | <profile-name>}
   no
   regulatory-domain-profile {default | <profile-name>}
   rf-optimization-profile {default | <profile-name>}
   virtual-ap {default | <profile-name>}
```

Description

This command configures a specific AP.

Syntax

Parameter	Description	Default
`ap-name <profile-name>`	Configures an AP name. Give a name that identifies the AP. By default, the name of an AP can either be its Ethernet MAC address, or if the AP has been previously provisioned with an earlier version of ArubaOS, a name in the format <building>.<floor>.<location>. The name must be 1–63 characters long. **NOTE:** You cannot use quotes (“) in the AP name.	—
`am-filter-profile <profile-name>`	Configures AM filter profile.	default
`am-multizone-profile <profile-name>`	Configures AP multizone profile.	default
`ap-system-profile <profile-name>`	Configures AP administrative operations, such as logging levels. See ap system-profile on page 249.	default

Parameter	Description	Default
`authorization-profile <profile-name>`	Restrictive group for unauthorized AP.	default
`clone <source>`	Name of an existing AP name from which profile names are copied.	default
`dot11a-radio-profile <profile-name>`	Configures 802.11a radio settings for the AP group; contains the ARM profile. See rf dot11a-radio-profile on page 843.	default
`dot11a-traffic-mgmt-profile <profile-name>`	Configures bandwidth allocation. See wlan traffic-management-profile on page 2646.	default
`dot11g-radio-profile <profile-name>`	Configures 802.11g radio settings for the AP group; contains the ARM profile. See rf dot11g-radio-profile on page 854.	default
`dot11g-traffic-mgmt-profile <profile-name>`	Configures bandwidth allocation. See wlan traffic-management-profile on page 2646.	default
`enet0-profile <profile-name>`	Configures the duplex and speed of the Ethernet 0 interface on the AP. See ap enet-link-profile on page 181.	default
`enet1-profile <profile-name>`	Configures the duplex and speed of the Ethernet 1 interface on the AP. See ap enet-link-profile on page 181.	default
`enet2-profile <profile-name>`	Configures the duplex and speed of the Ethernet 2 interface on the AP. See ap enet-link-profile on page 181.	default
`enet3-profile <profile-name>`	Configures the duplex and speed of the Ethernet 3 interface on the AP. See ap enet-link-profile on page 181.	default
`enet4-profile <profile-name>`	Configures the duplex and speed of the Ethernet 4 interface on the AP. See ap enet-link-profile on page 181.	default
`event-thresholds-profile <profile-name>`	Configures Received Signal Strength Indication (RSSI) metrics. See rf event-thresholds-profile on page 872.	default
`exclude-mesh-cluster-profile-ap <profile-name>`	Excludes the specified mesh cluster profile from this AP. The Secure Enterprise Mesh license must be installed.	—

Parameter	Description	Default
exclude-virtual-ap <profile-name>	Excludes the specified virtual AP profiles from this AP.	—
ids-profile <profile-name>	Configures Aruba's IDS. See ids profile on page 507.	default
mesh-cluster-profile <profile-name>	Configures the mesh cluster profile for the AP (mesh node). There is a "default" mesh cluster profile; however, it is not applied until you provision the mesh node. See ap mesh-cluster-profile on page 200. The Secure Enterprise Mesh license must be installed.	default
priority <priority>	Configures the priority of the mesh cluster profile. If more than two mesh cluster profiles are configured, mesh points use this number to identify primary and backup profile(s). The supported range of values is 1–16. The lower the number, the higher the priority.	1
mesh-radio-profile <profile-name>	Configures the 802.11g and 802.11a radio settings for the AP (mesh node). See ap mesh-ht-ssid-profile on page 203. The Secure Enterprise Mesh license must be installed.	default
no	Negates any configured parameter.	—
regulatory-domain-profile <profile-name>	Configures the country code and valid channels. See ap regulatory-domain-profile on page 239.	default
rf-optimization-profile <profile-name>	Configures load balancing and coverage hole and interference detection. See rf optimization-profile on page 877.	default
virtual-ap <profile-name>	One or more profiles, each of which configures a specified WLAN. See wlan virtual-ap on page 2652.	default

Usage Guidelines

Profiles that are applied to an AP group can be overridden on a per-AP name basis, and virtual APs can be added or excluded on a per-AP name basis. If a particular profile is overridden for an AP, all parameters from the overriding profile are used. There is no merging of individual parameters between the AP and the AP group to which the AP belongs.

Example

The following command excludes a virtual AP profile from a specific AP:

```
(host) [mynode] (config) #ap-name 00:0b:86:c0:cf:d8
(host) [mynode] (AP name "00:0b:86:c0:cf:d") #exclude-virtual-ap corpnet
```

Related Commands

Command	Description
show ap-name	To view the AP settings.

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ap-regroup

```
ap-regroup {ap-name <name>|serial-num <num>|wired-mac <macaddr>} <group>
```

Description

This command moves a specified AP into a group.

Syntax

Parameter	Description	Default
`ap-name`	Name of the AP.	—
`serial-num`	Serial number of the AP.	—
`wired-mac`	MAC address of the AP.	—
`<group>`	Name that identifies the AP group. The name must be 1-63 characters.	“default”

Usage Guidelines

All APs discovered by the Mobility Master are assigned to the “default” AP group. An AP can belong to only one AP group at a time. You can move an AP to an AP group that you created with the **ap-group** command.

This command automatically reboots the AP.

Example

The following command moves an AP to the ‘corpnet’ group:

```
(host) [mynode] (config) #ap-regroup wired-mac 00:0f:1e:11:00:00 corpnet
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Master.

ap-rename

```
ap-rename {ap-name <name>|serial-num <num>|wired-mac <macaddr>} >
```

Description

This command changes the name of an AP to the specified new name.

Syntax

Parameter	Description
`ap-name`	Current name of the AP.
`serial-num`	Serial number of the AP.
`wired-mac`	MAC address of the AP.

Usage Guidelines

An AP name must be unique within your network.

This command automatically reboots the AP.

Example

The following command renames an AP:

```
(host) [mynode] (config) #ap-rename wired-mac 00:0f:1e:11:00:00 building3-lobby
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable and Config mode on Mobility Master.

arm move-sta

```
arm move-sta <client-mac> <newbssid>
```

Description

This command moves a client station to another BSSID.

Syntax

Parameter	Description
`<mac>`	MAC address of the client to be moved to another BSSID
`<newbssid>`	BSSID of the AP to which the client should associate.

Usage Guidelines

Issue this command to manually move a client to a different BSSID.

Example

The following command moves a client with the MAC address **00:0B:86:01:7A:C0** to the BSSID **00:1C:B3:09:85:15**.

```
(host)[mynode](config) #arm move-sta 00:0B:86:01:7A:C0 00:1C:B3:09:85:15
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

arp

```
arp <ipaddr> <macaddr>
```

Description

This command adds a static Address Resolution Protocol (ARP) entry.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the device to be added.
`<macaddr>`	Hardware address of the device to be added, in the format xx:xx:xx:xx:xx:xx.

Usage Guidelines

If the IP address does not belong to a valid IP subnetwork, the ARP entry is not added. If the IP interface that defines the subnetwork for the static ARP entry is deleted, you will be unable to use the arp command to overwrite the entry's current values; use the no arp command to negate the entry and then enter a new arp command.

Example

The following command configures an ARP entry:

```
(host)[node](config) #arp 10.152.23.237 00:0B:86:01:7A:C0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

m	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

audit-trail

```
audit-trail [all]
```

Description

This command enables an audit trail.

Syntax

Parameter	Description
`all`	Enables audit trail for all commands, including enable mode commands. The **audit-trail** command without this option enables audit trail for all commands in configuration mode.

Usage Guidelines

By default, audit trail is enabled for all commands in configuration mode. Use the **show audit-trail** command to display the content of the audit trail.

Example

The following command enables an audit trail:

```
(host) [mynode] (config) #audit-trail
```

Related Commands

Command	Description
show audit-trail	Displays the audit trail log.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

backup

```
backup {config|flash}
```

Description

This command backs up compressed critical files in flash.

Syntax

Parameter	Description
`config`	Backs up flash config directories to configbackup.tar.gz
`flash`	Backs up flash directories to flashbackup.tar.gz file.

Usage Guidelines

To restore these directories, use the following commands:

- **`restore flash`**: untar and uncompress the flashbackup.tar.gz file.
- **`restore config`**: untar and uncompress the configbackup.tar.gz file.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config modes on the Mobility Master

banner motd

```
banner motd <delimiter> <textString>
```

Description

This command defines a text banner to be displayed at the login prompt when a user accesses Mobility Master.

Syntax

Parameter	Description	Range
`<delimiter>`	Indicates the beginning and end of the banner text.	—
`<textString>`	The text you want displayed.	up to 1023 characters

Usage Guidelines

The banner you define is displayed at the login prompt for Mobility Master. The banner is specific to the Mobility Master on which you configure it. The WebUI displays the configured banner at its login prompt, but you cannot use the WebUI to configure the banner.

The delimiter is a single character that indicates the beginning and the end of the text string in the banner. Select a delimiter that is not used in the text string you define, because the Mobility Master ends the banner when it sees the delimiter character repeated.

There are two ways of configuring the banner message:

- Enter a space between the delimiter and the beginning of the text string. The text can include any character except a quotation mark (“). Use quotation marks to enclose your text if you are including spaces (spaces are not recognized unless your text string is enclosed in quotation marks; without quotation marks, the text is truncated at the first space). You can also use the delimiter character within quotation marks.
- Press the **Enter** key after the delimiter to be placed into a mode where you can simply enter the banner text in lines of up to 255 characters, including spaces. Quotation marks are ignored.

Example

The following example configures a banner by enclosing the text within quotation marks:

```
(host) [mynode] (config) #banner motd * “Welcome to my controller. This controller is in the production network, so please do not save configuration changes. Zach Jennings is awesome. Maintenance will be performed at 7:30 PM, so please log off before 7:00 PM.”*
```

The following example configures a banner by pressing the **Enter** key after the delimiter:

```
(host) [mynode] (config) #banner motd *
Enter TEXT message [maximum of 1023 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '*'.

Welcome to my controller. This controller is in the production network, so please do not save configuration changes. Zach Jennings is awesome. Maintenance will be performed at 7:30 PM, so please log off before 7:00 PM.*
```

The banner display is as follows:

```
Welcome to my controller. This controller is in the production network, so please do not save configuration changes. Zach Jennings is awesome. Maintenance will be performed at 7:30 PM, so please log off before 7:00 PM.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

banner via

```
banner via <delimiter> <textstring>
```

Description

This command defines a login banner for Virtual Intranet Access (VIA) users.

Syntax

Parameter	Description	Range
`<delimiter>`	Indicates the beginning and end of the banner text.	—
`<textstring>`	The text you want displayed.	up to 1023 characters

Usage Guidelines

The banner you define is displayed when a user accesses VIA. The WebUI displays the configured banner at its login prompt, but you cannot use the WebUI to configure the banner.

The delimiter is a single character that indicates the beginning and the end of the text string in the banner. Select a delimiter that is not used in the text string you define.

There are two ways of configuring the banner message:

- Enter a space between the delimiter and the beginning of the text string. The text can include any character except a quotation mark (“). Use quotation marks to enclose your text if you are including spaces (spaces are not recognized unless your text string is enclosed in quotation marks; without quotation marks, the text is truncated at the first space). You can also use the delimiter character within quotation marks.
- Press the **Enter** key after the delimiter to be placed into a mode where you can simply enter the banner text in lines of up to 255 characters, including spaces. Quotation marks are ignored.

Example

The following example configures a banner by enclosing the text within quotation marks:

```
(host) [mynode] (config) #banner via * “Welcome”*
```

The following example configures a banner by pressing the **Enter** key after the delimiter:

```
(host) [mynode] (config) #banner via *
Enter TEXT message [maximum of 1023 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '*'.

Welcome*
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

ble_relay

```
ble_relay mgmt-server {type}
   https <https-endpoint> {token <token> [id <id>]}
   ws <ws-endpoint>
```

Description

This command configures the Bluetooth Low Energy (BLE) relay on devices.

Syntax

Parameter	Description
`mgmt-server {type}`	Registers the management server IP Address with the controller. This could be the Meridian server or any other server that receives messages from ble_relay using the specified protocol.
`https <https-endpoint>`	HTTPS-based endpoint URL or IP address.
`token <token>`	Authorization token for handshake.
`id <id>`	Location ID for handshake.
`ws <ws-endpoint>`	WebSocket-based endpoint URL or IP address.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

ble_relay set-attr

```
ble_relay set-attr {tag-logging <tag-logging> | ws-connect <ws-connect> | ws-loglvl <ws-loglvl>}
```

Description

This command configures the attribute values of Bluetooth Low Energy (BLE) relay.

Syntax

Parameter	Description
`tag-logging <tag-logging>`	Initiates or terminates the tag report logging. Enter one of the following values: ■ 1: initiate ■ 0: terminate
`ws-connect <ws-connect>`	Initiates or terminates the WebSocket connection.
`ws-loglvl <ws-loglvl>`	Enter the log level to debug the WebSocket connection.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

block-redirect-url

```
block-redirect-url <string>
```

Description

This command defines the URL to which a session is redirected if it is denied.

Syntax

Parameter	Description	Range
`<string>`	Redirect URL. This must be an absolute URL, with an http or https prefix.	—

Example

The following command configures a redirect URL. Use the **show block-redirect-url** command to view the configured redirect URLs.

```
(host) [mynode] (config) #block-redirect url https://www.redirectURL.com
```

Related Command

Command	Description
`show ap block-redirect-url`	Shows the redirect URL for blocked content

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

boot

```
boot
   cf-test [fast|read-only|read-write]
   system partition <partition_id>
   verbose
```

Description

Configure the boot options for the controller.

Syntax

Parameter	Description
`cf-test`	Sets the type of compact flash test to run when booting the controller.
`fast`	Performs a fast test, which does not include media testing.
`read-only`	Performs a read-only media test.
`read-write`	Performs a read-write media test.
`system partition {0 | 1}`	Enter **system partition** followed by the partition number (0 or 1) that you want the controller to use during the next boot (login) of the controller. **NOTE:** A controller reload is required before the new boot partition takes effect.
`verbose`	Prints extra debugging information at boot.

Usage Guidelines

Use the following options to control the boot behavior of the controller:

- `cf-test`—Test the flash during boot.
- `system partition`—Specify the system partition to use during the controller's next boot (login).
- `verbose`—Print extra debugging information during boot. The information is sent to the screen at boot time. Printing the extra debugging information is disabled using the `no boot verbose` command.

Example

The following command uses system partition 1 the next time the controller boots:

```
(host) [mynode] #boot system partition 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config and Enable mode on Mobility Master.

bulkedit import csv

```
bulkedit import csv <csv-name>
```

Description

Use the **bulkedit import csv** command to import data from a .csv file.

Syntax

Parameter	Description
`bulkedit import csv`	Imports data from a .csv file.
`<csv-name>`	Name of the .csv file

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config modes on the managed device or the Mobility Master

ccm-debug

```
ccm-debug
   config-rollback node <node-path> config-id <cfg-id>
   full-config-sync
```

Description

Use the **ccm-debug config-rollback** command to roll back the configuration of a node to the previous version.

Use the **ccm-debug full config sync** command to request a full configuration sync.

Syntax

Parameter	Description
`config-rollback`	Rolls back to the previous configuration.
`node <node>`	Specifies the configuration node.
`config-id <cfg-id>`	Specifies the configuration ID (full path name of the config node) to roll back to.
`full-config-sync`	Request for a full config sync.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on the managed device or the Mobility Master

cellular profile

```
cellular profile <name>
   dialer <group>
   driver {acm|hso|option|sierra|ptumlusbnet|netgear-341|netgear-340}
   import <address>
   modeswitch {eject <params>}|rezero|{usb-modeswitch <usb-param>}
   no
   priority <prior>
   serial <sernum>
   tty <ttyport>
   user <login> password <password>
   vendor <vend_id> product <prod_id>
```

Description

Create new profiles to support new USB modems or to customize USB characteristics.

Syntax

Parameter	Description
`cellular profile <name>`	Enter the keywords **cellular profile**, followed by your profile name. This command changes the configuration mode and the command line prompt changes to: `(host) [mynode] (config-cellular <profile_name>)#`
`dialer <group>`	Enter the keyword **dialer**, followed by a group name to specify the dialing parameters for the carrier. The parameters tend to be common between service providers on the same type of network (CDMA vs. GSM) as displayed in the show dialer group command.
`driver {acm|hso|option|sierra| ptumlusbnet|netgear-341|netgear-340}`	Enter the keyword **driver**, followed by a driver option to select the driver type: ■ **acm**: Linux ACM driver. ■ **hso**: Option High Speed driver. ■ **option**: Option USB data card driver (default). ■ **sierra**: Sierra Wireless driver. ■ **ptumlusbnet**: Pantech UML290 driver. ■ **netgear-341**: NETGEAR AirCard 341U USB modem. ■ **netgear-340**: NETGEAR AirCard 340U USB modem.

Parameter	Description
`import <address>`	Enter the keyword **import**, followed by the USB device address as displayed in the show usb command. **Import** retrieves the vendor or product serial numbers from the USB device list and populates them into the profile.
`modeswitch {eject <eject-param>} |rezero|{usb-modeswitch <usb-param>}`	Enter the keyword **modeswitch**, followed by a modswitch option: ■ **eject**: Ejects a device. This parameter must be followed by the name of the CDROM device. ■ **rezero**: Sends the SCSI CDROM rezero command. ■ **usb-modeswitch**: Switches modes for a USB device. **Modeswith** allows you to modify device modeswitch settings. Certain cellular devices must be modeswitched before the modem switches to data mode.
`no`	Enter the keyword **no** to negate the command and revert back to the default settings.
`priority <prior>`	Enter the keyword **priority** to override the default cellular priority (100). Range: 1 to 255. Default: 100
`serial <sernum>`	Enter the keyword **serial**, followed by the USB device serial number
`tty <ttyport>`	Enter the keyword **tty**, followed by the Modem TTY port (i.e. ttyUSB0, ttyACM0)
`user <login> password <password>`	Enter the keyword **user**, followed by your login, and then enter the keyword **password** followed by your password to establish user name authentication.
`vendor <vend_id> product <prod_id>`	Enter the keyword **vendor**, followed by the vendor ID in hexadecimal (see show usb on page 2292) and then enter the keyword **product**, followed by the product ID listed in the show usb command.

Usage Guidelines

The cellular modems are plug-and-play and support most native USB modems. Cellular modems are activated only if it is the uplink with the highest priority (see show uplink on page 2290). However, new profiles can be created using this command to support new data cards or to customize card characteristics. A list of supported modems is published at http://www.arubanetworks.com/products/usb-devices/.

Related Commands

Command	Description
show cellular profile	Displays each cellular profile and the corresponding profile settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

cfgm

```
cfgm {set config-chunk <size>|set heartbeat <time>|set timeout <time>|set vpnconnect_retry
<retry num>}
```

Description

This command configures the configuration module on Mobility Master.

Syntax

Parameter	Description	Range	Default
`set config-chunk`	Maximum packet size, in Kilobytes, that is sent every second to a managed device whenever a configuration is sent to that node. If the connection between the Mobility Master and managed device is slow or uneven, you can lower the size to reduce the amount of data that must be retransmitted. If the connection is very fast and stable, you can increase the size to make the transmission more efficient.	1-100	10 Kbytes
`set heartbeat`	Interval, in seconds, at which heartbeats are sent. You can increase the interval to reduce traffic load.	10-300	10 seconds
`set timeout`	Time, in seconds, of socket Rx inactivity before reconnecting with Mobility Master.	20-200	120 seconds

Example

The following command sets the maximum packet size as 20 KB per second whenever a configuration is sent to the managed device:

```
(host) [mm] (config) #cfgm set config-chunk 20
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **set timeout** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

change-config-node

```
change-config-node <node-path>
```

Description

This command changes the current CLI node context to the specified node. The desired node is specified by the node-path, which can be an absolute path from the root node or relative path from the current node.

Syntax

Parameter	Description
`<node-path>`	Path of the configuration node.

Usage Guidelines

Use the **show configuration node-hierarchy** command to view the list of all nodes in the configuration hierarchy.

Example

The following command changes the current node-path (**/mm/mynode**) to **/md**:

```
(host) [mynode] #change-config-node /md
(host) [md] #
```

Related Commands

Command	Description
`cd`	Changes the working node to the specified path.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

clear

```
clear
   aaa
   acl
   airgroup
   amon-receiver
   amon-sender
   ap
   arp
   counters
   crypto
   datapath
   dot1x
   fault
   gap-db
   gsm
   ifmap
   ip
   ipc
   ipv6
   lc-cluster
   lldp
   loginsession
   master-local
   master-local-entry
   master-local-session
   mon-serv
   mon-serv-fwv
   openflow
   openflow-controller
   pan
   perf-test
   phonehome
   port
   port-security-error
   provisioning-ap-list
   provisioning-params
   rap-wml
   ucc
   update-counter
   vpdn
   web-cc
   websocket
   whitelist-db
   wms
```

Description

This command clears various user-configured values from your running configuration.

Syntax

Parameter	Description
`aaa`	Clear all values associated with authentication profile.

Parameter	Description
`auth-survivability-cache`	Clear all auth survivability cached data. Parameters: ■ **all**—Clear all entries in the auth survivability cache. ■ **station**—Clear an entry in the auth survivability cache for station.
`authentication-server`	Provide authentication server details to clear values specific to an authentication server or all authentication server. Parameters: ■ **all**—Clear all server statistics. ■ **internal**—Clear Internal server statistics. ■ **ldap**—Clear LDAP server statistics. ■ **radius**—Clear RADIUS server statistics. ■ **tacacs**—Clear TACACS server statistics.
`device-id-cache`	Clear all device ID cache. Parameters: ■ **all**—Clear all entries in the device ID cache. ■ **mac**—Clear entries in the device ID cache for MAC address.
`load-balance|statistics`	Clear load balance statistics. Parameters: ■ **server group**—Clear load balance statistics of a server group.
`multiple-server-accounting|statistics`	Clear multiple server accounting statistics. Parameters: ■ **all**—Clear for all server groups. ■ **server-group**—Clear multiple server accounting statistics for a server group.
`state`	Clear internal status of authentication modules. Parameters: ■ **configuration**—Clear all configured objects. ■ **debug-statistics**—Clear debug statistics. ■ **messages**—Clear authentication messages that were sent and received.
`acl`	Clear ACL statistics.
`hits`	Clear ACL hit statistics.
`airgroup`	Clear AirGroup statistics and user entries from the user table.
`cli-policy all`	Clears AirGroup policies except ClearPass Policy Manager policies.
`server`	Clears AirGroup servers.

Parameter	Description
statistics	■ **blocked-queries**—Clears the statistics of service IDs which were queried but not available in the AirGroup service table. ■ **blocked-service-id**—Clears the statistics for the list of blocked services. ■ **cppm-entries**—Clears the statistics that are displayed for **show airgroup cppm entries** command. ■ **internal-state**—Clears internal state statistics of mDNS module. ■ **multi-controller**—Clears the statistics maintained for multi-controller message exchanges. ■ **query**—Clears statistics maintained in the user and server table. ■ **service**—Clears statistics maintained in the AirGroup service table.
user	■ **Mac Address**—Clears the AirGroup server Mac addresses. ■ **dlna**—Clears the AirGroup DLNA users. ■ **mdns**—Clears the AirGroup mDNS users. ■ **all**—Removes the current AirGroup user entries from the user table.
ap	Clear all AP related information.
arm bandwidth-management	Clears AP bandwidth management table counters. An AP can be specified by ap-name, BSSID, IPv4 address, or IPv6 address.
arm client-match	**rules file-name <file-name>** —Clears an imported file of ClientMatch rules. **summary**—Clears the ClientMatch summary information **unsupported**—Clears the MAC address of an unsteerable client or clients.
crash-info	Clears AP crash information. An AP can be specified by ap-name, IPv4 address, or IPv6 address.

Parameter	Description
debug	■ **bss-dmo-stats**— Clears DMO debug statistics from a specific BSSID of an AP. ■ **classification-counters**—Clears classification counters. ■ **client-stats**— Clears statistics from a client. ■ **dot11r {efficiency-stat}**— Clears 802.11r-related stats. ■ **lacp**—Clears transmitted and received packet counters displayed in the **show ap debug lacp** command. ■ **lldp**—Clears LLDP for an AP. **counters**—Clears LLDP statistics. ■ **openflow**— Clears openflow statistics. ■ **radio-stats**— Clears aggregate radio debug statistics of an AP. ■ **sta-msg-stats**—Clear AP-STM to STM message statistics.
mesh	Clear all mesh commands. ■ **debug**—Clears debug information. **counters**—Clears statistics for a mesh node.
port {ap-name | serial-num | wired-mac} <port>	Toggle the link on the specified port. **ap-name**—Clear specified port on AP with this name. **serial-num**—Clear specified port on AP with this serial number. ■ **wired-mac**—Clear specified port on AP at this MAC address.
remote flash-config	Clears the flash configuration from a specified AP. An AP can be specified by ap-name, BSSID, IPv4 address, or IPv6 address.
arm	Clear the following types of ARM ClientMatch information: ■ client-match-summary ■ client-match-unsteerable
arp	Clear all ARP table information. You can either clear all information or enter the IP address of the ARP entry to clear a specific value.
counters	Clear all interface configuration values.
gigabitethernet	Clears configuration related to gigabitethernet ports.
port-channel <id>	Clears statistics related to a port-channel. Port-channel ID ranges from 0 to 7.
tunnel	Clears all tunnel configuration values on interface ports.

Parameter	Description
`vrrp [ipv6]`	Clears all VRRP configuration values on interface ports. Include the ipv6 parameter to clear IPv6 counters.
`crypto`	Clears the specified crypto information.
`dp`	Clears crypto latest DP packets.
`ipsec sa [peer [[<ip-address>] [v6 <ipv6-address>]]]`	Clears crypto IPsec state SAs for the following: ■ **peer**—state for a peer ■ **v6**—state for an ipv6 peer
`isakmp sa [peer [[<source-ip>] [v6 <source-ipv6>]]]`	Clears crypto isakmp state SAs for the following: ■ **peer**—state for a peer ■ **v6**—state for an ipv6 peer
`stats`	Clears crypto statistics.
`datapath`	Clears all configuration values and statistics for the following datapath modules. ■ **application {counters}** ■ **bridge {counters}** ■ **bwm {counters}** ■ **compression {counters}** ■ **cp-bwm {counters}** ■ **crypto {counters}** ■ **debug {performance}** ■ **dma {counters}** ■ **eap {counters}** ■ **frame {counters}** ■ **hardware {counters|statistics}** ■ **ip-fragment-table {ipv4|ipv6}** ■ **ip-reassembly {counters}** ■ **maintenance {counters}** ■ **message-queue {counters}** ■ **mobility {stats}** ■ **network {egress|ingress}** ■ **papi {counters|remote-device-table}** ■ **route {counters}** ■ **route-cache {A.B.C.D|counters}** ■ **scheduler {counters}** ■ **session {dpi|counters}** ■ **ssl {counters}** ■ **station {counters}** ■ **tcp {counters}** ■ **tunnel {counters}** ■ **user {counters}** ■ **wan-hc {counters}** ■ **web-cc {counters}** ■ **wifi-reassembly {counters}** ■ **wmm {counters}**

Parameter	Description
`dot1x`	Clears all 802.1X-specific counters and supplicant statistics. Use the following parameters: ■ **counters** ■ **supplicant-info**
`fault`	Clears all SNMP fault configuration.
`gap-db`	Clears global AP database. This command is often used to clear all stale AP records. Use the following parameters: ■ **ap-name** ■ **lms** ■ **wired-mac**
`gsm`	Clear GSM statistics.
`ifmap`	Clear IF-MAP connection.
`ip`	Clears all IP information from DHCP bindings, IGMP groups and IP mobility configuration. Use the following parameters: ■ **dhcp** ■ **igmp {cluster|group|mobility-group|stats-counters}** ■ **mobile {host|multicast-vlan-table|traffic|trail}** ■ **probe {stats}**
`ipc|statistics`	Clears all inter process communication statistics. Use the following parameters: ■ **app-ap** ■ **app-id** ■ **app-name**
`app-ap`	Clears the statistics related to the following AP commands: ■ **am** ■ **ofald** ■ **sapd** ■ **stm**
`app-id`	Clears the statistics related to an application id.

Parameter	Description
app-name	Clears statistics application name related statistics: ■ **aaa** ■ **ads** ■ **auth-resp** ■ **authmgr** ■ **certmgr** ■ **cfgm** ■ **cluster_mgr** ■ **cpsec** ■ **cts** ■ **dbsync** ■ **dds** ■ **dhcp** ■ **esi** ■ **extifmgr** ■ **fpapps** ■ **gsmmgr** ■ **httpd** ■ **ike** ■ **ip_flow_export** ■ **l2tp L2TP** ■ **licensemgr** ■ **mdns** ■ **mobileip** ■ **ntp** ■ **ofa** ■ **ospf** ■ **phonehome** ■ **pim** ■ **pktfilter** ■ **pptp** ■ **profmgr** ■ **publisher** ■ **resolver** ■ **sapm** ■ **sapm-resp** ■ **snmpt** ■ **stm** ■ **stm-lopri** ■ **syslogd** ■ **ucm** ■ **userdb** ■ **web_cc** ■ **wms**
ipv6	Clears all IPv6 session statistics, MLD group and member information, MLD statistics, counters, and DHCPv6 binding information. Use the following parameters: ■ **datapath {session} counters** ■ **dhcp {binding}** ■ **mld {cluster <stats>|group|proxy-mobility-group|information|stats-counters}** ■ **neighbor {all|ipv6}**

Parameter	Description
`lc-cluster`	Clear cluster status.
`gsm counters`	Clear GSM counter information for that cluster.
`papi counters`	Clear PAPI counter information for that cluster.
`vlan-probe counters`	Clear vlan-probe counters for that cluster.
`lldp`	Clears LLDP information on all the interfaces. Use the following parameters: ■ **neighbors {interface gigabitethernet |fastethernet slot/module/port}** ■ **statistics {interface gigabitethernet |fastethernet slot/module/port}**
`loginsession`	Clears loginsession information for a specific login session, as identified by the session id.
`master-local`	Clears all master-local switch statistics.
`stats`	Clears the statistics of local or all switches connected to the Mobility Master or managed devices. Use the following sub-parameters: ■ **all**— Clears the statistics of all the managed devices. ■ **ip {ipv4-address | ipv6-address}**— Clears the statistics of IPv4 address or IPv6 address of the switch. ■ **local-stats**— Clears the master-local statistics at the managed device.
`master-local-entry`	Clears managed device information from the Mobility Master LMS list. Specify the IP address of the managed device to be removed from the Mobility Master active LMS list.
`master-local-session`	Clear and reset master local TCP connection. Specify the IP address of either the Mobility Master or managed device.
`mon-serv`	Clears all monitoring server statistics. Use the following parameters: ■ **ap-microboot-stats** — Clears the AP micro-bootstrapping statistics. ■ **message-stats** — Clears the monitoring and Advanced Monitoring (AMON) message statistics. ■ **microboot-stats-all** — Clears all micro-bootstrapping statistics. ■ **radio-microboot-stats** — Clears Radio micro-bootstrapping statistics. ■ **sta-microboot-stats** — Clears STA micro-bootstrapping statistics. ■ **vap-microboot-stats** — Clears VAP micro-bootstrapping statistics.

Parameter	Description
`mon-serv-fwv`	Clears all monitoring server statistics. Use the following parameters: ■ **apprf-pool-counters** — Clears AppRF Pool counters. ■ **message-stats** — Clears the monitoring and Advanced Monitoring (AMON) message statistics.
`openflow`	Clear openflow statistics.
`openflow-controller`	Clear openflow statistics of the controller.
`pan`	Clear Palo Alto Networks interface.
`perf-test`	Clear Iperf throughput test process.
`reports`	Displays Iperf throughput test reports. Use the following parameters: ■ **ap {ap-name | ip-addr| ip6-addr}**— All Iperf throughput test on the access point. ■ **controller** — All Iperf throughput test on the controller.
`phonehome`	Resets phonehome stats.
`port`	Clear all port statistics that includes link-event counters or all counters. Use the following parameters: ■ **link-event** ■ **stats**
`port-security-error gigabitethernet`	Clear all port-security-error counters. Use the following parameters: ■ **slot** ■ **module** ■ **port**
`provisioning-params`	Clear provisioning parameters and reset them to the default configuration values.
`rap-wml`	Clear wired MAC lookup cache for a DB server.
`ucc`	Clear UCC state information.
`client ip <ipaddr>`	Clear the UCC counter for a client.
`sessions ip <ipaddr>`	Clear active UCC sessions based on a specific client IP address.
`statistics counter call {client|global}`	Clear UCC call statistics based on particular client or system wide.
`update-counter`	Clear all update counter statistics.

Parameter	Description
vpdn	Clear all VPDN configuration for L2TP and PPTP tunnel. Use the following parameters: ■ **tunnel l2tp id <l2tp-tunnel-id>** ■ **tunnel pptp id <pptp-tunnel-id>**
web-cc	Clear all web content classification information.
web-cc cache <MD5-1>	Clear web content category URLs from the datapath cache by specifying the two MD5 values of the URL to be removed from the cache. To view all entries in the datapath, and the MD5 values for each entry, issue the command **show datapath web-cc**.
web-cc stats	Clear all web content classification statistics. To view current statistics information, issue the command **show web-cc stats**.
web-cc md	Clear all web content classification managed nodes. Use the following parameter: ■ **stats** — Clears all web content classification statistics.
websocket	Clear Web-Socket Interface statistics.
whitelist-db	Clear whitelist statistics. Use the following parameter: ■ **cpsec—stats** — Clear CPsec whitelist statistics.
wms	Clear all WLAN management commands. Use the following parameters: ■ **ap** — All AP related commands. Specify the BSSID of the AP. ■ **client** — Clear all wired client related commands. Specify the MAC address of the client. ■ **event** — Clears all events. Parameters: **database-id** — Clear a single event with database id. **event-type** — Clear all events with type. **target-mac** — Clear all events assigned to a target MAC. ■ **probe** — Clear all probe information. Specify the BSSID of the probe.
ap	Clear AP information.
client	Clear client information.
event	Clear event information.
probe	Clear probe information.

Parameter	Description
`wired-mac`	Clear learned and collected wired-mac information: **all** — Clear all learned and collected wired mac information. **gw-mac** — Clear gateway wired mac information collected from APs. **monitored-ap-wm** — Clear monitored AP wired mac information collected from APs. **prop-eth-mac** — Clear wired mac information collected from APs. **reg-ap-oui** — Clear registered AP OUI information collected from APs. **system-gw-mac** — Clear system gateway mac information learned at the controller . **system-wired-mac** — Clear system wired mac information learned at the controller. **wireless-device** — Clear routers or potential wireless devices information.

Usage Guidelines

The clear command clears the specified parameters of their current values.

Example

The following command clears all aaa counters for all authentication servers:

```
(host) [mynode] #clear aaa authentication-server all
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The **<port>** sub-parameter was added to the port parameter.
ArubaOS 8.2.0.0	The following parameters were added: ■ **master-local** ■ **mon-serv** ■ **mon-serv-fwv** ■ **perf-test** ■ **web-cc md**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

clear aaa auth-survivability-cache

```
clear aaa auth-survivability-cache
```

Description

This command allows you to clear the data that is currently in the local Survival Server cache.

Usage Guidelines

The **clear...cache** parameter has two sub-parameters:

- **all**: Clears all entries in the Authentication Survivability Cache.
- **station**: Clears the entry in the Authentication Survivability Cache for a particular station. Specify the station with its MAC address in *A:B:C:D:E:F* format.

Example

To clear the Auth-Survivability cache:

```
(host) [mynode] (config) #clear aaa auth-survivability-cache <all> | <station MAC_address>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

clear amon-receiver

```
show amon-receiver [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-stats-inst-1] | [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] | [dest-stats-inst-5] | [dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] | [error-counters] | [error-counters-all] | [interest-table] | [list-details] | [parameter] | [set-debug-level-dest] | [src-stats-all] | [stats-counters] | [stats-counters-all]]
```

Description

This command displays AMON receiver information.

Syntax

Parameter	Description
`dest-stats-inst-0`	Clears destination statistics instance 0
`dest-stats-inst-1`	Clears destination statistics instance 1
`dest-stats-inst-2`	Clears destination statistics instance 2
`dest-stats-inst-3`	Clears destination statistics instance 3
`dest-stats-inst-4`	Clears destination statistics instance 4
`dest-stats-inst-5`	Clears destination statistics instance 5
`dest-stats-inst-6`	Clears destination statistics instance 6
`dest-stats-inst-7`	Clears destination statistics instance 7
`error-counters`	Clears error counters
`src-stats-counters`	Clears stats counters for a particular source
`stats-counters`	Clears stats counters
`stats-counters-all`	Clears all stats counters

Example

The following command displays AMON receiver information for destination statistics instance 0:

```
(host) [mynode] #clear amon-receiver dest-stats-inst-0
Clear Amon Receiver Stats
-----------------
AMON-RECEIVER
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

clear amon-sender

```
show amon-sender [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-stats-inst-1]
| [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] | [dest-stats-inst-5] |
[dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] | [error-counters] | [error-counters-
all] | [interest-table] | [list-details] | [parameter] | [set-debug-level-dest] | [src-stats-
all] | [stats-counters] | [stats-counters-all]]
```

Description

This command displays AMON sender information. This command must be issued on the managed device.

Syntax

Parameter	Description
`dest-stats-inst-0`	Clears destination statistics instance 0
`dest-stats-inst-1`	Clears destination statistics instance 1
`dest-stats-inst-2`	Clears destination statistics instance 2
`dest-stats-inst-3`	Clears destination statistics instance 3
`dest-stats-inst-4`	Clears destination statistics instance 4
`dest-stats-inst-5`	Clears destination statistics instance 5
`dest-stats-inst-6`	Clears destination statistics instance 6
`dest-stats-inst-7`	Clears destination statistics instance 7
`error-counters`	Clears error counters
`src-stats-counters`	Clears stats counters for a particular source
`stats-counters`	Clears stats counters
`stats-counters-all`	Clears all stats counters

Example

The following command displays AMON sender information for destination statistics instance 0:

```
(host) [mynode] #logon 192.0.1.12
(MN-7240) #clear amon-sender dest-stats-inst-0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

clear wms wired-mac

```
clear wms wired-mac [ all | gw-mac <mac> | monitored-ap-wm <mac> | prop-eth-mac <mac> | reg-ap-oui <mac> | system-gw-mac <mac>| system-wired-mac <mac> | wireless-device <mac>]
```

Description

Clear *learned* and *collected* Wired MAC information. Optionally, enter the MAC address, in nn:nn:nn:nn:nn:nn format, of the AP that has seen the Wired Mac.

Syntax

Parameter	Description
`all`	Clear all the learned and collected wired Mac information.
`gw-mac <mac>`	Clear the gateway wired Mac information collected from the APs.
`monitored-ap-wm <mac>`	Clear monitored AP wired Mac information collected fom the APs.
`prop-eth-mac <mac>`	Clear the wired Mac information collected from the APs.
`reg-ap-oui <mac>`	Clear the registered AP OUI information collected from the APs.
`system-gw-mac <mac>`	Clear system gateway Mac information learned at the controller.
`system-wired-mac <mac>`	Clear system wired Mac information learned at the controller.
`wireless-device <mac>]`	Clear routers or potential wireless devices information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licens	Command Mode
All platforms	Base operating system.	Config and Enable mode on Mobility Master.

clock cli-timestamp

```
clock cli-timestamp
```

Description

This command enables the timestamp feature, adding a date and time to the output of **show** commands.

Syntax

No parameters.

Usage Guidelines

When you enable the timestamp feature, the CLI includes a timestamp in the output of each show command indicating when the show command was issued. Note that the output of **show clock** and **show log** commands do not include timestamps, even when this feature is enabled. You can disable timestamps using the command **no clock cli-timestamp**.

Example

The following example enables the timestamp feature.

```
(host)[mynode](config) #clock cli-timestamp
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

clock set

```
clock set <year> <month> <day> <time>
```

Description

This command sets the date and time.

Syntax

Parameter	Description	Range
`clock set`	Sets the time and date.	—
`<year>`	Sets the year. Requires all 4 digits.	Numeric
`<month>`	Sets the month. Give the complete month name.	january-december
`<day>`	Sets the day.	1–31
`time`	Sets the time. Specify hours, minutes, and seconds separated by spaces.	0–23 for hours 1–60 for minutes 1–60 for seconds

Usage Guidelines

You can configure the year, month, day, and time. You must configure all four parameters.

Specify the time using a 24-hour clock. You must specify the seconds.

Example

The following example configures the clock to January 1, 2017, at 16:22:52.

```
(host)[mynode] #clock set 2017 january 1 16 22 52
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode or Config mode on Mobility Master

clock summer-time recurring

```
clock summer-time <WORD> recurring
   <1-4> <start day> <start month> <hh:mm>
   first <start day> <start month> <hh:mm>
   last <start day> <start month> <hh:mm>
   <1-4> <end day> <end month> <hh:mm>
   first <end day> <end month> <hh:mm>
   last <end day> <end month> <hh:mm>
```

Description

This command sets the software clock to begin and end daylight savings time on a recurring basis.

Syntax

Parameter	Description	Range
`<WORD>`	Abbreviation for your time zone. For example, PDT for Pacific Daylight Time.	3-5 characters
`<1-4>`	Enter the week number to start and end daylight savings time. For example, enter 2 to start daylight savings time on the second week of the month.	1-4
`first`	Enter the keyword **first** to have the time change begin or end on the first week of the month.	—
`last`	Enter the keyword **last** to have the time change begin or end on the last week of the month.	—
`<start day>`	Enter the weekday when the time change begins or ends.	Sunday-Saturday
`<start month>`	Enter the month when the time change begins or ends.	January-December
`<hh:mm>`	Enter the time, in hours and minutes, that the time change begins or ends.	24 hours

Usage Guidelines

This command subtracts exactly 1 hour from the configured time.

The **WORD** can be any alphanumeric string, but cannot start with a colon (:). A **WORD** longer than five characters is not accepted. If you enter a **WORD** containing punctuations, the command is accepted, but the timezone is set to UTC.

You can configure the time to change on a recurring basis. To do so, set the week, day, month, and time when the change takes effect (daylight savings time starts). You must also set the week, day, month, and time when the time changes back (daylight savings time ends).

The **start day** requires the first three letters of the day. The **start month** requires the first three letters of the month.

You also have the option to set the number of hours by which to offset the clock from UTC. This has the same effect as the clock timezone command.

Example

The following example sets daylight savings time to occur starting at 2:00 AM on Sunday in the second week of March, and ending at 2:00 AM on Sunday in the first week of November. The example also sets the name of the time zone to PST with an offset of UTC - 8 hours.

```
(host) [mynode] (config) #clock summer-time PST recurring 2 Sun Mar 2:00 first Sun Nov 3:00 -8
```

Related Commands

Command	Description
show clock	Displays the system clock, configured for daylight savings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

clock timezone

```
clock timezone <name>
```

Description

This command sets the timezone on a controller.

Syntax

Parameter	Description	Range
`<name>`	Name of the timezone.	3-5 characters

Usage Guidelines

The **name** parameter can be any alphanumeric string, but cannot start with a colon (:). A time zone name longer than five characters is not accepted. If you enter a time zone name containing punctuation, the command is accepted, but the time zone is set to UTC.

Example

The following example configures the timezone to PST.

```
(host) [mynode] (config) #clock timezone PST
```

Related Commands

Command	Description
show clock	Displays the system clock under the configured timezone.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

cluster-debug

```
cluster-debug
   bucketmap essid <essid_name> bucketindex <buck_idx> active <active_uac_idx> standby
   <standby_uac_idx>
   standby-aac reassign [[active-aac-ip] <active_aac> [active-aac-ip6]] <active_aac_v6>
   [[standby-aac-ip] [standby-aac-ip6]] <new_standby_aac> <new_standby_aac_v6> [ap-group] <ap-
   group> [ap-mac] <ap-mac>
   calc-sta-uac <sta_mac> <essid_name>
```

Description

This command sets are used to change the bucketmap entries and to reassign the standby AAC. However, changing the bucketmap entries is not recommended by Aruba.

Syntax

Parameter	Description
`bucketmap`	Bucket map.
`essid <essid_name>`	Essid name.
`Bucketindex`	Index within bucket map. The valid range of values for index is <0-255>.
`active`	Index of UAC in bucket map's UAC List. The valid range of values for index is <0-11>.
`standby-uac`	Standby UAC . Index of UAC in bucket map's UAC List or -1 if no standby desired. The valid range of values for index is <0-11>.
`calc-sta-uac`	Calculate station UAC and index by using bucketmap in GSM channel.
`<sta_mac>`	Enter the station MAC Address.
`<essid_name>`	Enter the Essid name.
`standby-aac`	Standby AAC.
`reassign`	Reassign Standby AAC.
`active-aac-ip <active_aac>`	Active AAC IP Address. Enter the IP address of Active AAC. Use the following parameters: ■ **standby-aac-ip <new_standby_aac>**: Enter the IP Address of new standby AAC. ■ **standby-aac-ip6 <new_standby_aac_v6>** : Enter the IPv6 Address of new standby AAC.
`active-aac-ip6 <active_aac_v6>`	Active AAC IPv6 Address. Enter the IPv6 address of Active AAC.

Parameter	Description
`ap-group <ap-group>`	Enter the AP Group name. Use the following parameters: ■ **active-aac-ip <active_aac>**: Enter the IP Address of active AAC. ■ **active-aac-ip6 <active_aac_v6>**: Enter the IPv6 Address of active AAC. ■ **standby-aac-ip <new_standby_aac>**: Enter the IP Address of new standby AAC. ■ **standby-aac-ip6 <new_standby_aac_v6>**: Enter the IPv6 Address of new standby AAC.
`ap-mac <ap_mac>`	Enter the AP Mac Address.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **calc-sta-uac** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on managed devices.

cluster-member-custom-cert

```
cluster-member-custom-cert member-mac <mac> ca-cert <ca> server-cert <cert>
   suite-b <gcm-128 | gcm-256>]
```

Description

This command sets the managed device as a CPsec cluster root, and specifies a custom user-installed certificate for authenticating cluster members.

Syntax

Parameter	Description
`member-mac <ca>`	MAC address of the cluster member.
`ca-cert <ca>`	Name of the CA certificate uploaded via the WebUI.
`ca-cert <ca>`	Name of the CA certificate uploaded via the WebUI.
`server-cert <cert>`	Name of the server certificate uploaded via the WebUI.
`suite-b`	To use Suite-B encryption in the secure communication between the cluster root and cluster member, specify one of the following Suite-B algorithms: ■ **gcm-128**: Encryption using 128-bit AES-GCM ■ **gcm-256**: Encryption using 256-but AES-GCM

Usage Guidelines

If your network includes multiple Mobility Master each with their own hierarchy of APs and managed device, you can allow APs from one hierarchy to failover to any other hierarchy by defining a cluster of Mobility Master. Each cluster will have one Mobility Master as its cluster root, and all other managed devices as cluster members.

To define a managed device as a cluster root, issue one of the following commands on that managed device:

- cluster-member-custom-cert: Define the Mobility Master as a cluster root, and select a user-installed certificate to authenticate that cluster member.
- cluster-member-factory-cert: Define the Mobility Master as a cluster root, and select a factory-installed certificate to authenticate that cluster member.
- cluster-member-ip : Define the Mobility Master as a cluster root, and set the IPsec key to authenticate that cluster member.

For information on installing certificates on your controller, refer to the *Management Utilities* chapter of the *ArubaOS User Guide*.

Example

The following example selects a customer installed certificate for cluster member authentication.

```
(host)(config) # cluster-member-custom-cert member-mac 00:1E:37:CB:D4:52 ca-cert cacert1
server-cert servercert1
```

Related Commands

Parameter	Description	Mode
control-plane-security	Configure the CPsec profile.	Config mode
show cluster-config	Show the multi-master cluster configuration for the CPsec feature.	Enable mode
show cluster-switches	Issue this command on a Mobility Master using CPsec in a multi-master environment to show other managed devicesto which it is connected.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on managed devices.

cluster-member-factory-cert

```
cluster-member-factory-cert member-mac <mac>
```

Description

This command sets the managed device as a CPsec cluster root, and specifies a custom user-installed certificate for authenticating cluster members.

Syntax

Parameter	Description
`<mac>`	MAC address of the user-installed certificate on the cluster member.

Usage Guidelines

To define a controller as a cluster root, issue one of the following commands on that controller:

- cluster-member-custom-cert: Define the managed device as a cluster root, and select a user-installed certificate to authenticate that cluster member.
- cluster-member-factory-cert: Define the managed device as a cluster root, and select a factory-installed certificate to authenticate that cluster member.
- cluster-member-ip : Define the Managed device as a cluster root, and set the IPsec key to authenticate that cluster member.

For information on installing certificates on your controller, refer to the *Management Utilities* chapter of the *ArubaOS User Guide*.

Example

The following command sets the managed device on which you issue command as a root managed device, and adds the managed device **172.21.18.18** as a cluster member with the IPsec key **ipseckey1**:

```
(host) (config) #cluster-member-factory-cert member-mac 00:1E:37:CB:D4:52
```

Related Commands

Parameter	Description	Mode
control-plane-security	Configure the CPsec profile.	Config mode
show cluster-config	Show the multi-master cluster configuration for the CPsec feature.	Enable mode
show cluster-switches	Issue this command on a Mobility Master using CPsec in a multi-master environment to show other managed devices to which it is connected.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on managed devices.

cluster-member-ip

```
cluster-member-ip <ip-address>
   ipsec <key>
```

Description

This command sets the Mobility Master as a CPsec cluster root, and specifies the IPsec key for a cluster member.

Syntax

Parameter	Description
`<ip-address>`	Switch IP address of a CPsec cluster member. You can also use the IP address 0.0.0.0 to set a single IPsec key for all cluster members.
`ipsec <key>`	Configure the value of the IPsec key for secure communication between the cluster root and the specified cluster member. The key must be between 6-64 characters.

Usage Guidelines

The Mobility Master operating as the cluster root will use the CPsec feature to create a self-signed certificate, then certify it's own managed devices and APs. Next, the cluster root will send the certificate to each cluster member, which in turn certifies their own managed devices and APs. Since all managed devices and APs in the cluster get their certificates from the cluster root, they will all have the same trust anchor, and the APs can switch to any other managed device in the cluster and still remain connected to the secure network.

Issue the cluster-member-ip command on the Mobility Master you want to define as the cluster root to set the IPsec key for secure communication between the cluster root and each cluster member. Use the IP address **0.0.0.0** in this command to set a single IPsec key for all member managed devices, or repeat this command as desired to define a different IPsec key for each cluster member.

Once the cluster root has defined an IPsec key for all cluster members, you must access each of the member managed devices and issue the command cluster-root-ip to define the IPsec key for communication to the cluster root.

Example

The following command sets the managed device on which you issue command as a root managed device, and adds the managed device**172.21.18.18** as a cluster member with the IPsec key **ipseckey1**:

```
(host) (config) #cluster-member-ip 172.21.18.18 ipsec ipseckey1
```

Related Commands

Parameter	Description	Mode
control-plane-security	Configure the CPsec profile.	Config mode
show cluster-config	Show the multi-master cluster configuration for the CPsec feature.	Enable mode
show cluster-switches	Issue this command on a Mobility Master using CPsec in a multi-master environment to show other managed devices to which it is connected.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on managed devices.

cluster-root-ip

```
cluster-root-ip <ip-address>
   ipsec <key>
   ipsec-custom-cert root-mac1 <mac1> [root-mac2 <mac2>] ca-cert <ca> server-cert <cert>
   [suite-b <gcm-128 | gcm-256>]
   ipsec-factory-cert root-mac-1 <mac> [root-mac-1 <mac>]
```

Description

This command sets the Mobility Master as a CPsec cluster member, and defines the IPsec key or certificate for secure communication between the cluster member and the Mobility Master's cluster root.

Syntax

Parameter	Description
`<ip-address>`	The IP address of CPsec cluster root Mobility Master. To set a single IPsec key for all member managed devices in the cluster use the IP address **0.0.0.0**.
`ipsec <key>`	Set the value of the IPsec PSK for communication with the cluster root. This parameter must be have the same value as the IPsec key defined for the cluster member via the cluster-member-ip command.
`ipsec-factory-cert`	Use a factory-installed certificate for secure communication between the cluster root and the specified cluster member by specifying the MAC address of the certificate.
`root-mac-1 <mac>`	Specify MAC address of the cluster root.
`ipsec-custom-cert`	Use a custom user-installed certificate for secure communication between the cluster root and the specified cluster member.
`root-mac-1 <mac>`	Specify the MAC address of the cluster-root's certificate.
`root-mac-2 <mac>`	(Optional) If your network has multiple Mobility Master, use this parameter to specify he MAC address of the redundant cluster-root's certificate.
`ca-cert <ca>`	Name of the CA certificate uploaded via the WebUI
`server-cert <cert>`	Name of the server certificate uploaded via the WebUI.
`suite-b`	To use Suite-B encryption in the secure communication between the cluster root and cluster member, specify one of the following Suite-B algorithms ■ **gcm-128**: Encryption using 128-bit AES-GCM ■ **gcm-256**: Encryption using 256-but AES-GCM

Example

The following command defines the IPsec key for communication between the cluster member and the root managed device**172.21.45.22**:

```
(host) [MyNode] (config) #cluster-root-ip 172.21.45.22 ipsec ipseckey1
```

Related Commands

Parameter	Description	Mode
control-plane-security	Configure the CPsec profile.	Config mode
show cluster-config	Show the multi-master cluster configuration for the CPsec feature.	Enable mode
show cluster-switches	Issue this command on a Mobility Master using CPsec in a multi-master environment to show other managed devices to which it is connected.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on managed devices.

cm_mu_client_thresh

```
cm-mu-client-thresh <count>
```

Description

This ClientMatch command configures the client threshold on a multi-user-capable (MU-capable) radio.

Syntax

Parameter	Description	Range	Default
`count`	Total number of clients that can be associated to a radio, in which the radio can still be considered for MU-steering.	—	15

Usage Guidelines

This command is used when MU-capable clients attempt to steer to a MU-capable radio. Clients are not steered to radios that have already met the client threshold, preventing the need for load-balancing.

Example

The following example configures a threshold of 12 clients on a MU-MIMO-capable radio:

```
(host)(config) #cm-mu-client-thresh <12>
```

Command History

Version	Description
ArubaOS 6.4.4.0	The **cm-mu-client-thresh** command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on Mobility Master.

cm_mu_snr_thresh

```
cm-mu-snr-thresh <value>
```

Description

This ClientMatch command configures the Signal to Noise Ratio (SNR) threshold for a multi-user-capable (MU-capable) radio.

Syntax

Parameter	Description	Range	Default
`value <dB>`	Minimum SNR value of a client on the target radio, in which the radio can still be considered for MU-steering.	> 25	30

Usage Guidelines

The **cm-mu-snr-thresh** value must be greater than the **cm-sticky-snr** value for a MU-capable client to be steered to that radio.

Example

The following example configures an SNR threshold of 90 on a MU-MIMO-capable radio:

```
(host)(config) #cm-mu-snr-thresh <90>
```

Command History

Version	Description
ArubaOS 8.0.0.0	The **cm-mu-snr-thresh** command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system, except for noted parameters	Config mode on Mobility Master.

configuration device

```
configuration device
   default-node <node-path>
   <mac-address> device-model
   {A7005|A7008|A7010|A7024|A7030|A7205|A7210|A7220|A7240|A7240XM|A7280|MC-VA} [<config-path>]
   |move-to[<dest-path>][<mac-address-2>]
```

Description

This command maps a device to an existing node in the configuration hierarchy.

Syntax

Parameter	Description
`default-node <node-path>`	Specifies the node to which any device without explicit device-node mapping is attached. If a default node is not configured, unknown devices cannot connect to Mobility Master.
`<mac-address>`	MAC address of a device that must be mapped to a node in the configuration hierarchy.
`device-model`	Model number for the device: ■ A7005 ■ A7008 ■ A7010 ■ A7024 ■ A7030 ■ A7205 ■ A7210 ■ A7220 ■ A7240 ■ A7240XM ■ A7280 ■ MC-VA
`<config-path>`	Full configuration path to which the device is mapped. If the path is not specified, the device is mapped to the current node.
`move-to <dest-path>`	Moves the device to the specified configuration path of the destination node.
`<mac-address-2>`	MAC address of the destination node in the configuration hierarchy.

Usage Guidelines

The node to which the device is mapped is specified by the node-path, which can be an absolute path from the root node or relative path from the current node. If the node-path is not specified, the device is mapped to the current node. A device-specific node is created to store the configuration for the device. The node is named using the specified MAC address of the device.
Use the **show configuration devices** command to view the complete list of devices provisioned on your Mobility Master, and the **show configuration node-hierarchy** command to view the list of all nodes in the configuration hierarchy.

Example

The following command specifies **/md** as the default node:

```
(host) [mynode] (config) #configuration device default-node /md
```

Command History

Release	Modification
ArubaOS 8.3.0.0	The **A7280**option was added under the **device-model** parameter.
ArubaOS 8.2.0.0	The **move-to**, **dest-path**, and **mac-address-2** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

configuration node

```
configuration node
   replace-config <filename> [ignore-masterip-config] [<node-path>]
   <node-path>
      clone-from <source-path>
      move-to <dest-path>
```

Description

This command configures nodes in the configuration hierarchy. Node name and location are specified by the node-path, which can be an absolute path from the root node or relative path from the current node.

Syntax

Parameter	Description
`replace-config <filename>`	New configuration file to be applied for the specified node.
`ignore-masterip-config`	(Optional) Ignores any master IP related changes from the specified configuration file.
`<node-path>`	(Optional) Path of the configuration node to which the new configuration is to be applied.
`<node-path>`	Path of the configuration node to be added, removed, or moved.
`clone-from <source-path>`	Copies an existing node's configuration to a new node. The source and destination node names and locations are specified by the source node-path and node-path, respectively.
`move-to <dest-path>`	Moves an existing user-created node in the hierarchy to the specified destination node. System-generated nodes cannot be moved. Ensure the following points while moving a node or device, otherwise the move operation will fail: ■ The node to be moved is a leaf node and does not have any group node or a device node as a child node under it. ■ No configuration is pending on the parent nodes of the child node to be moved. ■ The configuration on the node to be moved is complaint with the configuration in the new ancestor nodes chain.

Usage Guidelines

Use the **show configuration node-hierarchy** command to view the list of all nodes in the configuration hierarchy.

Example

The following command clones the **/md/group2** node-path to the **/md/group1** node:

```
(host) [mynode] (config) #configuration node /md/group1 clone-from /md/group2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **move-to** sub-parameter was introduced under the **<node-path>** parameter.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

configuration purge-pending-config

```
configuration purge-pending-config [<node-path>]
```

Description

This command cleans up any pending configurations on nodes in the configuration hierarchy.

Syntax

Parameter	Description
`<node-path>`	Path of the configuration node to be purged.

Usage Guidelines

Issue this command without the **<node-path**> parameter to purge all pending configurations in the hierarchy. Use the **show configuration node-hierarchy** command to view the list of all nodes in the configuration hierarchy.

Example

The following command cleans up pending configuration on the **/md** node:

```
(host) [mynode] (config) #configuration purge-pending-config /md
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

configuration rename

```
configuration rename
   <old-path>
   <new-path>
```

Description

This command renames a node path to the specified new name.

Syntax

Parameter	Description
`<old-path>`	Name and path of the node to be renamed.
`<new-path>`	Renames the existing node name to the specified name. The node paths of the child nodes under the renamed node are automatically updated.

Usage Guidelines

Use the **show configuration node-hierarchy** command to view the list of all nodes in the configuration hierarchy.

Example

The following command renames the **/md/node1** node-path to the **/md/node2** node:

```
(host) [mynode] (config) #configuration rename /md/node1 /md/node2
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

configure terminal

```
configure terminal
```

Description

This command allows you to enter configuration commands.

Syntax

No parameters.

Usage Guidelines

Upon entering this command, the enable mode prompt changes to:

```
(host) (config) #
To return to enable mode, enter Ctrl-Z or exit.
```

Example

The following command allows you to enter configuration commands:

```
(host) # configure terminal
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

control-plane-security

```
control-plane-security
   auto-cert-allow-all
   auto-cert-allowed-addrs <start> <end>
   auto-cert-allowed-addrs <startv6> <endv6>
   auto-cert-prov
   cpsec-enable
   no
   timer
```

Description

Configure the control plane security profile by identifying APs to receive security certificates.

Syntax

Parameter	Description
`auto-cert-allow-all`	When you issue the **control-plane-security auto-cert-allow-all** command, the managed device sends a certificate to all associated APs when auto certificate provisioning is enabled. When disabled, the managed device sends certificates only to APs whose IP or IPv6 addresses are in the ranges specified by **auto-cert-allowed-addrs**.
`auto-cert-allowed-addrs <start> <end>`	Use this command to define a specific range of AP IP addresses. The managed device sends certificates to the APs in this IP range when auto certificate provisioning is enabled. Identify a range by entering the starting IP address and the ending IP address in the range, separated by a single space. You can repeat this command as many times as necessary to define multiple IP ranges.
`auto-cert-allowed-addrs <startv6> <endv6>`	Use this command to define a specific range of AP IPv6 addresses. The managed device sends certificates to the APs in this IPv6 range when auto certificate provisioning is enabled. Identify a range by entering the starting IPv6 address and the ending IPv6 address in the range, separated by a single space. You can repeat this command as many times as necessary to define multiple IP ranges.
`auto-cert-prov`	Issue this command to enable automatic certificate provisioning. When this feature is enabled, the managed device will attempt to send certificates to associated APs. To disable this feature, use the command **no auto-cert-prov**. Automatic certificate provisioning is disabled by default
`cpsec-enable`	Issue this command to enable control plane security. To disable this feature, use the command **no cpsec-enable**. Control plane security is enabled by default.
`no`	Negates any configured parameter.

Parameter	Description
`timer <timer>`	Timer value, in dd:hh (days:hours) format, that prevents APs from going into **unapproved-no-cert state** when the APs remain idle for two or more hours. The minimum value of hours in dd:hh format is 2 hours.

Usage Guidelines

The managed devices enabled with control plane security only send certificates to APs that you have identified as valid APs on the network. If you are confident that all campus APs currently on your network are valid APs, you can configure automatic certificate provisioning to send certificates from the managed device to each campus AP, or to all campus APs within a specific range of IP addresses. If you want closer control over each AP that gets certified, you can manually add individual campus APs to the secure network by adding each AP's information to a campus AP whitelist.

Example

The following command defines a range of IP addresses that should receive certificates from the managed device, and enables the control plane security feature:

```
(host) [md] (config) #control-plane-security
  auto-cert-allowed-addrs 10.21.18.10 10.21.10.90
  cpsec-enable
```

Related Commands

Command	Description
show control-plane-security	Displays the configured control plane security profile settings.

Command History

Release	Modification
ArubaOS 8.3.0.0	The **timer** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

controller-ip

```
controller-ip {loopback|vlan <id>}
```

Description

This command sets the IP address of the managed device to the loopback interface address or a specific VLAN interface address.

Syntax

Parameter	Description	Default
`loopback`	Sets the IP address to the loopback interface.	disabled
`vlan <id>`	Sets the IP address to a VLAN interface.	—

Usage Guidelines

This command allows you to set the managed device IP to the loopback interface address or a specific VLAN interface address. If the managed device IP command is not configured, the managed device IP defaults to the loopback interface address. If the loopback interface address is not configured, the first configured VLAN interface address is selected. Generally, VLAN 1 is the factory default setting and thus becomes the managed device IP address.

Example

The following command sets the IP address to VLAN interface 6.

```
(host) [md] #controller-ip vlan 6
```

Related Commands

Command	Description
show controller-ip	Displays the controller's IP address and VLAN interface ID.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master.

controller-ipv6

```
controller-ipv6 [loopback|{vlan <VLAN ID>}]
   no ...
```

Description

This command sets the default IPv6 address of the Mobility Master to the IPv6 loopback interface address or a specific VLAN interface address.

Syntax

Parameter	Description	Default
`loopback`	Sets the managed device IP to the loopback interface.	disabled
`vlan`	Set the managed device IP to a VLAN interface.	—
`vlan <id>`	Specifies the VLAN interface ID.	—
`address <X:X:X:X::X>`	Specifies the IPv6 address.	—

Usage Guidelines

This command allows you to set the default IPv6 address of the Mobility Master to the IPv6 loopback interface address or a specific IPv6 VLAN interface address. If the Mobility Master IPv6 command is not configured then the Mobility Master IP defaults to the loopback interface address. If the loopback interface address is not configured then the first configured VLAN interface address is selected. Generally, VLAN 1 is the factory default setting and thus becomes the Mobility Master IP address.

Example

The following command sets the Mobility Master IP address to VLAN interface 6:

```
(host) [mynode] (config) #controller-ipv6 vlan 6
```

The following example displays the use of extended scope of address range:

```
(host)[mynode](config) #controller-ipv6 vlan 294 address 2942::5
```

Related Commands

Command	Description
show controller-ipv6	Displays the controller's IPv6 address and VLAN interface ID.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Master.

copy

```
copy

   flash: <srcfilename> {flash: <destfilename>|ftp: <ftphost> <user> [<remote-dir>]
   [<destfilename>]|scp: <scphost> <username> <destfilename>|tftp: <tftphost>
   <destfilename>|usb: partition {0|1} <destfilename>}

   ftp: <ftphost> <user> <filename> system: partition {0|1}

   running-config {flash: <filename>|ftp: <ftphost> <user> <filename> [<remote-dir>]|tftp:
   <tftphost> <filename>}

   scp: <scphost> <username> <filename> {flash: <destfilename>|system: partition {0|1}}

   system: partition {<srcpartition> 0|1} [<destpartition> 0|1]

   tftp: <tftphost> <filename> {flash: <destfilename>|system: partition {0|1}}

   usb: partition <part> <usbfilename> {flash: <flashfilename>|system: partition {0|1}}

copy-provisioning-params
```

Description

This command copies files to and from the managed device.

Syntax

Parameter	Description
`flash: <srcfilename>`	Copies the contents of the managed device's flash file system, the system image, to a specified destination.
`flash:`	Copies the file to the flash file system.
`<destfilename>`	New name of the copied file.
`ftp:`	Copies the file to the FTP file system.
`<ftphost>`	IPv4 or IPv6 address of the FTP server.
`<user>`	Name of the FTP user.
`<remote-dir>`	Name of the remote directory.
`<destfilename>`	New name of the copied file.
`scp:`	Copies the file to the SCP file system.
`<scphost>`	IPv4 or IPv6 address of the remote SCP host.
`<username>`	Username for secure login.
`<destfilename>`	New name of the copied file.
`tftp:`	Copies the file to a TFTP server.

Parameter	Description
<tftphost>	IP address of the TFTP server.
<destfilename>	New name of the copied file.
usb:	Copies the file to an attached USB storage device.
partition	Specifies the partition on the USB device (0.1).
<destfilename>	New name of the copied file.
ftp:	Copies a file from the FTP server.
<ftphost>	IPv4 or IPv6 address or hostname of the FTP server.
<user>	User account name required to access the FTP server.
<filename>	Full name of the file to be copied.
partition	Specifies the system partition to save the file (0,1).
running-config	Copies the active or running configuration to a specified destination.
flash:	Copies the configuration to the flash file system.
<filename>	New name of the copied configuration file.
ftp:	Copies the configuration to an FTP server.
<ftphost>	IP address of the FTP server.
<user>	User account name required to access the FTP server.
<filename>	New name of the copied configuration file.
<remote-dir>	Specifies a remote directory, if needed.
startup-config	Copies the active, running configuration to the start-up configuration.
tftp:	Using TFTP, copy the configuration to a TFTP server
<tftphost>	Specifies the IP address or hostname of the TFTP server.
<filename>	New name of the copied configuration file.
scp:	Copies an ArubaOS image file or file from the flash file system using the Secure Copy protocol. The SCP server or remote host must support SSH version 2 protocol.
<scphost>	IPv4 or IPv6 address of the SCP server or remote host.
<username>	User account name required to access the SCP server or remote host.
<filename>	Absolute path of the filename to be copied.
flash:	Copies the file to the flash file system.
<destfilename>	New name of the copied file.

Parameter	Description
system:	Copies the file to the system partition.
partition	Specifies the system partition to save the file (0,1).
system:	Copies the specified system partition.
<srcpartition>	Disk partition from which to copy the system data (0,1).
<destpartition>	Disk partition to copy the system data to (0,1).
tftp:	Copies a file from the specified TFTP server to either the controller or another destination. This command is typically used when performing a system restoration, or to pull a specified file name into the wms database.
<tftphost>	IPv4 o IPv6 address of the TFTP server.
<filename>	Full name of the file to be copied.
flash:	Copies the file to the flash file system
<destfilename>	New name of the copied file.
system:	Copies the file to the system partition.
partition	Specifies the system partition to save the file (0,1).
usb:	Copies a file from an attached USB device to the flash file system.
partition <part>	Specifies the partition on the USB device (0,1).
<usbfilename>	Full name of the USB file to be copied.
flash:	Copies the file to the flash file system.
<flashfilename>	New name of the copied file.
system:	Copies the file to the system partition.
partition	Specifies the system partition to save the file (0,1).

Usage Guidelines

Use this command to save back-up copies of the configuration file to an FTP or TFTP server, or to load a saved file from an FTP or TFTP server.

Three partitions reside on the file system flash. Totalling 256MB, the three partitions provide space to hold the system image files (in partitions 1 and 2 which are 45MB each) and user files (in partition 3, which is 165MB). System software runs on the system partitions; the database, DHCP, startup configuration, and logs are positioned on the user partition.

To restore a database, copy the database from the network server and import the database.

To restore a configuration file, copy the file from network server to the managed device's flash system then copy the file from the flash system to the system configuration. This ensures that you do not accidentally overwrite your system startup configuration file.

Unlike the managed device's flash, the USB device has more than two partitions; not just 0 and 1. When copying a file from a USB device, you must know which partition the target file is on. Use the **show storage** command to identify the location of the file to identify the correct USB partition.

Example

The following commands copy the configuration file named "engineering" from the TFTP server to the managed device's flash file system, and then uses that file as the startup configuration. This example assumes the startup configuration file is named default.cfg:

```
(host) [mynode] (config) #copy tftp: 192.0.2.0 engineering flash: default.bak
   copy flash: default.bak flash: default.cfg
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

cp-bandwidth-contract

```
cp-bandwidth-contract <string> pps <1...256000>
```

Description

This command configures a bandwidth contract traffic rate, which can then be associated with a whitelist session ACL.

Syntax

Parameter	Description	Range	Default
`<string>`	Name of the bandwidth contract.	—	—
`<1...256000>`	Bandwidth rate in packets per second (pps). **NOTE:** It is recommended that you do not exceed 96000 packets per second or you may encounter buffer allocation issues.	1–256000	—

Example

The following example configures a bandwidth contract named “cp-rate” with a rate of 100 pps.

```
(host) [mynode] (config) #cp-bandwidth-contract cp-rate pps 100
```

Related Commands

Command	Description
show cp-bwcontracts	Displays a list of control processor bandwidth contracts for whitelist ACLs.
firewall cp	This command creates a new whitelist ACL and can associate a bandwidth contract with that ACL.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on Mobility Master.

crypto-local ipsec sa-cleanup

```
crypto-local ipsec sa-cleanup
```

Description

Issue this command to clean IPsec security associations (SAs).

Syntax

No parameters.

Usage Guidelines

Use this command to remove old IPsec security associations if remote APs on your network still use an old SA after upgrading to a newer version of ArubaOS.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto dynamic-map

```
crypto dynamic-map <dynamic-map-name> <dynamic-map-number>
   disable
   no ...
   set pfs {group1|group2|group14|group19|group20}
   set security-association lifetime kilobytes <kilobytes>
   set security-association lifetime seconds <seconds>
   set transform-set <name1> [[<name2>] [<name3>] [<name4>]]
   version {v1|v2}
```

Description

This command configures a new or existing dynamic map.

Syntax

Parameter	Description	Range	Default
`<dynamic-map-name>`	Name of the map.	—	—
`<dynamic-map-number>`	Priority number of the map.	1-10000	10000
`disable`	Disables the dynamic map.	—	—
`no`	Negates a configured parameter.	—	—
`set pfs`	Enables Perfect Forward Secrecy (PFS) mode. Use one of the following: ■ **group1**: 768-bit Diffie Hellman prime modulus group. ■ **group2**: 1024-bit Diffie Hellman ■ **group14**: 2048-bit Diffie Hellman. ■ **group19**: 256-bit random Diffie Hellman ECP modulus group. ■ **group20**: 384-bit random Diffie Hellman ECP modulus group.	—	group1
`set security-association lifetime seconds <seconds>`	Lifetime for the security association (SA) in seconds.	300-86400	7200
`set security-association lifetime kilobytes <kilobytes>`	Lifetime for the security association (SA) in kilobytes.	1000 - 1000000000	—
`set transform-set <name1> [[<name2>] [<name3>] [<name4>]]`	Name of the transform set for this dynamic map. You can specify up to four transform sets. You configure transform sets with the **crypto ipsec transform-set** command.	—	default-transform

Parameter	Description	Range	Default
`version {v1|v2}`	Version of IKE protocol used to set up a security association (SA) in the IPsec protocol suite: ■ **v1**:IKEv1 ■ **v2**: IKEv2	—	v1

Usage Guidelines

Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can optionally associate that map with the default global map using the command **crypto map global-map**.

Example

The following command configures a dynamic map:

```
(host) [mynode] (config) #crypto dynamic-map dmap1 100

  set pfs group2
  set security-association lifetime seconds 300
```

Related Commands

Command	Description
show crypto dynamic-map	Displays IPsec dynamic map configurations.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	The **group19** and **group20** PFS options requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Config mode on Mobility Master.

crypto ipsec

```
crypto ipsec
   mtu <max-mtu>
   transform-set <transform-set-name>
    esp-3des {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes128 {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes128-gcm
    esp-aes192 {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes256 {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-aes256-gcm
    esp-des {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
    esp-null {esp-md5-hmac|esp-null-hmac|esp-sha-hmac}
```

Description

This command configures IPsec parameters.

Syntax

Parameter	Description
`mtu <max-mtu>`	Configure the IPsec Maximum Transmission Unit (MTU) size. The supported range is 1024 to 1500 and the default is 1500.
`transform-set <transform-set-mtu>`	Create or modify a transform set.
`esp-3des`	Use ESP with 168-bit 3DES encryption.
`esp-aes128`	Use ESP with 128-bit AES encryption.
`esp-aes128-gcm`	Use ESP with 128-bit AES-GCM encryption.
`esp-aes192`	Use ESP with 192-bit AES encryption.
`esp-aes256`	Use ESP with 256-bit AES encryption.
`esp-aes256-gcm`	Use ESP with 256-bit AES-GCM encryption.
`esp-des`	Use ESP with 56-bit DES encryption.
`esp-null`	Use ESP with NULL encryption. Supported with only IKEv1.
The following fields are common to the parameters listed in the command definition:	
`esp-md5-hmac`	Use ESP with the MD5 (HMAC variant) authentication algorithm.
`esp-null-hmac`	Use ESP with no authentication. This option is not recommended.
`esp-sha-hmac`	Use ESP with the SHA (HMAC variant) authentication algorithm.

Usage Guidelines

Define the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security, and create or edit transform sets that define a specific encryption and authentication type.

Example

The following command configures 3DES encryption and MD5 authentication for a transform set named **set2**:

```
(host) [mynode] (config)# crypto ipsec transform-set set2 esp-3des esp-md5-hmac
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **esp-null** transform-set parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	The **esp-aes128-gcm** and **esp-aes56-gcm** transform-set parameters require the Advanced Cryptography (ACR) license. All other parameters are available in the base OS.	Config mode on Mobility Master.

crypto isakmp

```
crypto isakmp
   block-aruba-ca {enable|disable}
   eap-passthrough {eap-mschapv2|eap-peap|eap-tls}
   groupname <name>
   key {key <keystring>|key-hex <keystring-hex>}
   udpencap-behind-natdevice {enable|disable}
```

Description

This command configures Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`block-aruba-ca`	Configures the managed device to accept or reject Aruba-certified clients: ■ **enable**: Accepts Aruba-certified client certificates ■ **disable**: Rejects Aruba-certified client certificates and uses custom certificates instead
`eap-passthrough`	Select one of the following authentication types for IKEv2 user authentication using EAP. ■ **eap-mschapv2**: EAP-MSCHAPv2 authentication method ■ **eap-peap**: EAP-PEAP authentication method ■ **eap-tls**: EAP-TLS authentication method
`groupname <name>`	Configures the IKE Aggressive group name. Aggressive-mode IKE is a 3-packet IKE exchange that does not provide identity-protection, but is faster, because fewer messages are exchanged.
`key {key <keystring>| key-hex <keystring-hex>}`	Configures the IKE preshared key, which must be 6-64 characters in length: ■ **key**: Configures the IKE preshared key using text-based characters. ■ **key-hex**: Configures the IKE preshared key using hex-based characters (0-9, a-f, A-F).
`udpencap-behind-natdevice`	Configures NAT-T if the managed device is behind an NAT device (for Windows VPN Dialer only): ■ **enable**: Enables NAT-T ■ **disable**: Disables NAT-T

Usage Guidelines

Use this command to configure the IKE pre-shared key, set the EAP authentication method for IKEv2 clients using EAP user authentication, and enable source NAT if the IP addresses of clients need to be translated to access the network.

Example

The following command configures an ISAKMP peer IP address and subnet mask. After configuring an ISAKMP address and netmask, you will be prompted to enter the IKE preshared key.

```
(host) [mynode] (config) #crypto isakmp address 10.3.14.21 netmask 255.255.255.0
```

```
Key:*******Re-Type Key:*******
```

Related Commands

Command	Description
show crypto isakmp	Displays IKE parameters configured for ISAKMP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto isakmp policy

```
crypto isakmp policy <priority>
   authentication {pre-share|rsa-sig|ecdsa-256|ecdsa-384}
   disable
   enable [bypass|secret]
   encryption {3DES|AES128|AES192|AES256|DES}
   group {1|2|14|19|20}
   hash {md5|sha|sha1-96|sha2-256-128|sha2-384-192}
   prf {PRF-HMAC-MD5|PRF-HMAC-SHA1|PRF-HMAC-SHA256|PRF-HMAC-SHA384}
   lifetime <seconds>
   no disable
   version {v1|v2}
```

Description

This command configures Internet Key Exchange (IKE) policy parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`<priority>`	Specifies a number from 1 to 10,000 to define a priority level for the policy. The higher the number, the higher the priority level.
`authentication`	Configures the IKE authentication method: ■ **pre-share**: Preshared key ■ **rsa-sig**: RSA signatures ■ **ecdsa-256**: ECDSA-256-bit signatures ■ **ecdsa-384**: ECDSA-384-bit signatures
`disable`	Disables the IKE policy.
`enable [bypass|secret]`	Enables the IKE policy using the bypass or secret. **Bypass** prompts for the enable mode login and password. **Secret** prompts for the enable password.
`encryption`	Configures the IKE encryption algorithm: ■ **3DES**: 168-bit 3DES-CBC encryption algorithm ■ **AES128**: 128-bit AES-CBC encryption algorithm ■ **AES192**: 192-bit AES-CBC encryption algorithm ■ **AES256**: 256-bit AES-CBC encryption algorithm ■ **DES**: 56-bit DES-CBC encryption algorithm
`group`	Configures the IKE Diffie Hellman group: ■ **1**: 768-bit Diffie Hellman prime modulus group. This is the default group setting. ■ **2**: 1024-bit Diffie Hellman prime modulus group ■ **14**: 2048-bit Diffie Hellman DDH prime modulus group ■ **19**: 256-bit random Diffie Hellman ECP modulus group ■ **20**: 384-bit random Diffie Hellman ECP modulus group

Parameter	Description
`hash`	Configures the IKE hash algorithm: ■ **md5**: MD5 (HMAC variant) hash algorithm ■ **sha**: SHA1-160 (HMAC variant) hash algorithm ■ **sha1-96**: SHA1-96 (HMAC variant) hash algorithm ■ **sha2-256-128**: SHA2-256-128 (HMAC variant) hash algorithm ■ **sha2-384-192**: SHA2-384-192 (HMAC variant) hash algorithm
`prf`	Sets one of the following pseudo-random function (PRF) values for an IKEv2 policy: ■ **PRF-HMAC-MD5 (default)**: MD5 (HMAC variant) PRF ■ **PRF-HMAC-SHA1**: SHA1-160 (HMAC variant) PRF ■ **PRF-HMAC-SHA256**: SHA2-256 PRF ■ **PRF-HMAC-SHA384**: SHA2-384 PRF
`lifetime <seconds>`	Specifies the lifetime of the IKE security association (SA), from 300 - 86400 seconds.
`no disable`	Disables the IKE policy.
`version`	Specifies the version of IKE protocol for the IKE policy: ■ **v1**: IKEv1 ■ **v2**: IKEv2

Usage Guidelines

To define settings for a ISAKMP policy, issue the command **crypto isakmp policy <priority>** then press **Enter**. The CLI will enter **config-isakmp** mode, which allows you to configure the policy values.

Example

The following command configures the RSA signature authentication method for the given IKE policy:

```
(host) [mynode] (config) #crypto isakmp policy 1

(host) [mynode] (config-isakmp) #authentication rsa-sig

Key:*******Re-Type Key:*******
```

Related Commands

Command	Description
show crypto isakmp	Displays IKE policies configured for ISAKMP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	The following settings require the Advanced Cryptogram (ACR) license: ■ hash algorithm: **SHA-256-128**, **SHA-384-192** ■ Diffie-Hellman (DH) Groups: **19** and **20** ■ Pseudo-Random Function (PRF): **PRF-HMAC-SHA256**, **PRF-HMAC-SHA384** ■ Authentication: **ecdsa-256** and **ecdsa-384** All other parameters are supported in the base OS.	Config mode on Mobility Master.

crypto-local ipsec-map

```
crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>
   client-mode [<nat>|<network>]
   disable
   dst-net <ipsec-map-dst-net> <mask> | any
   dst-net-ipv6 <ipsec-map-dst-net-ipv6> <ipsec-map-dst-prefix-len>
   enrolled-cert-auth
   factory-cert-auth
   force-natt {enable|disable}
   force-tunnel-mode
   ip access-group in <access-group>
   ip-compression {enable|disable}
   load-balance
   local-fqdn <local_id_fqdn>
   monitor <ip> <frequency> <burst count> <retry num>
   no ...
   peer-cert-dn <peer-dn>
   peer-fqdn {any-fqdn|peer-fqdn <peer-id-fqdn>}
   peer-ip <ipaddr>
   peer-ipv6 <ipsec-map-peer-ipv6>
   pre-connect {disable|enable}
   set ca-certificate <cacert-name>
   set ike1-policy <policy-v1-number>
   set ikev2-policy <policy-v2-number>
   set pfs {group1|group2|group14|group19|group20}
   set security-association lifetime kilobytes <kilobytes>
   set security-association lifetime seconds <seconds>
   set server-certificate <cert-name>
   set transform-set <name1> [<name2>] [<name3>] [<name4>]
   src-net <ipsec-map-src-net> vlan <mask> | any
   src-net-ipv6 <ipsec-map-src-net-ipv6>
      <ipsec-map-src-prefix-len>
   trusted {enable|disable}
   uplink failover {enable|disable}
   version {v1|v2}
   vlan <ipsec-map-vlan-id>
```

Description

This command configures IPsec mapping for site-to-site VPNs.

Syntax

Parameter	Description	Range	Default
`<map>`	Name of the IPsec map.	—	—
`<priority>`	Priority of the entry.	1-9998	—
`client-mode [<nat>|<network>]`	Enables client-mode where: **nat** enables nat mode with any and any. **network** enables network mode	—	—

Parameter	Description	Range	Default
`dst-net`	IP address and netmask for the destination network.	—	—
`disable`	Disables an existing IPsec map. New maps are enabled by default.	—	—
`dst-net <ipsec-map-dst-net> <ipsec-map-dst-mask> | any`	IP address and netmask for the destination network.	—	—
`dst-net-ipv6 <ipsec-map-dst-net-ipv6> <ipsec-map-dst-prefix-len>`	IPv6 address and netmask for the destination network.	—	—
`enrolled-cert-auth`	Enables the enrolled certificate authentication for site-to-site tunnel.	—	—
`factory-cert-auth`	Enables factory certificate authentication for site-to-site VPNs.	—	Disabled
`force-natt`	Include this parameter to always enforce UDP 4500 for IKE and IPsec. This option is disabled by default.	—	Disabled
`force-tunnel-mode`	Configures the force-tunnel-mode flag.	—	—
`ip access-group in <access-group>`	Configures the IP access group name. Attach a route ACL to the IPsec map for a site-to-site VPN. When you associate a routing ACL to inbound traffic on a Mobility Master terminating a site-to-site VPN, that ACL can forward traffic as normal, route traffic to a nexthop router on a nexthop list, or redirect traffic over an L3 GRE tunnel or tunnel group. For more information on creating a routing ACL, see ip access-list route.	—	—
`ip-compression`	Enable compression for traffic in an IKEv2 site-to-site tunnel between a master and local 7000 Series Mobility Master. Compression is disabled by default.	—	Disabled

Parameter	Description	Range	Default
`load-balance`	Enable VPN load balancing for any tunnel.	—	Disabled
`local-fqdn <local_id_fqdn>`	If the managed device has a dynamic IP address, you must specify the FQDN of the managed device to configure it as a initiator of IKE aggressive-mode.	—	—
`monitor <monitor-ip> interval <interval_secs>`	Configure link monitor where **<monitor-ip>** is IP address of monitor server. **interval <interval_secs>** is optional interval in seconds.	—	—
`no`	Negates a configured parameter.	—	—
`peer-cert-dn <peer-dn>`	If you are using IKEv2 to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by entering its certificate subject name in the Peer Certificate Subject Name field	—	—
`peer-fqdn`	For site-to-site VPNs with dynamically addressed peers, specify a FQDN for the managed device: ■ **any-fqdn**: Any remote FQDN ID ■ **fqdn-id**: Unique remote FQDN ID	—	any-fqdn
`peer-ip <ipaddr>`	If you are using IKEv1 to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by entering the IP address of the peer gateway. **NOTE:** If you are configuring an IPsec map for a static-ip managed device with a dynamically addressed remote peer, you must leave the peer gateway set to its default value of 0.0.0.0.	—	—

Parameter	Description	Range	Default
`peer-ipv6 <ipsec-map-peer-ipv6>`	If you are using IKEv1 to establish a site-to-site VPN to a statically addressed remote peer, identify the peer device by entering the IPv6 address of the peer gateway. **NOTE:** If you are configuring an IPsec map for a static-ip managed device with a dynamically addressed remote peer, you must leave the peer gateway set to its default value.		
`pre-connect`	Enables or disables pre-connection.	—	disabled
`set ca-certificate <cacert-name>`	User-defined name of a trusted CA certificate installed on the Mobility Master. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the Mobility Master. The CA certificate name must be between 1-64 characters in length.	1-64 characters	—
`set ike1-policy <policy-v1-number>`	Select an IKEv1 policy for the ipsec-map. Predefined policies are described in the table below.	—	—
`set ikev2-policy <policy-v2-number>`	Select IKEv2 policy for the ipsec-map. Predefined policies are described in the table below.	—	—

Parameter	Description	Range	Default
`set pfs`	If you enable Perfect Forward Secrecy (PFS) mode, new session keys are not derived from previously used session keys. Therefore, if a key is compromised, that compromised key will not affect any previous session keys. To enable this feature, specify one of the following Perfect Forward Secrecy modes: ■ **group1**: 768-bit Diffie Hellman prime modulus group. ■ **group2**: 1024-bit Diffie Hellman prime modulus group. ■ **group14**: 2048-bit Diffie Hellman prime modulus group. ■ **group19**: 256-bit random Diffie Hellman ECP modulus group. (For IKEv2 only) ■ **group20**: 384-bit random Diffie Hellman ECP modulus group. (For IKEv2 only)	—	disabled
`set security-association lifetime kilobytes <kilobytes>`	Configures the lifetime for the security association (SA) in kilobytes.	1000 - 1000000000 kilobytes	–
`set security-association lifetime seconds <seconds>`	Configures the lifetime for the security association (SA) in seconds	300-86400 seconds	7200 seconds
`set server-certificate <cert-name>`	User-defined name of a server certificate installed for the site-to-site IPsec map. Use the **show crypto-local pki ServerCert** command to display the server certificates that have been imported into the Mobility Master. The server certificate name must be between 1-64 characters in length.	1-64 characters	—

Parameter	Description	Range	Default
`set transform-set <transform-set-name1> [<transform-set-name2>] [<transform-set-name3>] [<transform-set-name4>]`	Name of the transform set for this IPsec map. One transform set name is required, but you can specify up to four transform sets. Configure transform sets with the **crypto ipsec transform-set** command.	—	default-transform
`src-net <ipsec-map-src-net> <ipsec-map-src-mask> | any`	IP address and netmask for the source network.	—	—
`src-net-ipv6 <ipsec-map-src-net-ipv6> <ipsec-map-src-prefix-len>`	IPv6 address and netmask for the source network.	—	—
`trusted`	Enables or disables a trusted tunnel.	—	disabled
`uplink failover`	Enables or disables uplink failover for site-to-site tunnels.	—	disabled
`version`	Select the IKE version for the IPsec map. ■ **v1**: IKEv1 ■ **v2**: IKEv2		v1
`vlan <ipsec-map-vlan-id>`	VLAN ID. Enter 0 for the loopback, and 4095 for cellular.	1-4094	—

Usage Guidelines

You can use Mobility Master instead of VPN concentrators to connect sites at different physical locations.

You can configure separate CA and server certificates for each site-to-site VPN. You can also configure the same CA and server certificates for site-to-site VPN and client VPN. Use the **show crypto-local ipsec-map** command to display the certificates associated with all configured site-to-site VPN maps; use the **tag <map>** option to display certificates associated with a specific site-to-site VPN map.

Mobility Master supports site-to-site VPNs with two statically addressed managed device, or with one static and one dynamically addressed managed device. By default, site-to-site VPN uses IKE Main-mode with Pre-Shared-Keys to authenticate the IKE SA. This method uses the IP address of the peer, and therefore will not work for dynamically addressed peers.

To support site-site VPN with dynamically addressed devices, you must enable IKE Aggressive-Mode with Authentication based on a Pre-Shared-Key. A managed device with a dynamic IP address must be configured to be the initiator of IKE Aggressive-mode for Site-Site VPN, while the managed device with a static IP address must be configured as the responder of IKE Aggressive-mode.

IKEv2 site-to-site VPNs between Mobility Master and 7000 Series Mobility Master support traffic compression between those devices. When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Skype4b or Voice traffic) is not compromised by increased latency or decreased throughput.

Understanding Default IKE policies

ArubaOS includes the following default IKE policies. These policies are predefined and cannot be edited.

Table 8: *Default IKE Policy Settings*

Policy Name	Policy Number	IKE Version	Encryption Algorithm	Hash Algorithm	Authentica-tion Method	PRF Method	Diffie-Hellman Group
Default protection suite	10001	IKEv1	3DES-168	SHA 160	Pre-Shared Key	N/A	2 (1024 bit)
Default Remote AP Certificate protection suite	10002	IKEv1	AES -256	SHA 160	RSA Signature	N/A	2 (1024 bit)
Default Remote AP PSK protection suite	10003		AES -256	SHA 160	Pre-Shared Key	N/A	2 (1024 bit)
Default Remote AP IKEv2 RSA protection suite	1004	IKEv2	AES -256	SSHA160	RSA Signature	hmac-sha1	2 (1024 bit)
Default Cluster PSK protection suite	10005	IKEv1	AES -256	SHA160	Pre-Shared Key	Pre-Shared Key	2 (1024 bit)
Default IKEv2 RSA protection suite	1006	IKEv2	AES - 128	SHA 96	RSA Signature	hmac-sha1	2 (1024 bit)
Default IKEv2 PSK protection suite	10007	IKEv2	AES - 128	SHA 96	Pre-shared key	hmac-sha1	2 (1024 bit)
Default Suite-B 128bit ECDSA protection suite	10008	IKEv2	AES - 128	SHA 256-128	ECDSA-256 Signature	hmac-sha2-256	Random ECP Group (256 bit)

Policy Name	Policy Number	IKE Version	Encryption Algorithm	Hash Algorithm	Authentica-tion Method	PRF Method	Diffie-Hellman Group
Default Suite-B 256 bit ECDSA protection suite	10009	IKEv2	AES -256	SHA 384-192	ECDSA-384 Signature	hmac-sha2-384	Random ECP Group (384 bit)
Default Suite-B 128bit IKEv1 ECDSA protection suite	10010	IKEv1	AES-GCM-128	SHA 256-128	ECDSA-256 Signature	hmac-sha2-256	Random ECP Group (256 bit)
Default Suite-B 256-bit IKEv1 ECDSA protection suite	10011	IKEv1	AES-GCM-256	SHA 256-128	ECDSA-256 Signature	hmac-sha2-256	Random ECP Group (256 bit)

When using a default IKE (V1 or V2) policy for an IPsec map, the priority number should be the same as the policy number.

Examples

The following commands configures site-to-site VPN between two managed devices:

```
(host) [mynode] (config) #crypto-local ipsec-map sf-chi-vpn 100
   src-net 101.1.1.0 255.255.255.0
   dst-net 100.1.1.0 255.255.255.0
   peer-ip 172.16.0.254
   vlan 1
   trusted

(host) [mynode] (config) #crypto-local ipsec-map chi-sf-vpn 100
   src-net 100.1.1.0 255.255.255.0
   dst-net 101.1.1.0 255.255.255.0
   peer-ip 172.16.100.254
   vlan 1
   trusted
```

For a dynamically addressed managed device that initiates IKE Aggressive-mode for Site-Site VPN:

```
(host) [mynode] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>
   src-net <ipsec-map-src-net> <ipsec-map-src-mask>
   dst-net <ipsec-map-dst-net> <ipsec-map-dst-mask>
   peer-ip <ipaddr>
   local-fqdn <local_id_fqdn>
   vlan <ipsec-map-vlan-id>
   pre-connect {enable|disable}
   trusted enable
```

For the Pre-shared-key:

```
crypto-local isakmp key <key> address <ipaddr> netmask <mask>
```

For a static IP managed device that responds to IKE Aggressive-mode for Site-Site VPN:

```
(host) [mynode] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>
  src-net <ipsec-map-src-net> <ipsec-map-src-mask>
  dst-net <ipsec-map-dst-net> <ipsec-map-dst-mask>
  peer-ip 0.0.0.0
  peer-fqdn fqdn-id <peer_id_fqdn>
  vlan <ipsec-map-vlan-id>
  trusted enable
```

For the Pre-shared-key:

```
crypto-local isakmp key <key> fqdn <fqdn-id>
```

For a static IP managed device that responds to IKE Aggressive-mode for Site-Site VPN with One PSK for All FQDNs:

```
(host) [mynode] (config) #crypto-local ipsec-map <ipsec-map-name> <ipsec-map-number>
  src-net <ipaddr> <mask>
  peer-ip 0.0.0.0
  peer-fqdn any-fqdn
  vlan <id>
  trusted enable
```

For the Pre-shared-key for All FQDNs:

```
crypto-local isakmp key <key> fqdn-any
```

The following example displays the use of extended scope of address range:

```
(host) [mynode] (config) #crypto-local ipsec-map sparta2vesuvius 100
  version v2
  set ikev2-policy 10009
  peer-ipv6 2004::1
  peer-cert-dn "/C=US/ST=HI/L=Camp
  Smith/O=PACOM/OU=mil/CN=vesuvius.red1.vpn/emailAddress=admin@pacom.mil"
  vlan 202
  src-net-ipv6 2012:: 64
  dst-net-ipv6 2014:: 64
  set transform-set "default-gcm256"
  set pfs group20
  trusted
  set ca-certificate red.ca
  set server-certificate sparta.red.vpn
  !
```

Related Commands

Command	Description
show crypto-local ipsec-map	Displays current IPsec map configurations for site-to-site VPNs.
crypto_local isakmp disable-ipcomp	Globally disables IP compression on all site-to-site VPNs between Mobility Master and managed devices by disabling compression from the master.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **enrolled-cert-auth** and **force-tunnel-mode** parameter was added. Updated the new syntax as **ip access-group in <access-group>** .
ArubaOS 8.1	The **any** sub-parameter was added in **dst-net**, and **src-net** parameters. The **client-mode**, **load-balance**, and **monitor** parameters were added.
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	The **group19** and **group20** PFS options requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Config mode on Mobility Master.

crypto-local isakmp allow-via-subnet-routes

```
crypto-local isakmp allow-via-subnet-routes
```

Description

This command allows VIA clients to push subnet routes to Mobility Master.

Syntax

No parameters.

Example

This command enables VIA clients to push subnets to Mobility Master:

```
(host) [mynode] (config) #crypto-local isakmp allow-via-subnet-routes
```

Related Commands

Command	Description
show crypto-local isakmp	Indicates if Mobility Master can accept subnet routes from VIA clients.

Command History

Release	Modification
ArubaOS 8.0.1.0	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp ca-certificate

```
crypto-local isakmp ca-certificate <cacert-name>
```

Description

This command assigns the Certificate Authority (CA) certificate used to authenticate VPN clients.

Syntax

Parameter	Description
`<cacert-name>`	User-defined name of a trusted CA certificate installed on the Mobility Master. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the Mobility Master.

Usage Guidelines

You can assign multiple CA certificates. Use the **show crypto-local isakmp ca-certificate** command to view the CA certificates associated with VPN clients.

Example

This command configures a CA certificate:

```
(host) [mynode] (config) #crypto-local isakmp ca-certificate TrustedCA1
```

Related Commands

Command	Description
show crypto-local isakmp	Displays CA certificates configured for VPN clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp certificate-group

```
crypto-local isakmp certificate-group server-certificate <server_cert-name> ca-certificate
<ca_cert-name>
```

Description

The command configures an IKE certificate group for VPN Clients.

Syntax

Parameter	Description	Range	Default
`server-certificate <server-cert-name>`	The IKE server certificate name for VPN clients.	1-64 characters	—
`ca-certificate <ca-cert-name>`	The IKE CA certificate for this server certificate.	1-64 characters	—

Usage Guidelines

This feature allows you to create a certificate group so you can access multiple types of certificates on the same Mobility Master.

Example

This command configures a certificate group that consists of server certificate named “newtest” with the CA certificate “TrustedCA”.

```
(host) [mynode] (config) #crypto-local isakmp certificate-group server-certificate newtest ca-
certificate TrustedCA
```

Related Commands

Command	Description
show crypto-local isakmp	Displays the configured IKE certificate groups for VPN clients.
show crypto-local isakmp	Displays the configured IKE server certificate for VPN clients.
show crypto-local isakmp	Displays the configured IKE CA certificate for VPN clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp disable-aggressive-mode

```
crypto-local isakmp disable-aggressive-mode
```

Description

The command disables the IKEv1 aggressive mode.

Syntax

No parameters.

Usage Guidelines

The Mobility Master-managed device communication, by default, uses IPsec aggressive mode when a PSK is used for authentication. You need to convert Mobility Master-managed device communication to certificate-based IPsec authentication before disabling aggressive mode.

Disabling aggressive mode will impact other sessions that use aggressive mode, such as Master-local IKE session with PSK.

Example

```
(host) [mynode] (config) #crypto-local isakmp disable-aggressive-mode
```

Related Commands

Command	Description
show crypto-local isakmp	Indicates if aggressive mode is enabled or disabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto_local isakmp disable-ipcomp

```
crypto-local isakmp disable-ipcomp
```

Description

This command disables IP compression on Mobility Master.

Syntax

No parameters.

Usage Guidelines

When this hardware-based compression feature is enabled, the quality of unencrypted traffic (such as Skype4b or Voice traffic) is not compromised by increased latency or decreased throughput.

Example

```
(host) [mynode] (config) #crypto-local isakmp disable-ipcomp
```

Related Commands

Version	Modification
crypto-local ipsec-map	Locally disables IP compression on an individual site-to-site VPN by disabling compression on a specific IPsec map.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp dpd

```
crypto-local isakmp dpd idle-timeout <idle_sec> retry-timeout <retry_sec>  retry-attempts <retry_num>
```

Description

This command configures IKE DPD.

Syntax

Parameter	Description	Range	Default
`idle-timeout <idle_sec>`	Idle timeout, in seconds.	10-3600 seconds	22 seconds
`retry-timeout <retry_sec>`	Retry interval, in seconds.	2-60 seconds	2 seconds
`retry-attempts <retry_num>`	Number of retry attempts.	3-10	3

Usage Guidelines

DPD is enabled by default for site-to-site VPNs.

Example

The following command configures DPD parameters:

```
(host) [mynode] (config) #crypto-local isakmp dpd idle-timeout 60 retry-timeout 3 retry-attempts 5
```

Related Commands

Command	Description
show crypto-local isakmp	Displays the IKE DPD configured on a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp key

```
crypto-local isakmp {key <keystring>|key-hex <keystring>}
   address <peer-address> netmask <mask>
   addressv6 <peer-addressv6>
   fqdn <ike-id-fqdn>
   fqdn-any
```

Description

This command configures the IKE preshared key for site-to-site VPN.

Syntax

Parameter	Description
`key <keystring>`	IKE preshared key value, between 6-64 characters. To configure a pre-shared key that contains non-alphanumeric characters, surround the key with quotation marks. For example: **crypto-local isakmp key "key with spaces" fqdn-any**.
`key-hex <keystring>`	IKE preshared key value, between 6-64 hex-based characters. To configure a pre-shared key that contains non-alphanumeric characters, surround the key with quotation marks.
`address <peer-address>`	IP address for the preshared key.
`netmask <mask>`	Netmask for the preshared key.
`addressv6 <peer-addressv6>`	IPv6 address for the preshared key.
`fqdn <ike-id-fqdn>`	Configures the PSK for the specified FQDN.
`fqdn-any`	Configures the PSK for any FQDN.

Usage Guidelines

This command configures the IKE preshared key.

Example

The following command configures an IKE preshared key for site-to-site VPN:

```
(host) [mynode] (config) #crypto-local isakmp key R8nD0mK3y address 172.16.100.1 netmask
255.255.255.255
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp permit-invalid-cert

```
crypto-local isakmp permit-invalid-cert
```

Description

This command allows invalid or expired certificates to be used for site-to-site VPN.

Syntax

No parameters.

Usage Guidelines

This command allows invalid or expired certificates to be used for site-to-site VPN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp route ipsec

```
crypto-local isakmp route ipsec <route-ipsec-map-name> vlan <vlan-value>
```

Description

This command configures the subnet route using an IPsec map.

Syntax

Parameter	Description	Range
`<route-ipsec-map-name>`	Name of the IPsec map.	—
`vlan <vlan-value>`	VLAN for which the subnet route is pushed. Each VLAN must be separated by a comma and dash.	—

Usage Guidelines

The following example configures a subnet route for VLAN 1 using an IPsec map:

```
(host) [mynode] (config) #crypto-local isakmp route ipsec default-local-master-
ipsecmap192.190.189.1 vlan 1
```

Related Commands

Command	Description
show crypto-local ipsec-map	Displays the list of configured IPsec maps.
show vlan	Displays the list of configured VLANs.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp sa-cleanup

```
crypto-local isakmp sa-cleanup
```

Description

This command enables the cleanup of IKE SAs.

Syntax

No parameters.

Usage Guidelines

This command removes expired ISAKMP SAs from the Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp server-certificate

```
crypto-local isakmp server-certificate <cert-name>
```

Description

This command assigns the server certificate used to authenticate the Mobility Master or managed device for VPN clients using IKEv1 or IKEv2.

Syntax

Parameter	Description
`<cert-name>`	User-defined name of a server certificate installed on the Mobility Master or managed device.

Usage Guidelines

This certificate is only for VPN clients and not for site-to-site VPN clients. You can assign separate server certificates for VPN clients using IKEv1 and clients using IKEv2. Use the **show crypto-local isakmp server-certificate** command to view the server certificate associated with VPN clients.

There is a default server certificate installed on Mobility Master. However this certificate does not guarantee security for production networks. Best practices is to replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. You can use the WebUI to generate a Certificate Signing Request (CSR) to submit to a CA and then import the signed certificate received from the CA into Mobility Master. For more information, see "Managing Certificates" in the *ArubaOS User Guide*.

Example

This command configures a server certificate:

```
(host) [mynode] (config) #crypto-local isakmp server-certificate MyServerCert
```

Related Commands

Command	Description
show crypto-local isakmp	Displays the server certificates that have been imported into Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local isakmp xauth

```
crypto-local isakmp xauth
```

Description

This command enables IKE XAuth for VPN clients.

Syntax

No parameters.

Usage Guidelines

The **no crypto-local isakmp xauth** command disables IKE XAuth for VPN clients. This command only applies to VPN clients that use certificates for IKE authentication. If you disable XAuth, then a VPN client that uses certificates will not be authenticated using a username and password. You must disable XAuth for Cisco VPN clients using CAC Smart Cards.

Example

This command disables IKE XAuth for Cisco VPN clients using CAC Smart Cards:

```
(host) [mynode] (config) #no crypto-local isakmp xauth
```

Related Commands

Command	Description
show crypto-local isakmp	Indicates if IKE XAuth is enabled or disabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local pki

```
crypto-local pki
   allow-low-assurance-devices
   CRL <name> <filename>
   global-oscp-signer-cert
   IntermediateCA <name> <filename>
   OCSPResponderCert <certname> <filename>
   OCSPSignerCert <certname> <filename>
   PublicCert <name> <filename>
   rcp <name>
   ServerCert <name> <filename>
   service-ocsp-responder {enable|disable}
   TrustedCA <name> <filename>
```

Description

This command configures a local certificate, OCSP signer or responder certificate, and Certificate Revocation List (CRL). You can also list revocation checkpoints and enable the responder service.

Syntax

Parameter	Description
`allow-low-assurance-devices`	Enables or disables low assurance devices.
`CRL`	Specifies a Certificate Revocation list. Validation of the CRL is done when it imported through the WebUI (requires the CA to have been already present). CRLs can only be imported through the WebUI.
`<name>`	Name of the CRL.
`<filename>`	Original imported filename of the CRL.
`global-ocsp-signer-cert`	Specifies the global OCSP signer certificate used to sign OCSP responses if there is no checkpoint-specific OCSP signer certificate present. If the ocsp-signer-cert is not specified, OCSP responses are signed using the global OCSP signer certificate. If this is not present, an error message is sent out to clients. **NOTE:** The OCSP signer certificate (if configured) takes precedence over the global OCSP signer certificate as this is checkpoint-specific.
`IntermediateCA`	Configures an intermediate CA certificate.
`<name>`	Name of the intermediate CA certificate.
`<filename>`	Original imported filename of the CRL.
`OCSPResponderCert`	Configures an OCSP responder certificate.
`<certname>`	Name of responder certificate.
`<filename>`	Original imported filename of the responder certificate.
`OCSPSignerCert`	Configures an OCSP signer certificate.

Parameter	Description
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
PublicCert	Public key of a certificate. This allows an application to identify an exact certificate.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
rcp <name>	Specifies the revocation checkpoint. A revocation checkpoint is automatically created when a TrustedCA or IntermediateCA certificate is imported on the Mobility Master. See crypto-local pki rcp for more details.
ServerCert	Configures a server certificate. This certificate must contain both a public and private key (the public and private keys must match). You can import a server certificate in either PKCS12 or x509 PEM format; the certificate is stored in x509 PEM DES encrypted format on the Mobility Master.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.
service-ocsp-responder	Enables or disables the OCSP responder service. The default is **disabled**. To enable this option, a CRL must be configured for this revocation checkpoint, as this is the source of revocation information in the OCSP responses.
TrustedCA	Configures a trusted CA certificate. This can be either a root CA or intermediate CA. Aruba encourages (but does not require) an intermediate CA's signing CA to be the Mobility Master itself.
<certname>	Name of the signer certificate.
<filename>	Original imported filename of the signer certificate.

Usage Guidelines

This command lets you configure the Mobility Master to perform real-time certificate revocation checks using the Online Certificate Status Protocol (OCSP) or traditional certificate validation using the Certificate Revocation List (CRL) client. Refer to the *Certificate Revocation* chapter in the *ArubaOS 8.3.0.x User Guide* for more information on how to configure this feature using both the WebUI and CLI.

Example

The following example configures the Mobility Master as an OCSP responder:

```
(host) [mynode] (config) #crypto-local pki service-ocsp-responder
(host) [mynode] (config) #crypto-local pki rcp CARoot
   ocsp-signer-cert RootCA-Ocsp_signer
   crl-location file Security1-WIN-05PRGNGEKAO-CA-unrevoked.crl
  enable-ocsp-responder
```

Related Commands

Command	Description
crypto-local pki rcp	Specifies the certificates that are used to sign OCSP responses for this revocation check point
show crypto-local pki	Displays local certificates, OCSP signer or responder certificates, and CRL data and statistics.

Command History

Version	Modification
ArubaOS 8.2.0.0	The **allow-low-assurance-devices** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto-local pki rcp

```
crypto-local pki rcp <name> [allow-low-assurance-devices|crl-location <filename>|enable-ocsp-responder|ocsp-responder-cert <ocsp-responder-cert>|ocsp-signer-cert <ocsp-signer-cert>|ocsp-url <ocsp-url>|revocation-check <method1> [<method2>]|server-unreachable {revoke-cert|fail-over|allow-cert}]
```

Description

This command specifies the certificates used to sign OCSP for the revocation checkpoint. A revocation checkpoint is automatically created when a TrustedCA or IntermediateCA certificate is imported into Mobility Master.

Syntax

Parameter	Description
`allow-low-assurance-devices`	Enables or disables low assurance devices.
`crl-location <file>`	Location of the CRL that is used for the rcp. The specified CRL filename must be previously imported onto Mobility Master before using this option.
`enable-ocsp-responder`	Enables the OCSP Responder for this revocation checkpoint. The default is disabled.
`ocsp-responder-cert <ocsp-responder-cert>`	Specifies the certificate that is used to verify OCSP responses. The certificate must be one of the certificate names displayed when the **show crypto-local pki OCSPResponderCert** command is executed.
`ocsp-signer-cert <ocsp-signer-cert>`	Specifies the certificate that is used to sign OCSP responses for this revocation checkpoint. The OCSP signer certificate must be previously imported onto Mobility Master through the WebUI. The OCSP signer cert can be the same TrustedCA as the checkpoint, a designated OCSP signer certificate issued by the same CA as the checkpoint, or another local trusted authority. If the ocsp-signer-cert is not specified, OCSP responses are signed using the global OCSP signer certificate. If that is not present, an error message is sent out to clients. **NOTE:** The OCSP signer certificate (if configured) takes precedence over the global OCSP signer certificate as this is check point specific.
`ocsp-url <ocsp-url>`	Configures the OCSP Server URL. The URL must be in the form of **http://my.responder.com/path**. This parameter can contain only one responder URL at time.
`revocation-check <method1> [<method2>]`	Configures the revocation check methods used for this rcp. Options include: ■ **None (default)**: No revocation checks are performed ■ **CRL**: CRL revocation check method ■ **OCSP**: OCSP revocation check method You can configure one fallback method.

Parameter	Description
`server-unreachable {revoke-cert|fail-over|allow-cert}`	Configures one of the following methods to use upon failure to connect to the OCSP server: ■ **allow-cert**: The certificate is considered 'Good' upon failure to establish connection with the OCSP responder server. ■ **fail-over**: The certificate revocation is matched against the CRL upon failure to establish connection with the OCSP responder server. ■ **revoke-cert**: The certificate is considered 'Revoked' upon failure to establish connection with the OCSP responder server.

Usage Guidelines

This command allows you to configure the check methods that are used for the given revocation checkpoint. You can configure Mobility Master to perform real-time certificate revocation checks using the Online Certificate Status Protocol (OCSP) or traditional certificate validation using the Certificate Revocation List (CRL) client. Refer to the *Certificate Revocation* chapter in the *ArubaOS 8.3.0.x User Guide* for more information on how to configure this feature using both the WebUI and CLI.

Example

This example configures an OCSP client with the OCSP revocation check method and CRL backup method:

```
(host) [mynode] (config) #crypto-local pki rcp CARoot
  ocsp-responder-cert RootCA-Ocsp_responder
  ocsp-url http://10.4.46.202/ocsp
  crl-location file Security1-WIN-05PRGNGEKAO-CA-unrevoked.crl
  revocation-check ocsp crl
```

Related Commands

Command	Description
crypto-local pki	Configures local certificates, OCSP signer or responder certificates, and Certificate Revocation Lists (CRL). You can also list revocation checkpoints and enable the responder service.
show crypto-local pki	Displays local certificates, OCSP signer or responder certificates, and CRL data and statistics.

Command History

Version	Modification
ArubaOS 8.2.0.0	The **allow-low-assurance-devices** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto map global-map

```
crypto map global-map <map-number> ipsec-isakmp {dynamic <dynamic-map-name>|ipsec <ipsec-map-name>}
```

Description

This command configures the default global map.

Syntax

Parameter	Description
`<map-number>`	Priority of the map.
`ipsec-isakmp`	Configures an IPsec map.
`dynamic <dynamic-map-name>`	Uses a dynamic map.
`ipsec <ipsec-map-name>`	Uses an IPsec map.

Usage Guidelines

This command identifies the dynamic or IPsec map used as the default global map. If you have not yet defined a dynamic or IPsec map, issue the command **crypto map global-map** or **crypto-local ipsec-map** to define map parameters.

Example

The following command configures the global map with the dynamic map named *dynamic_map_2*.

```
(host) [mynode] (config) #crypto map global-map 2 ipsec-isakmp dynamic dynamic_map_2
```

The following examples display the use of extended scope of address range:

```
(host) [mynode] (config) #crypto map GLOBAL-IKEV2-MAP 10000 ipsec-isakmp dynamic default-rap-ipsecmap
(host) [mynode] (config) #crypto map GLOBAL-MAP 10000 ipsec-isakmp dynamic default-dynamicmap
```

Related Commands

Command	Description
show crypto map	Displays IPsec map configurations.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

crypto pki

```
crypto pki
   csr {ec|rsa}
      key_len <key_val>
      curve-name <key_val>
      common_name <common_val>
      country <country_val>
      state_or_province <state>
      city <city_val>
      organization <organization_val>
      unit <unit_val>
      email <email_val>
   expirycheck
   export ca-cert pem self-signed {console|<filename>}
```

Description

Generate a Certificate Signing Request (CSR) for the captive portal feature.

Syntax

Parameter	Description
`csr {ec|rsa}`	Generate a certificate signing request. Execute the **show crypto pki csr** command to view output again. This parameter has the following sub-parameters: ■ **ec**– Generate a certificate signing request with an Elliptic Curve (EC) key. ■ **rsa**– Generate a certificate signing request with a Rivest, Shamir and Adleman (RSA) key.
`key_len <key_val>`	Generate a certificate signing request with an RSA key with one of the following supported RSA key lengths: ■ 1024 ■ 2048 ■ 4096
`curve-name <key_val>`	Generate a certificate signing request with an EC key, with one of the following EC types: ■ secp256r1 ■ secp384r1
`common_name <common_val>`	Specify a common name, e.g., www.yourcompany.com.
`country <country_val>`	Specify a country name, e.g., US or CA.
`state_or_province <state>`	Specify the name of a state or province.
`city <city_val>`	Specify the name of a city.
`organization <organization_val>`	Specify the name of an organization unit, e.g., sales.

Parameter	Description
`unit <unit_val>`	Specify a unit value, e.g. EMEA.
`email <email_val>`	Specify an email address, in the format name@mycompany.com.
`expirycheck`	Run an expiry check on all certificates on the managed device.
`export`	Export self signed PKI CA certificate in **.pem** format.

Usage Guidelines

Use this command in enable mode to generate a CSR for the Captive Portal feature or to see all managed devices certificates are expiring.

Display the CSR output by entering the command **show crypto pki csr**.

Example

The following command configures a CSR for a user with the email address *jdoe@example.com*.

```
(host) [md] #crypto pki csr key 1024 common_name www.example.lcom country US state_or_province ca city Sunnyvale organization engineering unit pubs email jdoe@example.com
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

crypto pki-import

```
crypto pki-import
   {der|pem|pfx|pkcs12|pkcs7}
      CRL
      IntermediateCA
      OCSPResponderCert
      OCSPSignerCert
      PublicCert
      ServerCert
      TrustedCA
       <name> <filename> [<passphrase>]
```

Description

The command imports certificates for the captive portal feature.

Syntax

Parameter	Description
`der`	Import the following certificates in **.der** (Distinguished Encoding Rule) format.
`pem`	Import a certificate in X.509 **.pem** (Privacy-enhanced Electronic Mail) format.
`pfx`	Import a certificate in **.pfx** (Personal inFormation eXchange) format.
`pkcs12`	Import a certificate in **.p12** format.
`pkcs7`	Import a certificate in **.p7c** format.
`CRL`	Import a Certificate Revocation List.
`IntermediateCA`	Import an intermediate Certificate Authority (CA) certificate.
`OCSPResponderCert`	Import an Online Certificate Status Protocol (OCSP) Responder certificate.
`OCSPSignerCert`	Import an OCSP Signer certificate.
`PublicCert`	Import a public certificate.
`ServerCert`	Import a server certificate.
`TrustedCA`	Import a trusted CA certificate.
`<name> <filename> <passphrase>`	■ **name**– Name of the certificate. ■ **filename**– Original imported file name of the certificate. ■ **passphrase**– Optional passphrase for storing the certificate private key. **NOTE:** The passphrase is not stored in the system. It is used during the import process only.

Usage Guidelines

Use this command in enable mode to install a CSR for the Captive Portal feature.

Example

The following command installs a server certificate in **.der** format.

```
(host) [md] #crypto pki-import der ServerCert cert_20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

database synchronize

```
database synchronize
   captive-portal-custom
   period <minutes>
```

Description

This command configures the Mobility Master to synchronize the database with a standby or backup Mobility Master.

Syntax

Parameter	Description
`captive-portal custom`	Synchronizes custom captive portal files.
`period`	Configures the interval for automatic database synchronization.
`<minutes>`	Interval, in minutes. Range is 1 — 25200 minutes.

Usage Guidelines

This command should be executed from the **/mm** node hierarchy. The command takes effect immediately. Use the **database synchronize period** command in config mode to configure the interval for automatic database synchronization.

Example

The following command causes the database on the active Mobility Master to synchronize with the standby in 25 minute intervals.

```
(host) [mynode] (config) #database synchronize period 25
```

Related Commands

Command	Description
database-synchronize	This command synchronizes the Mobility Master database with a standby or backup Mobility Master.
show database	This command displays database synchronization status.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

database-synchronize

```
database-synchronize
```

Description

This command synchronizes the Mobility Master database with a standby or backup Mobility Master.

Syntax

No parameters.

Usage Guidelines

This command should be executed from the enable mode of the Mobility Master and takes effect immediately. If a peer is not configured, the Mobility Master displays an error message **Cannot start database synchronization: peer is not configured**.

Example

The following command invokes the database on the active Mobility Master to synchronize with the standby:

```
(host) [mynode] #database-synchronize
```

Related Commands

Command	Description
database synchronize	This command configures the Mobility Master to synchronizes the database with a standby or backup Mobility Master. This works in config mode.
show database	This command displays database synchronization status.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

datapath

```
datapath {coredump | energy-efficiency}
```

Description

This command configures datapath options.

Syntax

Parameter	Description	Range
`coredump`	Generates a coredump, which is a copy of the datapath memory, in the event that the datapath times out. This copy is saved in the system memory.	—
`energy-efficiency`	Minimizes idle CPU spinning.	—

Example

The following command enables datapath coredump:

```
(host) [mynode] (config) #datapath coredump
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

dds trace

```
dds trace {receive|transmit} [channel <channel>|peer <A.B.C.D>|peerv6 <X:X:X:X::X>]
```

Description

This command configures trace events.

Syntax

Parameter	Description
`receive`	Configures trace receiving events.
`transmit`	Configures trace transmitting events.
`channel`	GSM channel for tracing.
`<channel>`	Name of GSM channel.
`peer`	DDS peer.
`<A.B.C.D>`	Peer IP address.
`peerv6`	DDS IPv6 peer.
`<X:X:X:X::X>`	Peer IPv6 address.

Example

The following command configures a trace receiving event for the radio GSM channel. Use the **show gsm channel** command to view the list of available GSM channels.

```
(host) [mynode] (config) #dds trace receive channel radio peer 10.20.22.17
```

Command History

Version	Description
ArubaOS 8.2.0.0	The **peerv6** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

delete

```
delete
   filename <filename>
   ssh-host-addr <ipaddr>
   ssh-known-hosts
```

Description

This command deletes a file or RSA signature entry from flash.

Syntax

Parameter	Description
`filename`	Name of the file to be deleted.
`ssh-host-addr`	Deletes the entry stored in flash for the RSA host signature created when you run the **copy scp** command.
`ssh-known -hosts`	Deletes all entries stored in flash for the RSA host signatures created when you run the **copy scp** command.

Usage Guidelines

To prevent running out of flash file space, you should delete files that you no longer need. The **copy scp** command creates RSA signatures whenever it connects to a new host. These host signatures are stored in the flash file system.

Example

The following command deletes a file:

```
(host) [mynode] #delete filename december-config-backup.cfg
```

The following command deletes an RSA signature entry from flash:

```
(host) [mynode] #delete ssh-host-addr 10.100.102.101
```

The following command deletes all RSA signature entries from flash:

```
(host) [mynode] #delete ssh-known-hosts
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

delete-wired-blacklist-user

```
delete-wired-blacklist-user <macaddr>
```

Description

This command deletes a wired user from blacklist table.

Syntax

Parameter	Description
`<macaddr>`	MAC address, in the format xx:xx:xx:xx:xx:xx.

Example

The following command deletes a wired user from blacklist table:

```
(host) [mynode] #delete-wired-blacklist-user 00:0b:86:f0:05:60
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

dialer group

```
dialer group <name>
   dial-string <string>
   init-string <string>
   no  ...
```

Description

This command configures a dialer group with dialing parameters for a USB modem.

Syntax

Parameter	Description	Range
`<name>`	Name of the dialer group.	—
`dial-string <string>`	Specifies the modem dial string.	—
`init-string <string>`	Specifies the modem initialization string. The init string can contain carrier-specific dialing options for the USB modem. You can often find these settings in online forums or from your ISP.	—
`no`	Deletes the command.	—

Example

The following command configures dial settings for a USB modem:

```
(host) [mynode] (config) #dialer group gsm_us
   init-string AT+CGDCONT=1,"IP","ISP.CINGULAR"
```

Related Commands

Command	Description
show dialer group	Displays the list of configured dialer groups.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

dir

```
dir [usb:]
```

Description

This command displays a list of files stored in the flash file system.

Syntax

Parameter	Description
`usb:`	Displays the files in the external USB. **NOTE:** This parameter can be executed for managed devices that have an USB port.

Usage Guidelines

Use this command to view the system files associated with the Mobility Master. To view the system file associated with the managed device, login to the Mobility Master and initiate a telnet or SSH session to the managed device.

Output from this command includes the following:

- The first column contains ten place holders that display the file permissions.
  - First place holder: Displays **-** for a file or **d** for directory.
  - Next three place holders: Display file owner permissions: **r** for read access, **w** for write access permissions, **x** for executable.
  - Following three place holders: Display member permissions: **r** for read access or **x** for executable.
  - Last three place holders: Display non-member permissions: **r** for read access or **x** for executable.
- The second column displays the number of links the file has to other files or directories.
- The third column displays the file owner.
- The fourth column displays group/member information.
- The remaining columns display the file size, date and time the file was either created or last modified, and the file name.

Example

The following command displays the files currently residing on the system flash:

```
(host) [mynode] #dir
```

The following is sample output from this command:

```
-rw-r--r--    1 root     root         9338 Nov 20 10:33 class_ap.csv
-rw-r--r--    1 root     root         1457 Nov 20 10:33 class_sta.csv
-rw-r--r--    1 root     root        16182 Nov 14 09:39 config-backup.cfg
-rw-r--r--    1 root     root        14174 Nov  9  2005 default-backup-11-8-05.cfg
-rw-r--r--    1 root     root        16283 Nov  9 12:25 default.cfg
-rw-r--r--    1 root     root        22927 May 25 12:21 default.cfg.2016-05-25_20-21-38
-rw-r--r--    2 root     root        19869 May  9 12:20 default.cfg.2016-05-09_12-20-22
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

disable-whitelist-sync

`disable-whitelist-sync`

Description

This command disables whitelist synchronization with managed devices. Whitelist database synchronization is enabled by default.

Syntax

No parameters.

Usage Guidelines

By default, the whitelist database synchronization is enabled between Mobility Master and managed devices. Once the whitelist database entries are synchronized across all controllers, issue the **disable-whitelist-sync** command to disable synchronization. Configuring this parameter reduces the number of database queries on Mobility Master.

Enabling whitelist database synchronization may increase database process CPU utilization on Mobility Master if there is a large number of whitelist entries and managed devices terminating on the Mobility Master.

Example

The following command disables whitelist synchronization:

```
(host) [mynode] (config) #disable-whitelist-sync
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

disaster-recovery

```
disaster-recovery
   off
   on
```

Description

This command enables or disables disaster recovery mode on the managed device.

Syntax

Parameter	Description
`off`	Disables disaster recovery mode.
`on`	Enables disaster recovery mode.

Usage Guidelines

This command primarily addresses a failure of the auto-recovery mechanism to restore the connectivity disruption between Mobility Master and the managed device caused due to bad configuration synchronization from Mobility Master. In a worst case scenario, while trying to restore the managed device to the last known good configuration ID, the auto-recovery feature might fail and leave the managed device in an intermediate state with the Mobility Master-managed device connectivity still disrupted due to an unfixed configuration issue. In such a scenario, the administrator can enable the disaster recovery mode on the managed device.

This command can be executed from the managed device prompt only. Once you login to the managed device, execute the **disaster-recovery on** command to enter the disaster recovery mode. To exit this mode, execute the **disaster-recovery off** command.

On enabling this mode, the Mobility Master stops configuration synchronization with the managed device. This command is useful for debugging on the managed device and stop configuration synchronization during the process.

Configuration changes made on the managed device in the disaster recovery mode continues to remain even after the managed device establishes connectivity with Mobility Master and configuration synchronization is started. Configuration changes in the disaster recovery mode overrides the configuration synchronization unless manually deleted from the managed device.

Example

The following command enables the disaster recovery mode in the managed device:

```
(host-md) #disaster-recovery on

******************************
Entering disaster recovery mode
******************************
(DR-Mode) [mm] #
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable mode on Managed device

dot1x

```
high-watermark <1-32000>
stm-throttling percent <10-80> {multi-version}
```

Use this command only under the supervision of Aruba support.

Description

Use this command under the guidance of Aruba support to configure the maximum and minimum thresholds for the table that contains 802.1X sessions.

Syntax

Parameter	Description	Range
`high-watermark`	The maximum entries in the **Active** table. When the number of entries in the **Active** table reaches the **High Water Mark** value, new requests are queued on the **Pending** table.	1-32000 entries
`stm-throttling-percent <10-80>`	Enables STM throttling when the total entries in the **Pending** table are greater than (stm-throttling percent) * (high watermark). The default STM throttling percent is 50%.	10-80%
`multi-version`	Enables dummy multi-version check.	

Example

The following command sets the **High Water Mark** value to 200 entries:

```
(host) [mynode] (config) #dot1x high-watermark 200
```

Related Commands

Command	Description
show dot1x watermark	Displays information about the table that contains 802.1X sessions.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **multi-version** sub-parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

downloadable-role-delete

```
downloadable-role-delete STRING
```

Description

This command deletes a corrupted role downloaded from ClearPass Policy Manager.

Syntax

Parameter	Description
`STRING`	Downloadable role name.

Usage Guidelines

You can delete a downloadable role under the following conditions:

- If no user references the role
- If the role is in **Complete** or **Incomplete** state

Example

The following command deletes the *abc_profile-3023-8* user role:

```
(host) [mynode] #downloadable-role-delete abc_profile-3023-8
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

dpi

```
dpi
   app <string> ports [tcp <tportlist>][udp <uportlist>]
   appcategory <string> <categoryID>
   custom-app <appname> <appid> [appcategory|http {hostname-param <hostname> uri-param
     <uri>|referer-param <referer>}|https {common-name <commonname>}]
   global-bandwidth-contract {app <string>[downstream|upstream][kbits <256..2000000>|mbits
     <1..2000>}|appcategory <string>[downstream |upstream][kbits|mbits <value>}
   proto-bundle activate <string>
```

Description

This command configures DPI and the global bandwidth contract for an application or application category for the AppRF feature, and allows network administrators to define custom applications for use with DPI features.

Syntax

Parameter	Description	Range
`app <string>`	Name of the application for which you want to enable DPI. For a complete list of supported applications, issue the command **show dpi application all**.	—
`tcp <tportlist>`	Enables DPI on the selected TCP port(s). You can enter a range of ports (for example, **80-85**), or enter multiple individual port numbers separated by a comma (or example, **40,44,48**).	—
`udp <uportlist>`	Enables DPI on the selected TCP port(s). You can enter a range of ports (for example, **80-85**), or enter multiple individual port numbers separated by a comma (or example, **40,44,48**).	—
`appcategory`	Configures an application category.	—
`<string>`	Name of the application category. Allowed characters include: ■ a-z ■ 0-9 ■ "_" and "-"	—
`<categoryid>`	Sets a unique category ID.	1-32
`custom-app`	Creates a new custom application.	—
`<appname>`	Name of the custom application. Allowed characters include: ■ a-z ■ 0-9 ■ "_"	—
`<appID>`	Sets a unique application ID.	1-64
`appcategory`	Application category name.	—

Parameter	Description	Range
`http`	Creates a new HTTP-based custom application	—
`hostname-param <hostname> uri-param <uri>`	Specifies a hostname and URI to create an application based upon that server name and URI	—
`referer-param <referer>`	A referrer is the URL of a webpage from which a link was followed.Specify a referrer to create a HTTP referrer-based application.	—
`https`	Create a new HTTPS-based custom application	—
`common-name <commonname>`	Specify a CN to create an application based on it.	—
`global-bandwidth-contract`	Configures the global bandwidth contract for an application or application category.	256 kbps-2 gbps
`app <string>`	Name of the application. For a complete list of supported applications, issue the command **show dpi application all**. Applications can also be user-defined. Issue the **show dpi custom-app all** command to view all user-defined (custom) applications.	—
`appcategory <string>`	Name of the application category. For a complete list of supported application categories, issue the command **show dpi application category all**. Application categories can also be user-defined. Issue the **show dpi application category user-defined all** command to view all user-defined (custom) categories.	—
`downstream`	Bandwidth contract to downstream traffic.	—
`upstream`	Bandwidth contract to upstream traffic.	—
`kbits <value>`	Specifies bandwidth in kbits per second.	256-2000000 kbits
`mbits <value>`	Specifies bandwidth in mbits per second.	1-2000 mbits
`proto-bundle activate <STRING>`	After downloading a new protocol database image using the copy command, you must activate it by issuing the **proto-bundle activate <string>** command, where <string> is the name of the .txt protocol bundle file.	—

Usage Guidelines

You can configure bandwidth contracts to limit application and application categories on an application or global level.

Applications and application categories can be user-defined. Issue the **show dpi custom-app all** command to view all user-defined (custom) applications and the **show dpi application category user-defined all** command to view all user-defined categories.

Example

The following command configures a global bandwidth contract for downstream traffic:

```
(host) [md] (config) #dpi global-bandwidth-contract appcategory web downstream kbits 10000
```

Use the following commands to view global bandwidth contract configuration outputs:

```
(host) [md] #show dpi global-bandwidth-contract all
(host) [md] #show dpi global-bandwidth-contract application name
(host) [md] #show dpi global-bandwidth-contract appcategory name
```

Related Commands

Command	Description
show dpi	Displays the applications and application categories that are configured for Deep-Packet Inspection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

drop-cache

`drop-cache`

Description

This command frees unused or dirty memory from Mobility Master.

Syntax

No parameters.

Usage Guidelines

This command can be executed when Mobility Master has low memory. Execute this command under the supervision of Aruba TAC.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

dynamic-ip

```
dynamic-ip restart
```

Description

This command restarts the PPPoE or DHCP process.

Syntax

No parameters.

Usage Guidelines

This command can be used to renegotiate DHCP or PPPoE parameters. This can cause new addresses to be assigned on a VLAN where the DHCP or PPPoE client is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

eject usb

```
eject usb: slot {all|<slotno>}
```

Description

This command ejects an external USB device from the managed device.

Syntax

No parameters.

Parameter	Description
`all`	Eject all external USB devices.
`<slotno>`	Enter optional slot number to eject the USB device.

Usage Guidelines

Use this command to safely remove an external USB device. This command should be executed from the managed device only.

Example

This command ejects all external USB devices from the managed device.

```
(host-md) #eject usb: slot all
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Managed Device

encrypt

```
encrypt {disable|enable}
```

Description

This command allows passwords and keys to be displayed in plain text or encrypted.

Syntax

Parameter	Description	Default
`disable`	Passwords and keys are displayed in plain text.	—
`enable`	Passwords and keys are displayed in encrypted form.	enabled

Usage Guidelines

Certain commands, such as **show crypto isakmp key**, display configured key information. Use the **encrypt** command to display the key information in plain text or encrypted.

Example

The following command allows passwords and keys to be displayed in plain text:

```
(host) [mynode] #encrypt disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

esi group

```
esi group <group_inst> [ping <attributes>|server <server>]
```

Description

This command configures an ESI group.

Syntax

Parameter	Description	Range
`<group_inst>`	Specifies the ESI group configuration.	—
`ping <ping>`	Specifies a set of ping checking attributes. Only one set is allowed.	—
`server <server>`	Adds or removes a server from the ESI group.	—

Usage Guidelines

Use the **show esi groups** command to view ESI group information.

Example

The following command sets up the ESI group named “fortinet”:

```
(host) [md] (config) #esi group fortinet
  ping default
  server forti_1
```

Related Commands

Command	Description
show esi groups	Displays ESI group information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master.

esi parser domain

```
esi parser domain <domain-name>
   peer <peer-ip>
   server <ipaddr>
```

Description

This command configures an ESI syslog parser domain.

Syntax

Parameter	Description	Range
`<domain-name>`	ESI parser domain name.	—
`peer <peer-ip>`	Specifies the IP address of an another managed device in this domain, which is notified when the user cannot be found locally. This command is required only when multiple managed devices share a single ESI server.	—
`server <ipaddr>`	Specifies the IP address of the ESI server to which the managed device listens.	—

Usage Guidelines

The ESI parser is a generic syslog parser that accepts syslog messages from external third-party appliances, such as anti-virus gateways, content filters, and intrusion detection systems. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users.

ESI servers (see esi server on page 449) are configured into domains to which ESI syslog parser rules (see esi parser rule on page 444) are applied.

Example

The following commands configure a virus syslog parser domain named “fortinet” that contains the ESI server “forti_1” with a trusted IP address:

```
(host) [md] (config) #esi parser domain fortinet
   server 10.168.172.3
```

Related Commands

Command	Description
show esi parser	Displays information about the ESI parser domains.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master.

esi parser rule

```
esi parser rule <rule_name>
   condition <string>
   domain <word>
   enable
   match {ipaddr <string>|mac <string>|user <string>}
   no
   position <1-32>
   set {blacklist|role <word>}
   test {msg <syslog>|file <filename>}
```

Description

This command creates or changes an ESI syslog parser rule.

Syntax

Parameter	Description	Range	Default
`<rule-name>`	Name of the ESI parser rule.	—	—
`condition <string>`	Specifies the REGEX (regular expression) pattern that uniquely identifies the syslog.	—	—
`domain <word>`	(Optional) Specifies the ESI syslog parser domain to which this rule applies. If not specified, the rule matches with all configured ESI servers.	—	—
`enables`	Enables this rule. **Note**: The condition, user match, and set action parameters must be configured before the rule can be enabled.	—	Disabled
`match`	Specifies the user identifier to match, where **ipaddr**, **mac**, and **user** take a REGEX pattern that uniquely identifies the user.	—	—
`ipaddr <string>`	Matches using the client IP address.	—	—
`mac <string>`	Matches using the client MAC address.	—	—
`user <string>`	Matches using the client user name.	—	—
`no`	Negates any configured parameter.	—	—
`position`	Specifies the rule's priority position.	1–32; 1 highest	—
`set`	Specifies the action to take. **Note**: The role entity should be configured before it is accepted by the ESI rule.	—	—
`blacklist`	Blacklists the user.	—	—
`role <word>`	Changes the user role.	—	—

Parameter	Description	Range	Default
`test`	Tests the regular expression output configured in the **esi parser rules** command.	—	—
`msg <syslog>`	Tests the rule against a syslog message.	—	—
`file <filename>`	Tests the rule against a syslog file.	—	—

Usage Guidelines

The user creates an ESI rule by using characters and special operators to specify a pattern that uniquely identifies a syslog message. This "condition" defines the type of message and the ESI domain to which this message pertains. The rule contains three major fields:

- **Condition**: The pattern that uniquely identifies the syslog message type.
- **User**: The username identifier. It can be in the form of a name, MAC address, or IP address.
- **Action**: The action to take when a rule match occurs.

Once a condition match occurs, no further rule-matching will be made. For the matching rule, only one action can be defined.

For more details on the character-matching operators, repetition operators, and expression anchors used to defined the search or match target, refer to the *External Services Interface*chapter in the *ArubaOS 8.3.0.x User Guide* .

Use the **show esi parser rules** command to show ESI parser rule information. Use the **show esi parser stats** command to show ESI parser rule statistical information

Examples

The following command sets up the Fortigate virus rule named "forti_rule." This rule parses the virus detection syslog scanning for a condition match on the log_id value (log_id=) and a match on the IP address (src=).

```
(host) [md] (config) #esi parser rule forti_rule
   condition "log_id=[0-9]{10}[ ]"
   match ipaddr "src=(.*)[ ]"
   set blacklist
   domain fortinet
   enable
```

In this example, the corresponding ESI expression is:

```
< Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
```

The following example of the test command tests a rule against a specified single syslog message:

```
(host) [md] (config) #esi parser rule test msg "26 18:30:02 log_
id=0100030101 type=virus subtype=infected src=1.2.3.4"

< 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
=====
Condition:     Matched with rule "forti_rule"
User:          ipaddr = 1.2.3.4
=====
```

The following example of the test command tests a rule against a file named test.log, which contains several syslog messages:

```
(host) [md] (config) #esi parser rule test file test.log

 < Sep 26 18:30:02 log_id=0100030101 type=virus subtype=infected src=1.2.3.4 >
==========
```

```
Condition:      Matched with rule "forti_rule"
User:           ipaddr = 1.2.3.4
==========

 < Oct 18 10:43:40  cli[627]: PAPI_Send: To: 7f000001:8372 Type:0x4 Timed out. >
==========
Condition:      No matching rule condition found
==========

 < Oct 18 10:05:32  mobileip[499]: <500300> <DBUG> |mobileip|  Station 00:40:96:a6:a1:a4,
10.0.100.103: DHCP FSM received event: RECEIVE_BOOTP_REPLY current: PROXY_DHCP_NO_PROXY,
next: PROXY_DHCP_NO_PROXY >
==========
Condition:      No matching rule condition found
==========
```

Related Commands

Command	Description
show esi parser	Displays configuration information for the ESI parser rules.
show esi parser	Displays statistics information for the ESI parser rules.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms.	Requires the PEFNG license	Config mode on Mobility Master.

esi ping

```
esi ping <ping_inst>
   frequency <frequency_inst>
   no
   retry-count <retry-count_inst>
   timeout <timeout_inst>
```

Description

This command specifies the ESI ping health check configuration.

Syntax

Parameter	Description	Range	Default
`<ping_inst>`	Specifies the ping health check configuration.	—	—
`frequency <frequency_inst>`	Specifies the ping frequency, in seconds.	1–65536 seconds	5 seconds
`no`	Negates any configured parameter.	—	—
`retry-count <retry-count_inst>`	Specifies the ping retry count.	1–65536	2
`timeout <timeout_inst>`	Specifies the ping timeout, in seconds.	1–65536 seconds	2 seconds

Usage Guidelines

Use the show esi ping command to show ESI ping information.

Example

The following command specifies the ping health check attributes.

```
(host) [md] (config) #esi ping default
   frequency 5
   retry-count 2
   timeout 2
```

Related Commands

Command	Description
show esi ping	Displays ESI ping information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master.

esi server

```
esi server <server_inst>
   dport <tcp-udp-port>
   mode {bridge|nat|route}
   no
   trusted-ip-addr <trusted-ip-addr_inst> [health-check]
   trusted-port <slot/port>] |
   untrusted-ip-port <untrusted-ip-addr_inst> [health-check]
   untrusted-port <slot/port>
```

Description

This command configures an ESI server.

Syntax

Parameter	Description	Range
`<server_inst>`	Specifies the ESI server configuration.	—
`dport <tcp-udp-port>`	Specifies the NAT destination TCP or UDP port.	—
`mode`	Specifies the ESI server mode of operation: ■ **bridge**: ESI server operates as a transparent bridge ■ **nat**: NAT destination addresses for the ESI server ■ **route**: ESI server operates as a router	—
`no`	Negates any configured parameter.	—
`trusted-ip-addr <trusted-ip-addr_inst>`	Specifies the server IP address on the trusted network. As an option, you can also enable a health check on the specified address	—
`trusted-port <slot/port>`	Specifies the port connected to the trusted side of the ESI server. The interface must be in <slot>/<port> format.	—
`untrusted-ip-addr <untrusted-ip-addr_inst>`	Specifies the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address	—
`untrusted-port <slot/port>`	Specifies the port connected to the untrusted side of the ESI server. The interface must be in <slot>/<port> format.	—

Example

The following command specifies the ESI server attributes:

```
(host) [md] (config) #esi server forti_1
   mode route
   trusted-ip-addr 10.168.172.3
   untrusted-ip-addr 10.168.171.3
```

Related Commands

Command	Description
show esi servers	Displays configuration information for ESI servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master.

est

```
est profile <profile_name>
   arbitrary-label <arbitrary-label>
   challenge-password <challenge-password>
   clone <source>
   server-host <server-host>
   server-port <server-port>
   trustanchor-name <trustanchor-name>
   no..
```

Description

This command configures an EST profile on the Controller. This configuration is then pushed to the AP on successful enrollment.

Syntax

Parameter	Description
`profile <profile_name>`	Denotes the profile name of the EST profile.
`arbitrary-label <arbitrary-label>`	Sets an arbitrary label for the EST URI to distinguish it from the other EST profiles running on the EST server.
`challenge-password <challenge-password>`	Sets a challenge password used in CSR.
`clone <source>`	Name of an existing EST profile from which parameter values are copied.
`server-host <server-host>`	Denotes the IPv4 address or the hostname of the EST server.
`server-port <server-port>`	Indicates the port value of the EST server. The default value is 443.
`trustanchor-name <trustanchor-name>`	Denotes the server's trustanchor.
`no..`	Deletes the configuration.

Usage Guidelines

Use this command to configure an EST profile on the Controller.

Example

The following command configures an EST profile:

```
(host) [mynode] (config)# est profile est-new
(host) [mynode] (est profile "est-new" )# server-host 10.15.33.232
(host) [mynode] (est profile "est-new" )# server-port 443
(host) [mynode] (est profile "est-new" )# arbitrary-label /ca:2
(host) [mynode] (est profile "est-new" )# challenge-password pass123
(host) [mynode] (est profile "est-new" )# trustanchor-name trust456
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode and config submode on Mobility Master

est-activate

```
est-activate <profile_name>
```

Description

This command is used to activate an existing EST profile on the Controller or the AP.

Syntax

Parameter	Description
`<profile_name>`	Denotes the profile name of the EST profile to be activated.

Usage Guidelines

Use this command to activate an EST profile on the Controller or the AP.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

exit

```
exit
```

Description

This command exits the current CLI mode.

Syntax

No parameters.

Usage Guidelines

Upon entering this command in a configuration submode, you are returned to the configuration mode. Upon entering this command in configuration mode, you are returned to the enable mode. Upon entering this command in enable mode, you are returned to the user login.

Example

The following sequence of **exit** commands return the user from the interface configuration sub-mode to the user login:

```
(host) [mynode] (config-if) #exit
(host) [mynode] (config) #exit
(host) [mynode] #exit
User:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

export

```
export gap-db <filename>
```

Description

This command exports the global AP database to the specified file.

Syntax

Parameter	Description
`<filename>`	Name of the file to which the global AP database is exported.

Usage Guidelines

This command is intended for system troubleshooting. You should run this command only when directed to do so by an Aruba support representative.

The global AP database resides on Mobility Master and contains information about known APs on all managed devices in the system. You can view the contents of the global AP database with the **show ap database** command.

Example

The following command exports the global AP database to a file:

```
(host) [mynode] #export gap-db global-ap-db
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

extimfgr

```
extifmgr verose-log
```

Description

This command enables debug logs for the external interface manager process in Mobility Master.

Syntax

No parameters.

Usage Guidelines

The external interface manager process communicates with third-party applications like Palo Alto Networks firewall. Execute this command under the supervision of Aruba TAC.

Example

The following command exports the global AP database to a file:

```
(host) [mynode] #extifmgr verbose-log
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

file syncing profile

```
file syncing profile
   file-syncing-enable
   no
   sync-time <sync-time>
```

Description

This command allows the user to configure the file syncing profile.

Syntax

Parameter	Description	Range	Default
`file-syncing-enable`	Enables file syncing on the managed device.	—	Enabled
`no`	Negates any configured parameter.	—	—
`sync-time <sync-time>`	Configures the time between file syncs, in minutes.	30 -180 minutes	30 minutes

Usage Guidelines

This command enables or disables the file syncing. Additionally, the time between syncs can be configured as part of the file syncing profile.

Example

The following example shows how to enable the file syncing:

```
(host) [md] (config) #file syncing profile
(host) (File syncing profile) #file-syncing-enable
```

Related Commands

Command	Description
show file syncing profile	Displays the configured file syncing profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master.

fips

```
fips [disable|enable]
```

This command applies only to the FIPS version of ArubaOS.

Description

This command enables and disables the FIPS mode of operation.

Syntax

Parameter	Description
`enable`	Enables the FIPS mode of operation.
`disable`	Disables the FIPS mode of operation.

Usage Guidelines

This command enables or disables the FIPS mode of operation.

Example

The following example shows how to enable the FIPS mode of operation:

```
(host) [md] #fips enable
```

Related Commands

Command	Description
show fips	Indicates if FIPS is enabled or disabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Enable mode on Mobility Master.

firewall

```
firewall
   allow-tri-session
   amsdu
   attack-rate
           arp <1-16384> {blacklist|drop}
           cp <1-16384>
           grat-arp <1-16384> {blacklist|drop}
           ping <1-16384>
           session <1-16384>
           tcp-syn <1-16384>

   bwcontracts-subnet-broadcast
   cp-bandwidth-contract
   deny-inter-user-bridging
   deny-inter-user-traffic
   deny-source-routing
   disable-ftp-server
   dpi
   drop-ip-fragments
   enable-bridging
   enable-per-packet-logging
   enforce-tcp-handshake
   enforce-tcp-sequence
   gre-call-id-processing
   imm-fb
   jumbo
   local-valid-users
   log-icmp-error
   optimize-dad-frames
   prevent-dhcp-exhaustion
   prohibit-arp-spoofing
   prohibit-ip-spoofing
   prohibit-rst-replay
   public-access
   session-idle-timeout <seconds>
   session-mirror-destination
   session-mirror-ipsec
   session-tunnel-fib
   session-voip-timeout
   shape-mcast
   stall-crash
   voip-wmm-content-enforcement
   web-cc
   web-cc-cache-miss-drop
   wireless-bridge-aging
```

Description

This command configures firewall options on the managed device.

Syntax

Parameter	Description	Range	Default
`allow-tri-session`	Allows three-way session when performing destination NAT. This option should be enabled when the managed device is not the default gateway for wireless clients and the default gateway is behind the managed device. This option is typically used for captive portal configuration.	—	disabled
`amsdu`	Aggregated Medium Access Control Service Data Units (AMSDU) packets are dropped if this option is enabled.	–	disabled

`attack-rate`
`arp <1-16384> {blacklist|drop}`
`cp <1-16384>`
`grat-arp <1-16384> {blacklist|drop}`
`ping <1-16384>`
`session <1-16384>`
`tcp-syn <1-16384>`
	Sets rates which, if exceeded, can indicate a denial of service attack.
	■ **arp**: Monitor/police ARP attack (non Gratuitous ARP).
	■ **cp**: Monitor/police control processor attack.
	■ **grat-arp**: Monitor/police Gratuitous ARP attack.
	■ **ping**: Monitor ping attack.
	■ **session**: Monitor IP session attack.
	■ **tcp-syn**: Monitor TCP SYN attack.
	NOTE: <1-16384> denotes the number of arp, cp, grat-arp, ping, session, or tcp-syn requests per 30 seconds.
		1-16384	—

`bwcontracts-subnet-broadcast`	Applies bw contracts to local subnet broadcast traffic.	—	—
`cp-bandwidth-contract`	See firewall cp-bandwidth-contract on page 468		
`deny-inter-user-bridging`	Prevents the forwarding of Layer2 traffic between wired or wireless users. You can configure user role policies that prevent Layer3 traffic between users or networks but this does not block Layer2 traffic. This option can be used to prevent traffic, such as Appletalk or IPX from being forwarded. If enabled, traffic (all non-IP traffic) to untrusted port or tunnel is also blocked.	—	disabled

Parameter	Description	Range	Default
deny-inter-user-traffic	Denies downstream traffic between users in a wireless network (untrusted users) by disallowing layer2 and layer3 traffic. This parameter does not depend on the **deny-inter-user-bridging** parameter being enabled or disabled.	—	disabled
deny-source-routing	Disallows forwarding of IP frames with source routing with the source routing options set.	–	disabled
disable-ftp-server	Disables the FTP server on the managed device. Enabling this option prevents FTP transfers. Enabling this option could cause APs to not boot up. You should not enable this option unless instructed to do so by an Aruba representative.	—	disabled
dpi	Enables DPI	—	disabled
drop-ip-fragments	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by an Aruba representative.	—	disabled
enable-bridging	Enables bridging when the managed device is in factory default.	—	disabled
enable-per-packet-logging	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by an Aruba representative, as doing so may create unnecessary overhead on the managed device.	—	disabled
enforce-tcp-handshake	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.	—	disabled

Parameter	Description	Range	Default
`enforce-tcp-sequence`	Enforces the TCP sequence numbers for all packets.	—	disabled
`gre-call-id-processing`	Creates a unique state for each PPTP tunnel. Do not enable this option unless instructed to do so by a technical support representative.	—	disabled
`imm-fb`	Immediately free buffers on managed device. Do not enable this option unless instructed to do so by a technical support representative.	—	disabled
`jumbo`	Enables jumbo frames processing.	—	disabled
`local-valid-users`	Adds only IP addresses, which belong to a local subnet, to the user-table.	—	disabled
`log-icmp-error`	Logs received ICMP errors. You should not enable this option unless instructed to do so by a customer support representative.	—	disabled
`optimize-dad-frames`	Reduce flooding of IPv4 Gratuitous ARPs/IPv6 Duplicate Address Detection frames onto wireless clients.	—	enabled
`prevent-dhcp-exhaustion`	Enable check for DHCP client hardware address against the packet source MAC address. This command checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. Enabling this feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.	—	disabled
`prohibit-arp-spoofing`	Detects and prohibits arp spoofing. When this option is enabled, possible arp spoofing attacks are logged and an SNMP trap is sent.	—	disabled

Parameter	Description	Range	Default
prohibit-ip-spoofing	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, source and destination IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	enabled in IPv4 disabled in IPv6
prohibit-rst-replay	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by an Aruba representative.	—	disabled
session-idle-timeout	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by an Aruba representative.	16-300	16
session-mirror-destination	This parameter is deprecated. Use the packet-capture command.	–	—
session-mirror-ipsec	This parameter is deprecated. Use the packet-capture command.	—	—
session-tunnel-fib	Enable session tunnel-based forwarding. **NOTE:** Best practices is to enable this parameter only during maintenance window or off-peak production hours. On the M3, this parameter only enables tunnel-based forwarding, as session-based forwarding does not apply to this platform.	–	disabled
session-voip-timeout	Idle session timeout, in seconds, for sessions that are marked as voice sessions. If no voice packet exchange occurs over a voice session for the specified time, the voice session is removed.	16-300	300 seconds
shape-mcast	Enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.	—	disabled

Parameter	Description	Range	Default
`stall-crash`	Triggers datapath crash on stall detection. Applies to the to 7200 Series managed device only.	—	enabled
`voip-wmm-voip-content-enforcement`	If traffic to or from the user is inconsistent with the associated QoS policy for voice, the traffic is reclassified to best effort and data path counters incremented. This parameter requires the PEFNG license.	—	disabled
`web-cc`	Enables web content classification for all HTTP traffic. Once enabled, ArubaOS enforces ACLs and bandwidth policies associated with web content categories or reputation levels. **NOTE:** On enabling web-cc, the web-cc feature usage information will be sent to Aruba at every 7 days interval.	—	disabled
`web-cc-cache-miss-drop`	Issue this command to allow the managed device to drop any packets that do not match any web content category or reputation levels in the managed device's internal web content cache.	—	disabled
`wireless-bridge-aging`	Issue this command to prevent the aging of wireless client associated with AP.	—	disabled

Usage Guidelines

This command configures global firewall options on the managed device.

Example

The following command disallows forwarding of non-IP frames between users:

```
(host)[/md] (config) #firewall deny-inter-user-bridging
```

Related Commands

Release	Modification
firewall cp	Creates whitelist session ACLs.
firewall cp-bandwidth-contract	Configures bandwidth contract traffic rate limits, in packets per second, to prevent denial of service attacks.
show firewall	Display a list of global firewall policies.

Command History

Version	Description
ArubaOS 8.2.0.0	The **wireless-bridge-aging** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system except the **voip-wmm-voip-content-enforcement** parameter which requires the PEFNG license.	Config mode on Mobility Master.

firewall cp

```
firewall cp
   ipv4|ipv6 deny|permit <ip-addr><ip-mask>|any|{host <ip-addr>} proto{<ip-protocol-number>
   ports <start port number><end port number>}|ftp|http|https|icmp|snmp|ssh|telnet|tftp
   [bandwidth-contract <name>|<pbwm>]
   no...
```

Description

This command creates whitelist session ACLs. Whitelist ACLs consist of rules that explicitly permit or deny session traffic from being forwarded or not to the managed device. This prohibits traffic from being automatically forwarded to the managed device if it was not specifically denied in a blacklist. The maximum number of entries allowed in the whitelist is 64.

Syntax

Parameter	Description	Range	Default
`ipv4|ipv6`	Specifies ipv4 or ipv6.	—	—
`deny|permit <ip-addr><ip-mask>`	Specifies the entry to reject (deny) on the session ACL whitelist. Specifies an entry that is allowed (permit) on the session ACL whitelist.	—	—
`any`	Specifies any IPv4 or IPv6 source address.	—	—
`host <ip-addr>`	Indicates a specific IPv4 or IPv6 source address.	—	—
`proto`	Specify one of the following protocols used by the session traffic: ■ **ftp** ■ **http** ■ **https** ■ **icmp** ■ **scmp** ■ **ssh** ■ **telnet** ■ **tftp**	—	—
`IP protocol number`	Specifies the IP protocol number that is permitted or denied.	1-255	—
`start port`	Specifies the starting port, in the port range, on which session traffic is running.	1-65535	—
`end port`	Specifies the last port, in the port range, on which session traffic is running.	1-65535	—
`bandwidth-contract <name>`	Specify the name of a bandwidth contract. configures a bandwidth contract traffic rate, which can then be associated with a whitelist session ACL	—	—
`<name>`	Name of a bandwidth contract.	—	—
`<pbwm>`	Bandwidth rate in packets/seconds.	1–64000	—

Usage Guidelines

This command turns the session ACL from a blacklist to a whitelist. A rule must exist that explicitly permits the session before it is forwarded to the managed device and the last rule in the list denies everything else.

Example

The following command creates a whitelist ACL that allows on with the source address as 10.10.10.10 and the source mask as 2.2.2.2. The protocol is FTP and the bandwidth contract name is mycontract.

```
(host) [/md] (config-fw-cp) #ipv4 permit 10.10.10.10 2.2.2.2 proto ftp bandwidth-contract name mycontract
```

The following command creates a whitelist ACL entry that denies traffic using protocol 2 on port 5000 from being forwarded to the managed device:

```
(host) [/md] (config-fw-cp) #deny proto 6 ports 5000 6000
```

The following example configures a bandwidth contract named “cp-rate” with a rate of 100 pps.

```
(host) [/md] (config) #cp-bandwidth-contract cp-rate pps 100
```

Related Commands

Command	Description	Mode
show firewall-cp	Show Control Processor (CP) whitelist ACL info.	Enable or Config modes

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system, except for noted parameters.	Config mode on Mobility Master.

firewall cp-bandwidth-contract

```
firewall cp-bandwidth-contract {arp-traffic|auth|ike <rate>|l2-other|route|sessmirr|trusted-
mcast|trusted-ucast
|untrusted-mcast|untrusted-ucast}
```

Description

This command configures bandwidth contract traffic rate limits, in packets per second, to prevent denial of service attacks.

Syntax

Parameter	Description	Range	Default
`arp-traffic`	Specifies the arp traffic rate limit in packets per second. Is applied as a multiples of 32 in datapath.	1-65535 pps	976 pps
`auth`	Specifies the traffic rate limit that is forwarded to the authentication process.	1-65535 pps	976 pps
`ike <rate>`	Specifies the traffic rate limit from IKE to CP, in packets per second.	1-65535 pps	976 pps
`l2-other`	Specifies the traffic rate limit for L2 protocol and L2 special handling traffic.	1-65535 pps	976 pps
`route`	Specifies the traffic rate limit that needs ARP requests.	1-65535 pps	976 pps
`sessmirr`	Specifies the session mirrored traffic forwarded to the managed device.	1-65535 pps	976 pps
`trusted-mcast`	Specifies the trusted multicast traffic rate limit.	1-65535 pps	1953 pps
`trusted-ucast`	Specifies the trusted unicast traffic rate limit.	1-98304 pps	—
`untrusted-mcast`	Specifies the untrusted multicast traffic rate limit.	1-65535 pps	1953 pps
`untrusted-ucast`	Specifies the untrusted unicast traffic rate limit.	1-65535 pps	9765 pps
`vrrp`	Specifies the rate limit of VRRP traffic routed to the control plane.	1-65535 pps	9765 pps

Usage Guidelines

This command configures firewall bandwidth contract options on the managed device.

Example

The following command disallows forwarding of non-IP frames between users:

```
(host) [/md] (config) #firewall deny-inter-user-bridging
```

Related Commands

Command	Description
show firewall	Displays a list of global firewall policies and policy details.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license.	Config mode on Mobility Master.

firewall-visibility

```
firewall-visibility
   no ...
```

Description

Enables or disables policy enforcement firewall visibility feature.

Syntax

No parameters.

Usage Guideline

When you enable this feature, the **Firewall Monitoring** page on the **Dashboard** tab of the WebUI displays the summary of all sessions in the controller aggregated by users, devices, destinations, applications, WLANs, and roles.

Example

The following command enables firewall visibility.

```
(host) [/md] (config) #firewall-visibility
```

Related Commands

Command	Description	Mode
show firewall-visibility	Displays the policy enforcement firewall visibility process state and status information	Config or Enable mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license	Config mode on Mobility Master.

gateway health-check

```
gateway health-check
   <interval> <threshold>
```

Description

This command configures the default gateway health check for the managed device.

The managed device is rebooted if the default gateway becomes unreachable.

Syntax

Parameter	Description	Range
`<interval>`	Health check interval.	30-600 seconds
`<threshold>`	Number of missed pings before the managed device reboots.	3-64

Example

The following command configures the default gateway health check with an interval of 60 seconds and threshold of 10:

```
(host) [/md] (config) #gateway health-check 60 10
```

Related Commands

Command	Description
show gateway health-check	Displays the current status of the gateway health check feature.

History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

guest-access-email

```
guest-access-email
   smtp-port <port>
   smtp-server
   no
```

Description

This command configures the SMTP server that is used to send guest emails. Guest emails are generated when a guest user account is created or when the Guest Provisioning user sends a guest user account email at a later time.

Syntax

Parameter	Description	Range	Default
`smtp-port <port>`	Identifies the SMTP port through which the guest-access email is sent.	1–65535	25
`smtp-server <IP-Address>`	The SMTP server to which the guest-access email is sent.	—	—
`no`	Deletes the command configuration	—	—

Usage Guidelines

As part of the guest provisioning feature, the **guest-access-email** command allows you to set up the SMTP port and server that process guest provisioning email. This email process sends email to either the guest or the sponsor whenever a guest user account is created or when the Guest Provisioning user manually sends email from the **Guest Provisioning** page.

Example

The following command creates a guest-access email profile and sends guest user email through SMTP server IP address 1.1.1.1 on port 25:

```
(host) [mynode] (config) #guest-access-email
(host) [mynode] (Guest-access Email Profile) #
(host) [mynode] (Guest-access Email Profile) #smtp-port 25
(host) [mynode] (Guest-access Email Profile) #smtp-server 1.1.1.1
```

Related Commands

```
(host) #show guest-access-email
```

Command	Description
show guest-access-email	Displays the guest access email profile configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

ha

```
ha group-membership <group-membership>
ha group-profile <profile-name>
   clone <source>
   controller <ip> role {active|dual|standby}
   controller-v6 <ipv6> role {active|dual|standby}
   heartbeat
   heartbeat-interval <heartbeat-interval>
   heartbeat-threshold <heartbeat-threshold>
   no
   over-subscription
   pre-shared-key <pre-shared-key>
   preemption
   state-sync
```

Description

This command configures the High Availability:Fast Failover feature by assigning a managed device or standby controller to a high-availability group, and defining the deployment role for each controller.

Parameter	Description	Range	Default
`group-membership <group-membership>`	Displays the high availability group in which the managed device or standby controller is a member.	—	—
`ha group-profile <profile-name>`	Creates a new high availability group, or define settings for an existing group.	—	—
`clone <source>`	Name of an existing high availability profile from which parameter values are copied.	—	—
`controller <ip>`	IPv4 address of a controller that should be added to the specified high availability group.	—	—
`role`	Assign one of the following roles to each controller in the high availability group. ■ **Active**: Controller is active and is serving APs. ■ **Dual**: Controller serves some APs and acts as a standby controller for other APs. ■ **Standby**: Controller does not serve APs, as only acts as a standby in case of failover.	—	—
`controller-v6 <ipv6>`	IPv6 address of a controller that should be added to the specified high availability group.	—	—

Parameter	Description	Range	Default
`role`	Assign one of the following roles to each controller in the high availability group. ■ **Active**: Controller is active and is serving APs. ■ **Dual**: Controller serves some APs and acts as a standby controller for other APs. ■ **Standby**: Controller does not serve APs, as only acts as a standby in case of failover.	—	—
`heartbeat`	The high availability inter-controller heartbeat feature allows for faster AP failover from an active controller to a standby controller, especially in situations where the active controller reboots or loses connectivity to the network.	—	—
`heartbeat-interval <heartbeat-interval>`	Enter a heartbeat interval in the **Heartbeat Interval** field to define how often inter-controller heartbeats are sent.	100-1000 ms	100 ms
`heartbeat-threshold <heartbeat-threshold>`	Enter a heartbeat threshold in the **Heartbeat Threshold** field to define the number of heartbeats that must be missed before the APs are forced to fail over to the standby controller.	3-10 heartbeats	5 heartbeats
`no`	Negates or removes any configured parameter.	—	—
`over-subscription`	The standby controller over-subscription feature allows a standby controller to support connections to standby APs beyond the controller's original rated AP capacity. A controller acting as a standby controller can oversubscribe to standby APs by up to four times that controller's rated AP capacity, as long as the tunnels consumed the standby APs do not exceed the maximum tunnel capacity for that standby controller.	—	—
`pre-shared-key <pre-shared-key>`	Define a PSK to be used with the state synchronization feature.	8-32 characters	—

Parameter	Description	Range	Default
`preemption`	If you include this optional parameter to enable preemption, an AP that has failed over to a standby controller attempts to connect back to its original active controller once that controller is reachable again. When you enable this setting, the AP will wait for the time specified by the **lms-hold-down-period** parameter in the ap system-profile profile before the standby AP attempts to switch back to original controller.	—	—
`state-sync`	State synchronization improves failover performance by synchronizing PMK and Key cache values from the active controller to the standby controller, allowing clients to authenticate on the standby controller without repeating the complete 802.1X authentication process. **NOTE:** To use the state synchronization feature, configure a PSK with the pre-shared-key parameter.	—	—

Usage Guidelines

The High Availability:Fast Failover feature supports redundancy models with an active controller pair, or an active or standby deployment model with one backup controller supporting one or more active controllers. Each of these clusters of active and backup controllers comprises a high-availability group. Note that all active and backup controllers within a single high-availability group must be deployed in a single master-local topology. The High Availability:Fast Failover features works across Layer-3 networks, so there is no need for a direct Layer-2 connection between controllers in a high-availability group.

By default, the active controller of an AP is the controller to which the AP first connects when it comes up. Other dual mode or standby mode controllers in the same High Availability group become potential standby controllers for that AP. This feature does not require that the active controller act as the configuration master for the local standby controller. A master controller in a master-local deployment can act as an active or a standby controller.

When the AP first connects to its active controller, that controller sends the AP the IP address of a standby controller, and the AP attempts to connect to the standby controller. If an AP that is part of a cluster with multiple backup controllers fails to connect to the first standby controller, the active controller will select a new standby controller for that AP, and the AP will attempt to connect to that standby controller. APs using control plane security establish an IPsec tunnel to their standby controller. APs that are not configured to use control plane security send clear, unencrypted information to the standby controller.

An AP will failover to its backup controller if it fails to contact its active controller through regular heartbeats and keepalive messages, or if the user manually triggers a failover using the WebUI or CLI.

A controller using this feature can have one of three high-availability roles: **active**, **standby**, or **dual**. An active controller serves APs, but cannot act as a failover standby controller for any AP except the ones that it serves as active. A standby controller acts as a failover backup controller, but cannot be configured as the primary controller for any AP. A dual controller can support both roles, and acts as the active controller for one set of APs, and also acts as a standby controller for another set of APs.

Examples

The following commands configure a high availability group:

```
(host) [mynode] (config) #ha group-profile new
(host) [mynode] (HA group information "new") #controller 192.0.2.2 role active
(host) [mynode] (HA group information "new") #controller 192.0.2.3 role active
(host) [mynode] (HA group information "new") #controller 192.0.2.4 role standby
(host) [mynode] (HA group information "new") #preemption
```

Related Commands

Command	Description
show ha group	Displays HA profile settings.
show ha ap	Displays profile settings for APs using HA.
show ha heartbeat counters	Displays heartbeat statistics information for HA.
show ha oversubscription statistics	Displays oversubscription statistics information for HA.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

halt

```
halt
```

Description

This command halts all processes on the Mobility Master.

Syntax

No parameters.

Usage Guidelines

This command gracefully stops all processes on the Mobility Master. You should issue this command before rebooting or shutting down to avoid interrupting processes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

help

```
help
```

Description

This command displays help for the CLI.

Syntax

No parameters.

Usage Guidelines

This command displays keyboard editing commands that allow you to make corrections or changes to the command without retyping.

You can also enter the question mark (?) to get various types of command help:

- When typed at the beginning of a line, the question mark lists all commands available in the current mode.
- When typed at the end of a command or abbreviation, the question mark lists possible commands that match.
- When typed in place of a parameter, the question mark lists available options.

Example

The following command displays help:

```
(host) [mynode] #help
HELP:
Special keys:
DEL, BS .... delete previous character
Ctrl-A  .... go to beginning of line
Ctrl-E  .... go to end of line
Ctrl-F  .... go forward one character
Ctrl-B  .... go backward one character
Ctrl-D  .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K  .... delete to end of line
Ctrl-W  .... delete previous word
Ctrl-T  .... transpose previous character
Ctrl-P  .... go to previous line in history buffer
Ctrl-N  .... go to next line in history buffer
Ctrl-Z  .... return to root command prompt
Tab, <SPACE> command-line completion
Exit    .... go to next lower command prompt
?, Tab  .... list choices
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
command argument (e.g. 'show ?') and describes each possible
argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what arguments match the input
(e.g. 'show w?'.)
If on entering a 'tab', command-line completion is not possible
at that point, the behavior will be similar to entering a '?'.
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

hostname

```
hostname <hostname>
```

Description

This command changes the hostname of the Mobility Master, standby controller, or managed device.

Syntax

Parameter	Description	Range
`<hostname>`	The hostname of the Mobility Master, standby controller, or managed device.	1-63 characters

Usage Guidelines

The hostname is used as the default prompt. You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

Example

The following example configures the Mobility Master hostname to “Controller 1”.

```
(host) [mm] (config) #hostname “Controller 1”
```

Related Commands

Command	Description
show hostname	Displays the controller's hostname.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on the Mobility Master, standby controller, or managed device.

iap del branch-key

```
iap del branch-key <brkey>
```

Description

This command removes a branch from the managed device based on the branch key.

Syntax

Parameter	Description
`branch-key <brkey>`	Key for the branch, which is unique to each branch.

Example

```
(host) [mynode] #iap del branch-key b3c65c4d013836cf190566ca1afdf87c95350cffb1c782e463
```

Related Commands

Command	Description
show iap table	This command displays the branch details connected to the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

iap trusted-branch-db

```
iap trusted-branch-db
   add {mac-address <mac-address>}
   allow-all
   del {mac-address <mac-address>}
   del-all
```

Description

This command is used to configure an Instant AP (IAP)-VPN branch as trusted.

Syntax

Parameter	Description
`add`	Configure an IAP trusted branch entry.
mac-address <mac-address>	MAC-address of the IAP.
`allow-all`	Configure all branches as trusted.
`del`	Delete an IAP trusted branch entry.
mac-address <mac-address>	MAC-address of the IAP.
`del-all`	Delete all trusted branch entries.

Example

The following command configures a specific IAP-VPN branch as trusted:

```
(host) [mynode] #iap trusted-branch-db add mac-address 01:01:0e:3e:4c:33
```

The following is the output of the above command:

```
Trusted branch added
```

This following command configures all IAP-VPN branches as trusted:

```
(host) [mynode] #iap trusted-branch-db allow-all
All IAP+VPN branches are trusted
```

Related Commands

Command	Description
show iap detailed-table	This command displays the IAP trusted branch table

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters	Config or Enable mode on Mobility Master.

ids ap-classification-rule

```
ids ap-classification-rule <rule-name>
   check-min-discovered-aps
   classify-to-type [neighbor|suspected-rogue]
   clone <source>
   conf-level-incr <conf-level-incr>
   discovered-ap-cnt <discovered-ap-cnt>
   match-ssids
   no
   snr-max <snr-max>
   snr-min <snr-min>
   ssid <ssid>
```

Description

This command configures the IDS AP classification rule profile.

Syntax

Parameter	Description	Range	Default
`<rule-name>`	Name of the AP classification rule profile.	—	—
`check-min-discovered-aps`	Enables a rule check for the minimum number of APs.	—	true
`classify-to-type`	Specifies the AP classification type as **neighbor** or **suspected-rogue** if the rule is matched.	—	suspected-rogue
`clone <source>`	Copies data from another AP classification rule profile.	—	—
`conf-level-incr`	Increases the confidence level (in percentage) when the rule matches.	0-100	5
`discovered-ap-cnt <discovered-ap-cnt>`	The number of APs to be discovered.	0-100	0
`match-ssids`	Matches SSIDs.	true false	false
`no`	Negates any configured parameter.	—	—
`snr-max <snr-max>`	Configures the maximum SNR value.	0-100	0
`snr-min <snr-min>`	Configures the minimum SNR value.	0-100	0
`ssid <ssid>`	Enter the keyword **ssid** followed by the SSID string to be matched or excluded	—	—

Usage Guidelines

AP classification rule configuration is performed only on the Mobility Master. If AMP is enabled via the mobility-manager command, then processing of the AP classification rules is disabled on Mobility Master. A rule is identified by its ASCII character string name (32 characters maximum). The AP classification rules must have one of the following specifications:

- SSID of the AP

- SNR of the AP
- Discovered-AP-Count or the number of APs that can see the AP

After you have created an AP classification rule, you must enable the rule by adding it to the IDS AP Matching Rules profile:

```
ids ap-rule-matching
   rule-name <name>
```

SSID specification

Each rule can have up to six SSID parameters. If one or more SSIDs are specified in a rule, an option of whether to match any of the SSIDs, or to not match all of the SSIDs can be specified. The default is to check for a match operation.

SNR specification

Each rule can have only one specification of the SNR. A minimum and maximum can be specified in each rule, and the specification is in SNR (db).

Discovered-AP-Count specification

Each rule can have only one specification of the discovered-AP-count. Each rule can specify a minimum or maximum of the discovered-AP-count. The minimum or maximum operation must be specified if the discovered-AP-count is specified. The default setting is to check for the minimum discovered-AP-count.

Example

The following example configures the AP Configuration Rule Profile named “rule1”, and then enables the rule by adding it to the IDS AP Matching Rules profile:

```
(host) [mynode] (config) #ids ap-classification-rule rule1
(host) [mynode] (IDS AP Classification Rule Profile "rule1") #check-min-discovered-aps
(host) [mynode] (IDS AP Classification Rule Profile "rule1") #classify-to-type neighbor
```

Related Commands

Command	Description
show ids ap-classification-rule	Displays the IDS AP classification rule profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids ap-rule-matching

```
ids ap-rule-matching
   no
   rule-name <rule-name>
```

Description

This command configures the IDS active AP rules profile by enabling an AP classification rule.

Syntax

Parameter	Description
`no`	Negates any configured parameter.
`rule-name <rule-name>`	Name of the IDS AP classification rule to activate.

Usage Guidelines

This command activates an active AP rule created by the **ids ap-classification-rule** command. You must create the rule before you can activate it.

Example

```
(host) [mynode] (IDS Active AP Rules Profile) #rule-name rule2
```

Related Commands

Command	Description
ids ap-classification-rule	Configures an IDS AP classification rule.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master.

ids dos-profile

```
ids dos-profile <profile-name>
   ap-flood-inc-time <ap-flood-inc-time>
   ap-flood-quiet-time <ap-flood-quiet-time>
   ap-flood-threshold <ap-flood-threshold>
   assoc-rate-thresholds <assoc-rate-thresholds>
   auth-rate-thresholds <auth-rate-thresholds>
   block-ack-dos-quiet-time <block-ack-dos-quiet-time>
   chopchop-quiet-time <chopchop-quiet-time>
   client-ht-40mhz-intol-quiet-time <client-ht-40mhz-intol-quiet=time>
   client-flood-inc-time <client-flood-inc-time>
   client-flood-quiet-time <client-flood-quiet-time>
   client-flood-threshold <client-flood-threshold>
   clone <source>
   cts-rate-quiet-time <cts-rate-quiet-time>
   cts-rate-threshold <cts-rate-threshold>
   cts-rate-time-interval <cts-rate-time-interval>
   deauth-rate-thresholds <deauth-rate-thresholds>
   detect-ap-flood
   detect-block-ack-dos
   detect-chopchop-attack
   detect-client-flood
   detect-cts-rate-anomaly
   detect-disconnect-sta
   detect-eap-rate-anomaly
   detect-fata-jack-attack
   detect-ht-40mhz-intolerance
   detect-invalid-address
   detect-malformed-association-request
   detect-malformed-auth-frame
   detect-malformed-htie
   detect-malformed-large-duration
   detect-omerta-attack
   detect-overflow-eapol-key
   detect-overflow-ie
   detect-power-save-dos-attack
   detect-rate-anomalies
   detect-rts-rate-anomaly
   detect-tkip-replay-attack
   detect-wpa-ft-attack
   disassoc-rate-thresholds <disassoc-rate-thresholds>
   disconnect-deauth-disassoc-threshold <disconnect-deauth-disassoc-threshold>
   disconnect-sta-assoc-resp-threshold <disconnect-sta-assoc-resp-threshold>
   disconnect-sta-quiet-time <disconnect-sta-quiet-time>
   eap-rate-quiet-time <eap-rate-quiet-time>
   eap-rate-threshold <eap-rate-threshold>
   eap-rate-time-interval <eap-rate-time-interval>
   fata-jack-quiet-time <fata-jack-quiet-time>
   invalid-address-combination-quiet-time <invalid-address-combination-quiet-time>
   malformed-association-request-quiet-time <malformed-association-request-quiet-time>
   malformed-auth-frame-quiet-time <malformed-auth-frame-quiet-time>
   malformed-htie-quiet-time <malformed-htie-quiet-time>
   malformed-large-duration-quiet-time <malformed-large-duration-quiet-time>
   no
   omerta-quiet-time <omerta-quiet-time>
   omerta-threshold <omerta-threshold>
   overflow-eapol-key-quiet-time <overflow-eapol-key-quiet-time>
   overflow-ie-quiet-time <overflow-ie-quiet-time>
   power-save-dos-min-frames <power-save-dos-min-frames>
```

```
power-save-dos-quiet-time <power-save-dos-quiet-time>
power-save-dos-threshold <power-save-dos-threshold>
probe-request-rate-thresholds <probe-request-rate-thresholds>
probe-response-rate-thresholds <probe-response-rate-thresholds>
rts-rate-quiet-time <rts-rate-quiet-time>
rts-rate-threshold <rts-rate-threshold>
rts-rate-time-interval <rts-rate-time-interval>
spoofed-deauth-blacklist
tkip-replay-quiet-time  <tkip-replay-quiet-time>
wpa-ft-quiet-time
wpa-ft-threshold
wpa-ft-time-interval
```

Description

This command configures traffic anomalies for DoS attacks.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the IDS DoS profile.	1-63 characters	“default”
`ap-flood-inc-time <ap-flood-inc-time>`	Time, in seconds, during which the AP count is over the threshold (AP flood).	0-36000 seconds	3600 seconds
`ap-flood-quiet-time <ap-flood-quiet-time>`	After an alarm has been triggered by an AP flood, the time, in seconds, that must elapse before an identical alarm may be triggered.	60-360000 seconds	900 seconds
`ap-flood-threshold <ap-flood-threshold>`	Threshold for the number of spurious APs in the system.	0-100,000	50
`assoc-rate-thresholds <assoc-rate-thresholds>`	Rate threshold for associate request frames.	—	—
`auth-rate-thresholds <auth-rate-thresholds>`	Rate threshold for authenticate frames.	—	—
`block-ack-dos-quiet-time <block-ack-dos-quiet-time>`	Time to wait, in seconds, after detecting an attempt to reset the receive window using a forged block ACK add.	60-360000 seconds	900 seconds
`chopchop-quiet-time <chopchop-quiet-time>`	Time to wait, in seconds, after detecting a ChopChop attack after which the check can be resumed.	60-360000 seconds	900 seconds

Parameter	Description	Range	Default
`client-ht-40mhz-intol-quiet-time <client-ht-40mhz-intol-quiet=time>`	Quiet time (when to stop reporting intolerant STAs if they have not been detected), in seconds, for detection of 802.11n 40 MHz intolerance setting.	60-360000 seconds	900 seconds
`client-flood-inc-time <client-flood-inc-time>`	Number of consecutive seconds over which the client count is more than the threshold.	0-36000 seconds	3 seconds
`client-flood-quiet-time <client-flood-quiet-time>`	Time to wait, in seconds, after detecting a client flood before continuing the check.	60-360000 seconds	900 seconds
`client-flood-threshold <client-flood-threshold>`	Threshold for the number of spurious clients in the system.	0-100000	150
`clone <source>`	Copies data from another IDS Denial Of Service Profile.	—	—
`cts-rate-quiet-time <cts-rate-quiet-time>`	Time to wait, in seconds, after detecting a CTS rate anomaly after which the check can be resumed.	60-360000 seconds	900 seconds
`cts-rate-threshold <cts-rate-threshold>`	Number of CTS control packets over the time interval that constitutes an anomaly.	0-100000	5000
`cts-rate-time-interval <cts-rate-time-interval>`	Time interval, in seconds, over which the packet count should be checked.	1-120 seconds	5 seconds
`deauth-rate-thresholds <deauth-rate-thresholds>`	Rate threshold for deauthenticate frames.	—	—
`detect-ap-flood`	Enables or disables detection of AP flood attacks.	—	disabled
`detect-block-ack-dos`	Enables or disables detection of attempts to reset traffic receive windows using forged Block ACK Add messages.	—	enabled
`detect-chopchop-attack`	Enables or disables detection of ChopChop attacks.	—	disabled
`detect-client-flood`	Enables or disables detection of client flood attacks.	—	disabled

Parameter	Description	Range	Default
`detect-cts-rate-anomaly`	Enables or disables detection of CTS rate anomalies.	—	disabled
`detect-disconnect-sta`	In a station disconnection attack, an attacker spoofs the MAC address of either an active client or an active AP. The attacker then sends deauthenticate frames to the target device, causing it to lose its active association. Use this command to enable the detection of disconnect station attack.	—	enabled
`detect-eap-rate-anomaly`	Enables or disables detection of the EAP handshake rate anomaly.	—	disabled
`detect-fata-jack-attack`	Enables or disables detection of FATA-Jack attacks.	—	enabled
`detect-ht-40mhz-intolerance`	Enables or disables detection of 802.11n 40 MHz intolerance setting, which controls whether stations and APs advertising 40 MHz intolerance will be reported.	—	disabled
`detect-invalid-address`	Enables or disables detection of invalid address combinations	—	disabled
`detect-malformed-association-request`	Enables or disables detection of malformed association requests.	—	disabled
`detect-malformed-auth-frame`	Enables or disables detection of malformed authentication frames.	—	disabled
`detect-malformed-htie`	Enables or disables detection of malformed HT IE.	—	disabled
`detect-malformed-large-duration`	Enables or disables detection of unusually large durations in frames.	—	enabled
`detect-omerta-attack`	Enables or disables detection of Omerta attacks.	—	enabled

Parameter	Description	Range	Default
detect-overflow-eapol-key	Enables or disables detection of overflow EAPOL key requests.	—	disabled
detect-overflow-ie	Enables or disables detection of overflow IEs.	—	disabled
detect-power-save-dos-attack	Enables or disables detection of Power Save DoS attacks.	—	enabled
detect-rate-anomalies	Enables or disables detection of rate anomalies.	—	disabled
detect-rts-rate-anomaly	Enables or disables detection of RTS rate anomalies.	—	disabled
detect-tkip-replay-attack	Enables or disables detection of TKIP replay attacks.	—	disabled
detect-wpa-ft-attack	Enables or disables detection of WPA FT attacks.	—	disabled
disassoc-rate-thresholds <disassoc-rate-thresholds>	Rate threshold for disassociate frames.	—	—
disconnect-deauth-disassoc-threshold <disconnect-deauth-disassoc-threshold>	Number of deauthentication or disassociation frames seen in an interval of 10 seconds.	1-50	8
disconnect-sta-assoc-resp-threshold <disconnect-sta-assoc-resp-threshold>	The number of successful Association Response or Reassociation response frames seen in an interval of 10 seconds.	1-30	5
disconnect-sta-quiet-time <disconnect-sta-quiet-time>	After a station disconnection attack is detected, the time, in seconds, that must elapse before the check can be resumed.	60-360000 seconds	900 seconds
eap-rate-quiet-time <eap-rate-quiet-time>	After an EAP rate anomaly alarm has been triggered, the time, in seconds, that must elapse before the check can be resumed.	60-360000 seconds	900 seconds
eap-rate-threshold <eap-rate-threshold>	Number of EAP handshakes that must be received within the EAP rate time interval to trigger an alarm.	0-100000	60

Parameter	Description	Range	Default
`eap-rate-time-interval <eap-rate-time-interval>`	Time, in seconds, during which the configured number of EAP handshakes must be received to trigger an alarm.	1-120 seconds	3 seconds
`fata-jack-quiet-time <fata-jack-quiet-time>`	Time to wait, in seconds, after detecting a FATA-Jack attack after which the check can be resumed.	60-360000 seconds	900 seconds
`invalid-address-combination-quiet-time <invalid-address-combination-quiet-time>`	Time to wait, in seconds, after detecting an invalid address combination after which the check can be resumed.	60-360000 seconds	900 seconds
`malformed-association-request-quiet-time <malformed-association-request-quiet-time>`	Time to wait, in seconds, after detecting a malformed association request after which the check can be resumed.	60-360000 seconds	900 seconds
`malformed-auth-frame-quiet-time <malformed-auth-frame-quiet-time>`	Time to wait, in seconds, after detecting a malformed authentication frame after which the check can be resumed.	60-360000 seconds	900 seconds
`malformed-htie-quiet-time <malformed-htie-quiet-time>`	Time to wait, in seconds, after detecting a malformed HT IE after which the check can be resumed.	60-360000 seconds	900 seconds
`malformed-large-duration-quiet-time <malformed-large-duration-quiet-time>`	Time to wait, in seconds, after detecting a large duration for a frame after which the check can be resumed.	60-360000 seconds	900 seconds
`no`	Negates any configured parameter.	—	—
`omerta-quiet-time <omerta-quiet-time>`	Time to wait, in seconds, after detecting an Omerta attack after which the check can be resumed.	60-360000 seconds	900 seconds
`omerta-threshold <omerta-threshold>`	The Disassociation packets received by a station as a percentage of the number of data packets sent, in an interval of 10 seconds.	1-100	10%

Parameter	Description	Range	Default
`overflow-eapol-key-quiet-time <overflow-eapol-key-quiet-time>`	Time to wait, in seconds, after detecting a overflow EAPOL key request after which the check can be resumed.	60-360000 seconds	900 seconds
`overflow-ie-quiet-time <overflow-ie-quiet-time>`	Time to wait, in seconds, after detecting a overflow IE after which the check can be resumed.	60-360000 seconds	900 seconds
`power-save-dos-min-frames <power-save-dos-min-frames>`	The minimum number of Power Management OFF packets that are required to be seen from a station, in intervals of 10 second, in order for the Power Save DoS check to be done.	1-1000	120
`power-save-dos-quiet-time <power-save-dos-quiet-time>`	Time to wait, in seconds, after detecting a Power Save DoS attack after which the check can be resumed.	60-360000 seconds	900 seconds
`power-save-dos-threshold <power-save-dos-threshold>`	The Power Management ON packets sent by a station as a percentage of the Power Management OFF packets sent, in intervals of 10 second, which will trigger this event.	1- 100%	80%
`probe-request-rate-thresholds <probe-request-rate-thresholds>`	Rate threshold for probe request frames.	—	—
`probe-response-rate-thresholds <probe-response-rate-thresholds>`	Rate threshold for probe response frames.	—	—
`rts-rate-quiet-time <rts-rate-quiet-time>`	Time to wait, in seconds, after detecting an RTS rate anomaly after which the check can be resumed.	60-360000 seconds	900 seconds
`rts-rate-threshold <rts-rate-threshold>`	Number of RTS control packets over the time interval that constitutes an anomaly.	0-100000	5000
`rts-rate-time-interval <rts-rate-time-interval>`	Time interval, in seconds, over which the packet count should be checked.	1-120 seconds	5 seconds

Parameter	Description	Range	Default
`spoofed-deauth-blacklist`	Enable or disable detection of a deauth attack initiated against a client associated to an AP. When such an attack is detected, the client is quarantined from the network to prevent a man-in-the-middle attack from being successful.	—	disabled
`tkip-replay-quiet-time <tkip-replay-quiet-time>`	Time to wait, in seconds, after detecting a TKIP replay attack after which the check can be resumed.	60-360000 seconds	900 seconds
`wpa-ft-quiet-time <wpa-ft-quiet-time>`	Time to wait, in seconds, after detecting a WPA FT attack after which the check can be resumed. Minimum is 60.	60-360000 seconds	900 seconds
`wpa-ft-threshold <wpa-ft-threshold>`	Number of reassociation management packets for a particular client over the time interval that constitutes a WPA FT attack.	0-100000	45
`wpa-ft-time-interval <wpa-ft-time-interval>`	Time interval, in seconds, over which the packet count should be checked.	1-120 seconds	60 seconds

Usage Guidelines

DoS attacks are designed to prevent or inhibit legitimate clients from accessing the network. This includes blocking network access completely, degrading network service, and increasing processing load on clients and network equipment.

Example

The following command enables a detection in the DoS profile named “floor2”:

```
(host) [mynode] (config) #ids dos-profile floor2
(host) [mynode] (IDS Denial Of Service Profile "floor2") detect-ap-flood
```

Related Commands

Command	Description
show ids dos-profile	Displays the IDS DoS profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: ■ **detect-wpa-ft-attack** ■ **wpa-ft-quiet-time** ■ **wpa-ft-threshold** ■ **wpa-ft-time-interval**
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids general-profile

```
ids general-profile <profile-name>
   adhoc-ap-inactivity-timeout
   adhoc-ap-max-unseen-timeout
   ap-inactivity-timeout <seconds>
   ap-max-unseen-timeout
   ap-nbr-msg
   ap-nbr-msg-interval <ap-nbr-msg-interval>
   clone <profile>
   frame-types-for-rssi [all | ba | ctrl | dhigh | dlow | dnull | mgmt | pr]
   ids-events [logs-and-traps | logs-only | none | traps-only]
   max-monitored-devices <max-monitored-devices>
   max-unassociated-stations <max-unassociated-stations>
   min-pot-ap-beacon-rate <percent>
   min-pot-ap-monitor-time <seconds>
   mobility-manager-rtls
   mon-stats-update-interval
   no ...
   packet-snr-threshold <packet-snr-threshold>
   send-adhoc-info-to-controller
   signature-quiet-time <seconds>
   sta-inactivity-timeout <seconds>
   sta-max-unseen-timeout <seconds>
   sta-rssi-msg
   sta-rssi-msg-interval <sta-rssi-msg-interval>
   stats-update-interval <seconds>
   unclass-ap-update
   unclass-device-update-interval
   unclass-sta-update
   wired-containment
   wired-containment-ap-adj-mac
   wired-containment-susp-l3-rogue
   wireless-containment [deauth-only | none | tarpit-all-sta | tarpit-non-valid-sta]
   wired-containment-ap-adj-mac
   wireless-containment-debug
```

Description

This command configures an IDS general profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	default
`adhoc-ap-inactivity-timeout`	Ad hoc (IBSS) AP inactivity timeout, in number of scans.	5-36000 seconds	5 seconds
`adhoc-ap-max-unseen-timeout`	Ageout time, in seconds, since ad hoc (IBSS) AP was last seen.	5-36000 seconds	5 seconds
`ap-inactivity-timeout`	Time, in seconds, after which an AP is aged out.	5-36000 seconds	5 seconds

Parameter	Description	Range	Default
`ap-max-unseen-timeout`	Ageout time, in seconds, since AP was last seen.	5-36000 seconds	600 seconds
`ap-nbr-msg`	Enables or disables AP neighbor messages.	—	disabled
`ap-nbr-msg-interval`	Interval, in seconds, at which an AP delivers AP neighbor messages to the management server.	1-36000 seconds	1 second
`clone`	Name of an existing IDS general profile from which parameter values are copied.	—	—

`frame-types-for-rssi`
`all`
`ba`
`ctrl`
`dhigh`
`dlow`
`dnull`
`mgmt`
`pr`
	Select frame types to be used in AM RSSI calculation.
	Frame types:
	■ **all**—All types of frames. This frame type overrides any other frame types.
	■ **ba**—Block ACK frame types.
	■ **ctrl**—All control frames except ACK.
	■ **dhigh**—Data frames more than 36 Mbps except null data frames.
	■ **dlow**—Data frames less than 36 Mbps except null data frames.
	■ **dnull**—Null data frames.
	■ **mgmt**—All management frames except probe request.
	■ **pr**—Probe request frames.
	NOTE: Configure this parameter under the supervision of Aruba Technical Support.
		—	ba, ctrl, dlow, dnull, mgmt, pr

`ids-events`
`logs-and-traps`
`logs-only`
`none`
`traps-only]`
	Enables or disables IDS event generation from the AP. Event generation from the AP can be enabled for syslogs, traps, or both. This does not affect generation of IDS correlated events on the switch.	—	logs-and-traps

`max-monitored-devices`	Maximum number of APs and stations that can be monitored. This number does not include stations that are not associated to any AP. Within this max value, the AP reserves a buffer for stations that are associated locally. **NOTE:** This parameter is currently available on 220 Series access points only. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support.	1024-4096	1024
`max-unassociated-stations`	Maximum number of unassociated stations. **NOTE:** This parameter is currently available on 220 Series access points only. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support.	256-4096	512
`min-pot-ap-beacon-rate`	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.	0-100%	25%

Parameter	Description	Range	Default
min-pot-ap-monitor-time	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.	2-36000	2 seconds
mobility-manager-rtls	Enables or disables RTLS communication with the configured mobility-manager.	enabled disabled	disabled
mon-stats-update-interval	Time interval, in seconds, for the AP to update the switch with stats for monitored devices.	60-36000 seconds	60 seconds
no	Negates any configured parameter.	—	—
packet-snr-threshold	Sets the packet SNR threshold. All packets with SNR below this threshold is dropped from IDS and ARM processing. No packets are dropped if the threshold is set to 0. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support.	0-90 dB	0
send-adhoc-info-to-controller	Enables or disables sending ad hoc information to the controller from the AP.	—	disabled
signature-quiet-time	After a signature match is detected, the time to wait, in seconds, to resume checking.	60-36000 seconds	900 seconds
sta-inactivity-timeout	Time, in seconds, after which a station is aged out.	30-36000 seconds	60 seconds
sta-max-unseen-timeout	Ageout time, in seconds, since station was last seen. Minimum is 5.	5-36000 seconds	600 seconds
sta-rssi-msg	Enables or disables station RSSI messages.	enable disable	disabled
sta-rssi-msg-interval	Interval, in seconds, at which the AP delivers station RSSI messages to the management server.	1-36000	1 second
stats-update-interval	Interval, in seconds, for the AP to update the controller with statistics.	60-36000 seconds	60 seconds
unclass-ap-update	Enables or disables classification updates for monitored APs. If this option is enabled, there is a decrease in the delay with which the devices are classified.	enable disable	disabled
unclass-device-update-interval	The time interval, in seconds, for the AP to send the WMS a list of unclassified APs and clients.	30-36000 seconds	60 seconds

Parameter	Description	Range	Default
`unclass-sta-update`	Enables or disables classification updates for monitored clients. If this option is enabled, there is a decrease in the delay with which the devices are classified.	—	disabled
`wired-containment`	Enables or disables containment from the wired side.	—	disabled
`wired-containment-ap-adj-mac`	Enables or disables wired containment of MACs offset by one from APs BSSID.	—	disabled
`wired-containment-susp-l3-rogue`	The basic wired containment feature enabled using the command contains layer-3 APs whose wired interface MAC addresses are either the same as (or one character off from) their BSSIDs. This feature can also identify and contain an AP with a preset wired MAC address that is completely different from the AP's BSSID if the MAC address that the AP provides to wireless clients as the 'gateway MAC' is offset by one character from its wired MAC address. **NOTE:** This feature requires that the following parameter in the ids general-profile is also enabled, and that the confidence level of the suspected rogue exceeds the level configured by the and parameters in the ids unauthorized-device-profile.	—	disabled
`wireless-containment`	Selects one of the following containment types from the wireless side: ■ **deauth-only**: Containment using deauthentication only. ■ **none**: Disables wireless containment. ■ **tarpit-all-sta**: Wireless containment by tarpit of all stations. ■ **tarpit-non-valid-sta**: Wireless containment by tarpit of non-valid clients.	—	`deauth-only`
`wireless-containment-debug`	Enables or disables debugging of containment from the wireless side. **NOTE:** Enabling this debug option will cause containment to not function properly.	—	disabled

Usage Guidelines

This command configures general IDS profile attributes.

Warning Message for Containment Features

The feature for enabling wireless containment under the **IDS Unauthorized Device** profile and **IDS Impersonation** profile may be in violation of certain FCC regulatory statutes. To address this, a warning message will be issued each time the command is enabled through the CLI. The warning message will appear after the command is executed.

Example

The following command enables containment in the general IDS profile:

```
(host) [mynode] (config) #ids general-profile floor7
(host) [mynode] (IDS General Profile "floor7") #wired-containment
(host) [mynode] (IDS General Profile "floor7") #wireless-containment tarpit-all-sta
(host) [mynode] (IDS General Profile "floor7") #wireless-containment-debug
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids impersonation-profile

```
ids impersonation-profile <profile-name>
   ap-spoofing-quiet-time <ap-spoofing-quiet-time>
   beacon-diff-threshold <beacon-diff-threshold>
   beacon-inc-wait-time <beacon-inc-wait-time >
   beacon-wrong-channel-quiet-time <beacon-wrong-channel-quiet-time>
   chan-based-mitm-quiet-time <chan-based-mitm-quiet-time>
   clone <source>
   detect-ap-impersonation
   detect-ap-spoofing
   detect-beacon-wrong-channel
   detect-chan-based-mitm
   detect-hotspotter
   hotspotter-quiet-time <hotspotter-quiet-time>
   no
   protect-ap-impersonation
```

Description

This command configures anomalies for impersonation attacks.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	1-63 characters	"default"
`ap-spoofing-quiet-time <ap-spoofing-quiet-time>`	Time to wait, in seconds, after detecting AP Spoofing after which the check can be resumed.	60-360000 seconds	60 seconds
`beacon-diff-threshold <beacon-diff-threshold>`	Percentage increase, in beacon rates, that triggers an AP impersonation event.	0-100%	50%
`beacon-inc-wait-time <beacon-inc-wait-time >`	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated.	—	3 seconds
`beacon-wrong-channel-quiet-time <beacon-wrong-channel-quiet-time>`	Time to wait, in seconds, after detecting a beacon with the wrong channel after which the check can be resumed.	60-360000 seconds	900 seconds
`chan-based-mitm-quiet-time <chan-based-mitm-quiet-time>`	Time to wait, in seconds, after detecting man-in-the-middle attack after which the check can be resumed.	60-360000 seconds	900 seconds
`clone <source>`	Name of an existing IDS impersonation profile from which parameter values are copied.	—	—

Parameter	Description	Range	Default
`detect-ap-impersonation`	Enables or disables detection of AP impersonation. In AP impersonation attacks, the attacker sets up an AP that assumes the BSSID and ESSID of a valid AP. AP impersonation attacks can be done for man-in-the-middle attacks, a rogue AP attempting to bypass detection, or a honeypot attack.	—	enabled
`detect-ap-spoofing`	Enables or disables AP Spoofing detection	—	enabled
`detect-beacon-wrong-channel`	Enables or disables detection of beacons advertising the incorrect channel	—	disabled
`detect-chan-based-mitm`	Enables or disables channe-based man-in-the-middle attack detection.	—	disabled
`detect-hotspotter`	Enables or disables detection of the Hotspotter attack to lure away valid clients.	—	disabled
`hotspotter-quiet-time <hotspotter-quiet-time>`	Time to wait, in seconds, after detecting an attempt to use the Hotspotter tool against clients.	60-360000 seconds	900 seconds
`no`	Negates any configured parameter.	—	—
`protect-ap-impersonation`	When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a denial of service attack.	—	disabled

Usage Guidelines

A successful man-in-the-middle attack will insert an attacker into the data path between the client and the AP. In such a position, the attacker can delete, add, or modify data, provided he has access to the encryption keys. Such an attack also enables other attacks that can learn a client's authentication credentials. Man-in-the-middle attacks often rely on a number of different vulnerabilities.

Example

The following command enables detections in the impersonation profile:

```
(host) [mynode] (config) #ids impersonation-profile floor1
(host) [mynode] (IDS Impersonation Profile "floor1") #detect-beacon-wrong-channel
(host) [mynode] (IDS Impersonation Profile "floor1") #detect-ap-impersonation
```

Related Commands

Command	Description
show ids impersonation-profile	Displays the IDS impersonation profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: ■ **chan-based-mitm-quiet-time** ■ **detect-chan-based-mitm**
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids management-profile

```
ids management-profile
   event-correlation [logs-and-traps|logs-only|none|traps-only]
   event-correlation-quiet-time <event-correlation-quiet-time>
```

Description

This command configures the IDS WMS management profile.

Syntax

Parameter	Description	Range	Default
`event-correlation`	Correlation mode for IDS event traps and syslogs (logs). Event correlation can be enabled with generation of correlated logs, traps, or both. To disable correlation, enter the keyword **none**. ■ **logs-and-traps**: Enables IDS event correlation with generation of correlated syslogs and traps. ■ **logs-only**: Enables IDS event correlation with generation of correlated syslogs only. ■ **none**: Disables IDS event correlation. ■ **traps-only**: Enables IDS event correlation with generation of correlated traps only.	—	logs-and-traps
`event-correlation-quiet-time`	Time to wait, in seconds, after generating a correlated event after which the event could be raised again. This only applies to events that are repeatedly raised by an AP.	30-360000 seconds	900 seconds

Usage Guidelines

Manage the events correlation for IDS event traps and syslogs (logs).

Example

```
(host) [mynode] (config) #ids management-profile
(host) [mynode] (IDS Management Profile) #event-correlation-quiet-time 30
(host) [mynode] (IDS Management Profile) #event-correlation logs-and-traps
```

Related Commands

Command	Description
show ids management-profile	Displays the IDS WMS management profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master.

ids profile

```
ids profile <profile-name>
   clone <source>
   dos-profile <profile-name>
   general-profile <profile-name>
   impersonation-profile <profile-name>
   no
   signature-matching-profile <profile-name>
   unauthorized-device-profile <profile-name>
```

Description

This command defines a set of IDS profiles.

Syntax

Parameter	Description	Default
`<profile-name>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	"default"
`clone <source>`	Name of an existing IDS profile from which parameter values are copied.	—
`dos-profile <profile-name>`	Name of a IDS DoS profile to be applied to the AP group or name. See ids dos-profile on page 488.	"default"
`general-profile <profile-name>`	Name of an IDS general profile to be applied to the AP group or name. See ids general-profile on page 497.	"default"
`impersonation-profile <profile-name>`	Name of an IDS impersonation profile to be applied to the AP group or name. See ids impersonation-profile on page 502.	"default"
`no`	Negates any configured parameter.	—
`signature-matching-profile <profile-name>`	Name of an IDS signature matching profile to be applied to the AP group or name. See ids signature-matching-profile on page 515	"default"
`unauthorized-device-profile <profile-name>`	Name of an IDS unauthorized device profile to be applied to the AP group or name. See ids unauthorized-device-profile on page 520.	"default"

Usage Guidelines

This command defines a set of IDS profiles that you can then apply to an AP group (with the **ap-group** command) or to a specific AP (with the **ap-name** command).

Example

The following command defines a set of IDS profiles:

```
(host) [mynode] (config) #ids profile floor2
(host) [mynode] (IDS Profile "floor2") #dos-profile dos1
   general-profile general1
   impersonation-profile mitm1
```

```
signature-matching-profile sig1
unauthorized-device-profile unauth1
```

Related Commands

Command	Description
ids dos-profile	Configures an IDS DoS profile.
ids general-profile	Configures an IDS general profile.
ids impersonation-profile	Configures an IDS impersonation profile.
ids signature-matching-profile	Configures an IDS signature matching profile.
ids unauthorized-device-profile	Configures an IDS unauthorized device profile.
show ids profile	Displays all IDS profiles or a specific IDS profile.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids rap-wml-server-profile

```
ids rap-wml-server-profile <server-name>
   ageout <ageout>
   cache{disable|enable}
   clone <source>
   db-name <db-name>
   ip-addr <ip-addr>
   password <password>
   type {mssql|mysql}
   user <user>
```

Description

Use this command to configure an IDS remote AP WML (MSSQL or MySQL) server profile.

Syntax

Parameter	Description	Range	Default
`<server-name>`	Name of the remote AP WML server.	—	—
`ageout <ageout>`	Specifies the cache ageout period, in seconds.	—	0
`cache`	Enables or disables the cache.	—	disabled
`clone <source>`	Copies configuration settings from an existing profile.	—	—
`db-name <db-name>`	Specifies the name of the database.	—	—
`ip-addr <ip-addr>`	Specifies the IP address of the named WML server.	—	0.0.0.0
`no`	Negates any configured parameter.	—	—
`password <password>`	Specifies the password required for database login.	—	—
`type`	Specifies the server type: ■ MSSQL server ■ MySQL server	—	—
`user <user>`	Specifies the user name required for database login.	—	—

Usage Guidelines

Use the **show rap-wml cache** command to show the cache of all lookups for a database server. Use the **show rap-wml servers** command to show the database server state. Use the **show rap-wml wired-mac** command to show wired MAC discovered on traffic through the AP.

Example

This example configures an MSSQL server and sets up associated rap-wml table attributes for that server:

```
(host) [mynode] (config) # ids rap-wml-server-profile mssqlserver type mssql ip-addr
10.4.11.11 db-name automatedtestdatabase user sa password sa
```

```
ids rap-wml-table-profile mssqlserver table-name mactest_undelimited timestamp-
column time lookup-time 600
ids rap-wml-table-profile mssqlserver table-name mactest_delimited mac-delimiter : timestamp-
column time lookup-time 600
```

Related Commands

Command	Description
show rap-wml	Displays configuration information for the MSSQL or MySQL server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids rap-wml-table-profile

```
ids rap-wml-table-profile <table-name>
   clone <source>
   column-name <column-name>
   lookup-time <lookup-time>
   mac-delimiter <mac-delimiter>
   no
   table-name <table-name>
   timestamp-column <timestamp-column-name>
```

Description

This command configures an IDS remote AP WML table profile.

Syntax

Parameter	Description	Range	Default
`<table-name>`	Name of an IDS remote AP WML table profile.	—	—
`clone <source>`	Copies data from another IDS remote AP WML table profile.	—	—
`column-name <column-name>`	Specifies the database column name containing the MAC address.	—	—
`lookup-time <lookup-time>`	Specifies how far back, in seconds, to look for the MAC address. Use 0 seconds to look up everything.	—	0
`mac-delimiter <mac-delimter>`	Specifies the optional delimiter character for the MAC address in the database.	—	No delimiter
`no`	Negates the rap-wml table for the named server.	—	—
`table-name <table-name>`	Specifies the database table name.	—	—
`timestamp-column <timestamp-column-name>`	Specifies the database column name with the timestamp last seen.	—	—

Usage Guidelines

Use the **ids rap-wml-server-profile <servername>** command to configure a MySQL or an MSSQL server, then use the **ids rap-wml-table-profile** command to configure the associated database table for the server.

Example

This example configures a MySQL server and sets up associated rap-wml table attributes for that server:

```
(host) [mynode] (config) #ids rap-wml-server-profile mysqlserver type mysql ip-addr 10.4.11.10
db-name automatedtestdatabase user sa password sa
ids rap-wml-table-profile mysqlserver table-name mactest_undelimited timestamp-
column time lookup-time 600
ids rap-wml-table-profile table-name mysqlserver mactest_delimited mac-delimiter : timestamp-
column time lookup-time 600
```

This example configures an MSSQL server and sets up associated rap-wml table attributes for that server:

```
(host) [mynode] (config) # ids rap-wml-server-profile mssqlserver type mssql ip-addr
10.4.11.11 db-name automatedtestdatabase user sa password sa
ids rap-wml-table-profile mssqlserver table-name mactest_undelimited timestamp-
column time lookup-time 600
ids rap-wml-table-profile mssqlserver table-name mactest_delimited mac-delimiter : timestamp-
column time lookup-time 600
```

Related Commands

Command	Description
ids rap-wml-server-profile	Configures an IDS remote AP WML (MSSQL or MySQL) server profile.
show rap-wml	Displays configuration information for the MSSQL or MySQL server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the RF Protect license	Config mode on Mobility Master

ids rate-thresholds-profile

```
ids rate-thresholds-profile <profile-name>
   channel-inc-time <channel-inc-time>
   channel-quiet-time <channel-quiet-time>
   channel-threshold <channel-threshold>
   clone <profile>
   no ...
   node-quiet-time <node-quiet-time>
   node-threshold <node-threshold>
   node-time-interval <node-time-interval>
```

Description

This command configures an IDS rate thresholds profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	default
`channel-inc-time <channel-inc-time>`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.	0 - 360000 seconds	15 seconds
`channel-quiet-time <channel-quiet-time>`	After a channel rate anomaly alarm has been triggered, the time that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file.	60-360000 seconds	900 seconds
`channel-threshold`	Number of specific frame types that must be exceeded within a specific interval in a channel to trigger an alarm.	0-100000 frames	300
`clone <source>`	Copies an existing IDS rate thresholds profile.	—	—
`no`	Negates any configured parameter.	—	—
`node-quiet-time <node-quiet-time>`	After a node rate anomaly alarm has been triggered, the time, in seconds, that must elapse before another identical alarm may be triggered. This option prevents excessive messages in the log file.	60-360000 seconds	900 seconds
`node-threshold <node-threshold>`	Number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.	0 -100000 frames	200
`node-time-interval <node-time-interval>`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.	1-120 seconds	15 seconds

Usage Guidelines

A profile of this type is attached to each of the following 802.11 frame types in the IDS denial of service profile:

- Association frames
- Disassociation frames
- Deauthentication frames

- Probe Request frames
- Probe Response frames
- Authentication frames

Example

The following command configures frame thresholds:

```
(host) [mynode] (config) #ids rate-thresholds-profile Lobby
(host) [mynode] (IDS Rate Thresholds Profile "Lobby") #channel-threshold 250
```

Related Commands

Command	Description
show ids rate-thresholds-profile	Displays the IDS rate thresholds profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids signature-matching-profile

```
ids signature-matching-profile <profile-name>
   clone <source>
   no
   signature <profile-name>
```

Description

This command configures an IDS signature matching profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile.	1-63 characters	"default"
`clone <source>`	Name of an existing IDS signature matching profile from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`signature <profile-name>`	Name of a signature profile. See ids signature-profile on page 517.	—	—

Usage Guidelines

You can include one or more predefined signature profiles or a user-defined signature profile in a signature matching profile.

Example

The following command configures a signature matching profile:

```
(host) [mynode] (config) IDS signature matching LobbyEast
(host) [mynode] (IDS Signature Matching Profile "LobbyEast") #signature Null-Probe-Response
```

Related Commands

Command	Description
show ids signature-matching-profile	Displays the IDS signature matching profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids signature-profile

```
ids signature-profile <profile-name>
   bssid <mac-addr> [valid-ap]
   clone <source>
   dst-mac <mac-addr> [valid-ap]
   frame-type {assoc|auth|beacon|control|data|deauth|disassoc|mgmt|probe-request {ssid <ssid>}
   {ssid-length <ssid-length>}|probe-response {ssid <ssid>}{ssid-length <ssid-length>}}
   no
   payload <pattern> [offset <offset>]
   seq-num <seq-num>
   src-mac <mac-addr> [valid-ap]
```

Description

This command configures signatures for wireless intrusion detection.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile. The name must be 1-63 characters.	—	“default”
`bssid <mac-addr>`	BSSID field in the 802.11 frame header.	—	—
`valid-ap`	Matches a valid AP SSID.	—	—
`clone <source>`	Name of an existing IDS signature profile from which parameter values are copied.	—	—
`dst-mac <mac-addr>`	Destination MAC address in the 802.11 frame header.	—	—
`valid-ap`	Matches a valid AP SSID.	—	—
`frame-type`	Type of 802.11 frame. For each type of frame, further parameters can be specified to filter and detect only the required frames.	—	—
`assoc`	Association frame type	—	—
`auth`	Authentication frame type	—	—
`beacon`	Beacon frame type	—	—
`control`	All control frames	—	—
`data`	All data frames	—	—
`deauth`	Deauthentication frame type	—	—
`disassoc`	Disassociation frame type	—	—
`mgmt`	Management frame type	—	—
`probe-request`	Probe request frame type	—	—

Parameter	Description	Range	Default
probe-response	Probe response frame type	—	—
ssid <ssid>	For beacon, probe-request, and probe-response frame types, specify the SSID as either a string or hex pattern.	0-32 bytes	—
ssid-length <ssid-length>	For beacon, probe-request, and probe-response frame types, specify the length, in bytes, of the SSID.	0-32 bytes	—
no	Negates any configured parameter.	—	—
payload <pattern>	Pattern at a fixed offset in the payload of an 802.11 frame. Specify the pattern to be matched as a string or hex pattern.	0-32 bytes	—
offset <offset>	When a payload pattern is configured, specify the offset in the payload where the pattern is expected to be found in the frame.	—	—
seq-num <seq-num>	Sequence number of the frame.	—	—
src-mac <mac-addr>	Source MAC address in the 802.11 frame header.	—	—
valid-ap	Matches a valid AP SSID.	—	—

Example

The following command configures a signature profile:

```
(host) [mynode] (config) #ids signature-profile floor4
(host) [mynode] (IDS Signature Profile "floor4") #frame-type assoc
(host) [mynode] (IDS Signature Profile "floor4") #src-mac 00:00:00:00:00:00
```

Usage Guidelines

The following describes the configuration for the predefined signature profiles:

Signature Profile	Parameter	Value
AirJack	frame-type	beacon ssid = AirJack
ASLEAP	frame-type	beacon ssid = asleap
Deauth-Broadcast	frame-type	deauth
	dst-mac	ff:ff:ff:ff:ff:ff
Netstumbler Generic	payload	offset=3 pattern=0x00601d
	payload	offset=6 pattern=0x0001
Netstumbler Version 3.3.0x	payload	offset=3 pattern=0x00601d
	payload	offset=12 pattern=0x000102
Null-Probe-Response	frame-type	probe-response ssid length = 0

Related Commands

Command	Description
show ids signature-profile	Displays the IDS signature profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids unauthorized-device-profile

```
ids unauthorized-device-profile <profile-name>
   adhoc-using-valid-ssid-quiet-time <adhoc-using-valid-ssid-quiet-time>
   allow-well-known-mac [hsrp|iana|local-mac|vmware|vmware1|vmware2|vmware3]
   cfg-valid-11a-channel <channel>
   cfg-valid-11g-channel <channel>
   classification
   clone <source>
   detect-adhoc-network
   detect-adhoc-using-valid-ssid
   detect-bad-wep
   detect-ht-greenfield
   detect-invalid-mac-oui
   detect-misconfigured-ap
   detect-sta-assoc-to-rogue
   detect-unencrypted-valid-client
   detect-valid-client-misassociation
   detect-valid-ssid-misuse
   detect-windows-bridge
   detect-wireless-bridge
   detect-wireless-hosted-network
   mac-oui-quiet-time <mac-oui-quiet-time>
   no
   oui-classification
   overlay-classification
   privacy
   prop-wm-classification
   protect-adhoc-enhanced
   protect-adhoc-network
   protect-adhoc-using-valid-ssid
   protect-high-throughput
   protect-ht-40mhz
   protect-misconfigured-ap
   protect-ssid
   protect-valid-sta x
   protect-windows-bridge
   protect-wireless-hosted-network
   require-wpa
   rogue-containment
   suspect-rogue-conf-level <suspect-rogue-conf-level>
   suspect-rogue-containment
   unencrypted-valid-client-quiet-time
   valid-and-protected-ssid <valid-and-protected-ssid>
   valid-oui <valid-oui>
   valid-wired-mac <valid-wired-mac>
   wireless-bridge-quiet-time <wireless-bridge-quiet-time>
   wireless-hosted-network-quiet-time <wireless-hosted-network-quiet-time>
```

Description

This command configures detection of unauthorized devices, as well as rogue AP detection and containment.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name that identifies an instance of the profile.	1-63 characters	“default”
`adhoc-using-valid-ssid-quiet-time`	Time to wait, in seconds, after detecting an ad hoc network using a valid SSID, after which the check can be resumed.	60-360000 seconds	900 seconds
`allow-well-known-mac`	Allows devices with known MAC addresses to classify rogues APs. Depending on your network, configure one or more of the following options for classifying rogue APs: ■ **hsrp**: Routers configured for HSRP, a Cisco-proprietary redundancy protocol, with the HSRP MAC OUI 00:00:0c. ■ **iana**: Routers using the IANA MAC OUI 00:00:5e. ■ **local-mac**: Devices with locally administered MAC addresses starting with 02. ■ **vmware**: Devices with any of the following VMWare OUIs: 00:0c:29, 00:05:69, or 00:50:56 ■ **vmware1**: Devices with VMWare OUI 00:0c:29. ■ **vmware2**: Devices with VMWare OUI 00:05:69. ■ **vmware3**: Devices with VMWare OUI 00:50:56. If you modify an existing configuration, the new configuration overrides the original configuration. For example, if you configure **allow-well-known-mac hsrp** and then configure **allow-well-known-mac iana**, the original configuration is lost. To add more options to the original configuration, include all of the required options, for example: **allow-well-known-mac hsrp iana**. Use caution when configuring this command. If the neighboring network uses similar routers, those APs might be classified as rogues. If containment is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack. To clear the well known MACs in the system, use the following commands: ■ **clear wms wired-mac**:This clears all of the learned wired MAC information on Mobility Master. ■ **reload**: This reboots Mobility Master.	—	—

Parameter	Description	Range	Default
`cfg-valid-11a-channel <channel>`	List of valid 802.11a channels that third-party APs are allowed to use.	34-165	—
`cfg-valid-11g-channel <channel>`	List of valid 802.11b/g channels that third-party APs are allowed to use.	1-14	—
`classification`	Enables or disables rogue AP classification. A rogue AP is one that is unauthorized and plugged into the wired side of the network. Any other AP seen in the RF environment that is not part of the valid enterprise network is considered to be interfering — it has the potential to cause RF interference but it is not connected to the wired network and thus does not represent a direct threat.	—	enabled
`clone <source>`	Name of an existing IDS rate thresholds profile from which parameter values are copied.	—	—
`detect-adhoc-network`	Enables or disables detection of ad hoc networks.	—	disabled
`detect-adhoc-using-valid-ssid`	Enables or disables detection of ad hoc networks using valid or protected SSIDs.	—	enabled
`detect-bad-wep`	Enables or disables detection of WEP initialization vectors that are known to be weak or repeating. A primary means of cracking WEP keys is to capture 802.11 frames over an extended period of time and search for implementations that are still used by many legacy devices.	—	disabled
`detect-ht-greenfield`	Enables or disables detection of high-throughput devices advertising greenfield preamble capability.	—	disabled
`detect-invalid-mac-oui`	Enables or disables checking of the first three bytes of a MAC address, known as the organizationally unique identifier (OUI), assigned by the IEEE to known manufacturers. Often clients using a spoofed MAC address do not use a valid OUI and instead use a randomly generated MAC address. Enabling MAC OUI checking causes an alarm to be triggered if an unrecognized MAC address is in use.	—	disabled

Parameter	Description	Range	Default
`detect-misconfigured-ap`	Enables or disables detection of misconfigured APs. An AP is classified as misconfigured if it is classified as valid and does not meet any of the following configurable parameters: ■ valid channels ■ encryption type ■ list of valid AP MAC OUIs ■ valid SSID list	—	disabled
`detect-sta-assoc-to-rogue`	Enables or disables detection of station association to rogue AP.	—	enabled
`detect-unencrypted-valid-client`	Enables or disables detection of unencrypted valid clients.	—	enabled
`detect-valid-client-misassociation`	Enables or disables detection of misassociation between a valid client and an unsafe AP. This setting can detect the following misassociation types: ■ MisassociationToRogueAP ■ MisassociationToExternalAP ■ MisassociationToHoneypotAP ■ MisassociationToAdhocAP ■ MisassociationToHostedAP	—	enabled
`detect-valid-ssid-misuse`	Enables or disables detection of Interfering or Neighbor APs using valid or protected SSIDs.	—	disabled
`detect-windows-bridge`	Enables or disables detection of Windows station bridging.	—	enabled
`detect-wireless-bridge`	Enables or disables detection of wireless bridging.	—	disabled
`detect-wireless-hosted-network`	If enabled, this feature can detect the presence of a wireless hosted network. When a wireless hosted network is detected this feature sends a “Wireless Hosted Network” warning level security log message and the *wlsxWirelessHostedNetworkDetected* SNMP trap. If there are clients associated to the hosted network, this feature will send a “Client Associated To Hosted Network” warning level security log message and the *wlsxClientAssociatedToHostedNetworkDetected* SNMP trap.	—	enabled
`mac-oui-quiet-time`	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.	60-360000 seconds	900 seconds

Parameter	Description	Range	Default
no	Negates any configured parameter.	—	—
oui-classification	Enables or disables OUI based rogue AP classification.	—	enabled
overlay-classification	Enables or disables overlay rogue AP classification.	—	enabled
privacy	Enables or disables encryption as a valid AP configuration.	—	disabled
prop-wm-classification	Enables or disables rogue AP classification through propagated wired MACs.	—	enabled
protect-adhoc-enhanced	Enable or disable advanced protection from open or WEP ad hoc networks. When enhanced ad hoc containment is carried out, a new repeatable event, syslog and SNMP trap will be generated for each containment event.	—	disabled
protect-adhoc-network	Enable or disable protection from ad hoc networks using WPA or WPA2 security. When ad hoc networks are detected, they are disabled using a DoS attack.	—	disabled
protect-adhoc-using-valid-ssid	Enable or disable protection from ad hoc networks using valid or protected SSIDs.	—	disabled
protect-high-throughput	Enable or disable protection of high-throughput (802.11n) devices.	—	disabled
protect-ht-40mhz	Enable or disable protection of high-throughput (802.11n) devices operating in 40 MHz mode.	—	disabled
protect-misconfigured-ap	Enable or disable protection of misconfigured APs.	—	disabled
protect-ssid	Enable or disable use of SSID by valid APs only.	—	disabled
protect-valid-sta	When enabled, does not allow valid stations to connect to a non-valid AP.	—	disabled
protect-windows-bridge	Enable or disable protection of a windows station bridging	—	disabled

Parameter	Description	Range	Default
`protect-wireless-hosted-network`	When you enable the wireless hosted network protection feature, Mobility Master enforces containment on a wireless hosted network by launching a denial of service attack to disrupt associations between a Windows 7 software-enabled Access Point (softAP) and a client, and disrupt associations between the client that is hosting the softAP and any access point to which the host connects. When a wireless hosted network triggers this feature, wireless hosted network protection sends the Wireless Hosted Network Containment and Host of Wireless Network Containment warning level security log messages, and the *wlsxWirelessHostedNetworkContainment* and *wlsxHostOfWirelessNetworkContainment* SNMP traps. **NOTE:** The existing generic containment SNMP traps and log messages will also be sent when Wireless Hosted Network Containment or Host of Wireless Network Containment is enforced.	—	disabled
`require-wpa`	When enabled, any valid AP that is not using WPA encryption is flagged as misconfigured.	—	disabled
`rogue-containment`	Rogue APs can be detected (see classification) but are not automatically disabled. This option automatically shuts down rogue APs. When this option is enabled, clients attempting to associate to an AP classified as a rogue are disconnected through a denial of service attack.	—	disabled
`suspect-rogue-conf-level <suspect-rogue-conf-level>`	Confidence level of suspected Rogue AP to trigger containment. When an AP is classified as a suspected rogue AP, it is assigned a 50% confidence level. If multiple APs trigger the same events that classify the AP as a suspected rogue, the confidence level increases by 5% up to 95%. In combination with suspected rogue containment, this option configures the threshold by which containment should occur. Suspected rogue containment occurs only when the configured confidence level is met.	50-100%	60%

Parameter	Description	Range	Default
suspect-rogue-containment	Suspected rogue APs are treated as interfering APs, thereby Mobility Master attempts to reclassify them as rogue APs. Suspected rogue APs are not automatically contained. In combination with the configured confidence level (see suspect-rogue-conf-level), this option contains the suspected rogue APs.	—	false
unencrypted-valid-client-quiet-time <unencrypted-valid-client-quiet-time>	Time to wait, in seconds, after detecting an unencrypted valid client after which the check can be resumed.	60-360000 seconds	900 seconds
valid-and-protected-ssid <ssid>	List of valid and protected SSIDs.	—	—
valid-oui <valid-oui>	List of valid MAC OUIs.	—	—
valid-wired-mac <valid-wired-mac>	List of MAC addresses of wired devices in the network, typically gateways or servers.	—	—
wireless-bridge-quiet-time <wireless-bridge-quiet-time>	Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.	60-360000 seconds	900 seconds
wireless-hosted-network-quiet-time <wireless-hosted-network-quiet-time>	The wireless hosted network detection feature sends a log message and trap when a wireless hosted network is detected. The quiet time defined by this parameter sets the amount of time, in seconds, that must elapse after a wireless hosted network log message or trap has been triggered before an identical log message or trap can be sent again.	60-360000 seconds	900 seconds

Usage Guidelines

Unauthorized device detection includes the ability to detect and disable rogue APs and other devices that can potentially disrupt network operations.

Example

The following command copies the settings from the ids-unauthorized-device-disabled profile and then enables detection and protection from ad hoc networks:

```
(host) [mynode] (config) #ids unauthorized-device-profile floor7
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #unauth1
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #clone ids-unauthorized-device-disable
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #detect-adhoc-network
(host) [mynode] (IDS Unauthorized Device Profile "floor7") #protect-adhoc-network
```

Related Commands

Command	Description
show ids unauthorized-device-profile	Displays an IDS unauthorized device profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the RFprotect license	Config mode on Mobility Master

ids wms-general-profile

```
ids wms-general-profile
   adhoc-ap-ageout-interval <adhoc-ap-ageout-interval>
   ap-ageout-interval <ap-ageout-interval>
   collect-stats
   learn-ap
   learn-system-wired-macs
   no
   persistent-neighbor
   persistent-valid-sta
   poll-interval <poll-interval>
   poll-retries <poll-retries>
   propagate-wired-macs
   sta-ageout-interval <sta-ageout-interval>
   stat-update
```

Description

This command configures the IDS WLAN management system (WMS) general profile.

Syntax

Parameter	Description	Range	Default
`adhoc-ap-ageout-interval <adhoc-ap-ageout-interval>`	Time, in minutes, that an ad hoc (IBSS) AP remains unseen before it is deleted (ageout) from the database.	0-10000	30 minutes
`ap-ageout-interval <ap-ageout-interval>`	Time, in minutes, that an AP remains unseen by any probes before it is deleted from the database.	0-10000	30 minutes
`collect-stats`	Enables or disables collection of statistics (up to 25,000 entries) on Mobility Master for monitored APs and clients.	Enable Disable	Disable
`learn-ap`	Enables or disables “learning” of non-Aruba APs.	Enable Disable	Disable
`learn-system-wired-macs`	Enables or disables “learning” of wired MACs.	Enable Disable	Disable
`no`	Negates any configured parameter.	—	—
`persistent-neighbor`	Does not age out known AP neighbors.	Enable Disable	Disable
`persistent-valid-sta`	Does not age out valid stations.	Enable Disable	Disable

Parameter	Description	Range	Default
`poll-interval <poll-interval>`	Interval, in milliseconds, for communication between Mobility Master and Aruba AMs. Mobility Master contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics.	—	60000 milliseconds (1 minute)
`poll-retries <poll-retries>`	Maximum number of failed polling attempts before the polled AM is considered to be down.	—	2
`propagate-wired-macs`	Enable/disable propagation of the gateway wired MAC information.	Enable Disable	Enable
`sta-ageout-interval <sta-ageout-interval>`	Time, in minutes, that a client remains unseen by any probes before it is deleted from the database.	—	30 minutes
`stat-update`	Enable/disable statistics updating in the database.	Enable Disable	Enable

Usage Guidelines

The WLAN management system (WMS) on Mobility Master monitors wireless traffic to detect any new AP or wireless client station in the RF environment. When an AP or wireless client is detected, it is classified, and its classification is used to determine the security policies that should be enforced on the AP or client.

By default, non-Aruba APs that are connected on the same wired networks as Aruba APs are classified as "rogue" APs. Enabling AP learning classifies non-Aruba APs as "valid" APs. Typically, you would want to enable AP learning in environments with large numbers of existing non-Aruba APs and leave AP learning enabled until all APs in the network have been detected and classified as valid. Then, disable AP learning and reclassify any unknown APs as interfering.

VLAN Trunking

In deployments where Aruba APs are not placed on every VLAN and where it is *not* possible to trunk all VLANs to an Aruba AP, enable the parameter **learned-system-wired-mac**. When this is enabled, ArubaOS is able to classify rogues on all the VLANs that belong to a Mobility Master, as long as Aruba APs can *see* the rogues in the air. If there are VLANs in the network residing on a third party controller and if those VLANs are trunked to a port on a Mobility Master, enabling this feature will allow detection of rogues on those VLANs as well.

Mobility Master/Managed Device

When **learned-system-wired-mac** is enabled in a Mobility Master deployment, the learning of Wired and Gateway MACs will happen at each managed device. For topologies with managed devices in different geographical locations, the managed device collects the Wired and Gateway MAC info and passes it to the APs that are connected to it. Even though the locals do the collection of Wired and Gateway MACs, Mobility Master is still responsible for classification.

Example

The following command enables AP learning:

```
(host) [mynode] (IDS WMS General Profile) #learn-ap
```

The following command disables AP learning:

```
(host) [mynode] (IDS WMS General Profile) #no learn-ap
```

Related Commands

Command	Description
show ids wms-general-profile	Displays general statistics for the WMS configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

ids wms-local-system-profile

```
ids wms-local-system-profile
   max-ap-threshold <max-ap-threshold>
   max-rbtree-entries <max-rbtree-entries>
   max-sta-threshold <max-sta-threshold>
   max-system-wm  <max-system-wm>
   no
   override-svc-termination <override-svc-termination>
   periodic-ap-snapshot-interval <periodic-ap-snapshot-interval>
   periodic-rogue-ap-snapshot-interval <periodic-rogue-ap-snapshot-interval>
   periodic-sta-snapshot-interval <periodic-sta-snapshot-interval>
   system-wm-update-interval <system-wm-update-interval>
```

Description

This command configures the WLAN management system (WMS) service to terminate on individual managed devices instead of Mobility Master.

Syntax

Parameter	Description	Range	Default
`max-ap-threshold`	Sets the max threshold for the total number of APs	0 to 50,000,000	—
`max-rbtree-entries`	Sets the max threshold for the total number of AP and station RBTree entries.	—	—
`max-sta-threshold`	Sets the max threshold for the total number of stations.	—	—
`max-system-wm`	Sets the max number of system wired MAC table entries learned by the managed device.	1-2000	1000
`no`	Negates or deletes an existing parameter	—	—
`override-svc-termination`	Overrides the system-determined termination mode, and terminates WMS service at the managed device to which the AP is associated. Do not use this option if you have multiple managed devices in one location, as WMS will not operate correctly.	Enable Disable	Disable

Parameter	Description	Range	Default
`periodic-ap-snapshot-interval`	Sets the interval, in minutes, at which to generate a periodic snapshot of monitored APs. The (AMON) messages comprising the snapshot are spread over this interval.	60-360 minutes	180 minutes
`periodic-rogue-ap-snapshot-interval`	Sets the interval, in minutes, at which to generate a periodic snapshot of monitored rogue APs. The (AMON) messages comprising the snapshot are spread over this interval.	5-360 minutes	30 minutes
`periodic-sta-snapshot-interval`	Sets the interval, in minutes, at which to generate a periodic snapshot of monitored clients. The (AMON) messages comprising the snapshot are spread over this interval.	60-360 minutes	180 minutes
`system-wm-update-interval`	Sets the interval, in minutes, for repopulating the system wired MAC table at the managed device.	1-30 minutes	8 minutes

Usage Guidelines

The WLAN management system (WMS) on the controller monitors wireless traffic to detect any new AP or wireless client station in the RF environment. When an AP or wireless client is detected, it is classified, and its classification is used to determine the security policies that should be enforced on the AP or client. By default, the WMS service is terminated at Mobility Master, which requires every AP across the network to communicate with the WMS service on Mobility Master. The IDS WMS local system profile includes a WMS service termination override parameter that optimizes limited bandwidth between the managed device and Mobility Master by allowing the AP communicate directly with the managed device to which it is associated.

When local WMS service termination is enabled, the WMS service on the managed device will:

- perform device classification for associated APs
- correlate events from associated APs
- update the local WMS database
- aggregate and redistribute WMS data such as wired MAC addresses, tarpit BSSIDs and valid or registered OUIs to associated APs

The devices and events detected by the managed device can (optionally) be sent to Mobility Master, allowing Mobility Master to update its database with AP, client and event information from that managed device. Note,

however, that enabling this option increases the bandwidth usage between the managed device and Mobility Master.

The configuration parameters in IDS WMS local system profile enables local termination of the WMS service, sets maximum thresholds for the maximum number of managed APs and stations, and defines the intervals at which valid AP, rogue AP and station data is sent to the managed device. Increasing the max AP or max station threshold limits in the IDS local system profile will cause an increase in usage in the memory by WMS. In general, each entry will consume about 500 bytes of memory. If a setting is bumped up by 2000, then it will cause an increase in WMS memory usage by 1 MB.

Example

The following commands first set the interval time for repopulating the MAC table to 10 minutes and then sets the maximum number of APs to 100:

```
(host) [mynode] (config) #ids wms-local-system-profile system-wm-update-interval 10
(host) [mynode] (config)# ids wms-local-system-profile max-ap-threshold 100
```

Related Commands

	Modification
mgmt-server	Configures the management server profile.
ids management-profile	Manages the events correlation for IDS event traps and syslogs (logs).
show ids wms-local-system-profile	Displays the local WLAN management system (WMS) service profile settings .

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ifmap

```
ifmap cppm
   enable
   no
   server host <host>
   port <port>
   username<username>
   passwd <password>
```

Description

This command is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass Policy Manager so that it can make more accurate decisions about what types of devices are connecting to the network.

Syntax

Parameter	Description	Default
`enable`	Enables the IFMAP protocol.	—
`server`	Configures the ClearPass Policy Manager IF-MAP server.	—
`host <host>`	IP address or hostname of the ClearPass Policy Manager IF-MAP server.	—
`port <port>`	Port number for the ClearPass Policy Manager IF-MAP server. The range is 1-65535.	443
`username <username>`	Username for the user who performs actions on the ClearPass Policy Manager IF-MAP server. The name must be between 1-255 bytes in length.	—
`passwd <password>`	Password of the user who performs actions on the ClearPass Policy Manager IF-MAP server. The password must be between 6-100 bytes in length.	—

Example

This example configures IFMAP and enables it.

```
(host) [md] (config) #ifmap
(host) [md] (config) #ifmap cppm
(host) [md] (CPPM IF-MAP Profile) #server host <host>
(host) [md] (CPPM IF-MAP Profile) #port <port>
(host) [md] (CPPM IF-MAP Profile) #passwd <psswd>
(host) [md] (CPPM IF-MAP Profile) #enable
```

Usage Guidelines

Use this command in conjunction with ClearPass Policy Manager.

Related Commands

Command	Description	Mode
show ifmap	This command is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass Policy Manager so that it can make more accurate decisions about what types of devices are connecting to the network.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on managed device

Interface cellular

```
interface cellular ip access-group session <name>
interface cellular bandwidth-contract {app | appcategory} <appname>
   <STRING> [upstream | downstream]
interface cellular bandwidth-contract exclude [app | appcategory]
   <appname>
interface cellular bandwidth-contract <STRING> [upstream | downstream]
```

Description

This command allows you to specify an ingress or egress ACL to the cellular interface of an EVDO modem.

Syntax

Parameter	Description
`interface cellular`	Configures the cellular interface.
`ip access-group session <name>`	Enter the name or number of the access group you want to apply to the EVDO modem.
`bandwidth-contract {app | appcategory | exclude | <STRING>}`	Configures the bandwidth contract for the physical interface.
`<appname>`	Specifies the app name or the app category name.

Example

```
(host) [mynode](config-submode)#ip access-group session 3
(host) [mynode](config-submode)#bandwidth-contract app myapp bc1 downstream
```

Related Command

Command	Description
show interface cellular access-group	List the Access groups configured on the cellular interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	Updated the new syntax as **ip access-group session <name>**.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration Mode (config-submode) of Mobility Master

interface gigabitethernet

```
interface gigabitethernet <slot>/<module>/<port>
   bandwidth-contract <name>|{{app <app-name>|appcategory <app-category-name>} <bw-contract-
   name>} upstream|downstream [exclude]
   description <string>
   duplex {auto|full|half}
   ip access-group {in|out|session {vlan <vlanId>}} <name>
   jumbo
   lacp {group|port-priority|timeout}
   lldp {fast-transmit-counter <1-8>|fast-transmit-interval <1-3600>|med|proprietary
   [<neighbor><discovery>]|receive|sys-tlv<disable>|transmit|transmit-hold <1-100>|transmit-
   interval <1-3600> }600>
   no ...
   openflow-disable
   poe
   port monitor {gigabitethernet <slot>/<module>/<port> | port-channel <pid>}
   priority-map <name>
   sfp-alternate-detection
   shutdown
   spanning-tree {[bpduguard]|[cost <value>]|[point-to-point]|[port-priority <value>]|
   [portfast] [vlan]}
   speed {10|100|auto}
   speed-mode {10Gbps|1Gbps|40Gbps}
   switchport {access vlan <vlan>|mode {access|trunk}|trunk {allowed vlan {<vlans>|add
   <vlans>|all|except <vlans>|remove <vlans>|<WORD>}| native vlan <vlan>}}
   transmit
   trusted {vlan <word>}
   tunneled-node-port
   xsec {point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]|vlan <vlan>}
```

Description

This command configures a GigabitEthernet interface.

Syntax

Parameter	Description	Range	Default
`<slot/module/port>`	Interface in <slot>/<module>/<port> format.	—	—
`bandwidth-contract`	Apply a bandwidth contract to all upstream of downstream traffic, or to traffic for a specified application or application category	—	—

Parameter	Description	Range	Default
`<name>`	Name of a bandwidth contract configured with the aaa bandwidth-contract command. If you specify a bandwidth contract name *before* you specify an application or application category, the bandwidth contract is applied to all downstream or upstream traffic.		
`app <name>`	Name of the application to which the bandwidth contract is applied. For a complete list of supported applications, issue the command **show dpi application all**.	—	—
`appcategory <name>`	Name of the application category to which the bandwidth contract is applied. For a complete list of supported applications, issue the command **show dpi application category all**.	—	—
`downstream`	Apply the bandwidth contract to downstream traffic.	—	—
`upstream`	Apply the bandwidth contract to upstream traffic.	—	—
`exclude <app>|<appcategory>`	Use this parameter to exclude application or application category traffic from a bandwidth contract.		
`description`	String that describes this interface.	—	—
`duplex`	Transmission mode on the interface: full or half-duplex or auto to automatically adjust transmission.	auto/full/half	auto

Parameter	Description	Range	Default
`ip access-group`	Applies the specified ACL to the interface. Use the **ip access-list** command to configure an ACL. This parameter requires the PEFNG license.	—	—
`in`	Applies ACL to interface's inbound traffic.	—	—
`out`	Applies ACL to interface's outbound traffic.	—	—
`session`	Applies session ACL to interface and optionally to a selected VLAN associated with this port.	—	—
`jumbo`	Enables or disables jumbo frame MTU configured via firewall on a port.	—	disabled
`lacp`	Configure an LACP group to the interface.	—	—

Parameter	Description	Range	Default
group <id> mode [active|passive]	Enter the LAG number (0-7) and specify the mode (**active** or **passive**). ■ Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets. ■ Passive mode—the interface is not in an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.	—	—
port-priority	Enter the port-priority value. The higher the value, the lower the priority.	1-65535	255
timeout	Enter the keyword **long** to set the LACP session to 90 seconds. Enter the keyword **short** to set the LACP session to 3 seconds.	—	90
lldp	Configures an LLDP functionality on an interface.	—	—
fast-transmit-counter	Set the number of the LLDP data units sent each time fast LLDP data unit transmission is triggered	1-8	4

Parameter	Description	Range	Default
fast-transmit-interval	Set the LLDP fast transmission interval in seconds.	1-3600	1
med	Enables the LLDP MED protocol.	—	disabled
proprietary neighbor discovery	Configures proprietary neighbor discovery.	—	—
receive	Enables processing of LLDP PDU received.	—	disabled
sys-tlv disable	Disables system TLV options.	—	enabled
transmit	Enables LLDP PDU transmit.	—	disabled
transmit-hold <1-100>	Set the transmit hold multiplier.	1-100	4
transmit-interval <1-3600>	Sets the transmit interval in seconds.	1-3600	30
no	Negates any configured parameter.	—	—
openflow-disable	Enables or disables Openflow on Gigabit Ethernet	—	disabled
poe	Enables PoE on the interface.	—	enabled
cisco	Enables Cisco-style PoE on the interface.	—	disabled
port monitor gigabitethernet port-channel	Monitors another interface on the managed device.	—	—
priority-map	Applies a priority map to the interface. Use the **priority-map** command to configure a priority map which allows you to map ToS and CoS values into high priority traffic queues.	—	—
sfp-alternate-detection	Enables detection of SFP+ via alternative communications protocol. This paramater is required for some SFP+ transceivers.	—	—

Parameter	Description	Range	Default
shutdown	Causes a hard shutdown of the interface.	—	—
spanning-tree	Enables Rapid spanning tree or Per-VLAN spanning tree.	—	enabled
bpduguard	Enables bpduguard on the edge ports.	—	disabled
cost	Administrative cost associated with the spanning tree. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.	1-65535	4
point-to-point	Set interface as point to point.	—	disabled
port-priority	Spanning tree priority of the interface. A lower setting brings the port closer to root port position (favorable for forwarding traffic) than does a higher setting. This is useful if ports may contend for root position if they are connected to an identical bridge.	0-255	128
portfast	Enables forwarding of traffic from the interface.	—	disabled
vlan	Configure a VLAN instance or a range of VLAN IDs for spanning tree.	1-4094	disabled
speed	Sets the interface speed: 10 Mbps, 100 Mbps, 1000 Mbps, or auto configuration.	10|100|1000|auto	auto

Parameter	Description	Range	Default
`speed-mode {10Gbps|1Gbps|40Gbps}`	Sets the interface speed-mode to one of the following values: ■ 10 Gbps- - You can configure this on the ports, G0/0/0, G0/0/4, G0/0/8, and G0/0/12. ■ 1 Gbps- - You can configure this on the ports, G0/0/8 and G0/0/12. ■ 40 Gbps- - You can configure this on the ports, G0/0/0 and G0/0/4. The port range details are as follows: ■ G0/0/0 - When applied on this port, the speed change is applicable to the port range 0/0/0 - 0/0/3. ■ G0/0/4 - When applied on this port, the speed change is applicable to the port range 0/0/4 - 0/0/7. ■ G0/0/8 - When applied on this port, the speed change is applicable to the port range 0/0/8 - 0/0/11. ■ G0/0/12 - When applied on this port, the speed change is applicable to the port range 0/0/12 - 0/0/15. **NOTE:** This parameter is applicable only to Aruba 7280 controllers. **NOTE:** You must reboot the controller after configuring this parameter.	10|1|40	—
`switchport`	Sets switching mode parameters for the interface.	—	—

Parameter	Description	Range	Default
`access vlan <id>`	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	1
`mode {access | trunk}`	Sets the mode of the interface to access or trunk mode only.	access|trunk	access
`port-security maximum <num> [level [[drop] [logging] [shutdown interval <seconds>]]`	Sets the port security parameters such as the maximum number of addresses that can be configured on the port. Upon exceeding the maximum limit, the port drops the packets on the port. You can also set one of the following levels for dropping the packets on exceeding the limit: ■ **drop**—drops the packets ■ **logging**—drops the packets and records a message in the log file. This is the default level. ■ **shutdown**—drops the packet, records a log message, and shuts the port down for the specified time interval.	—	—

Parameter	Description	Range	Default
`trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans> |remove <vlans>|<WORD>} | native vlan <vlan>}}`	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the managed device, or add or remove specified VLANs. You can also remove all the VLANs from the list of allowed VLANs configured on a trunk port. Specify **native** to identify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
`transmit max-rate mbits <txrate> scheduler-profile <profile-name>`	Sets a maximum transmit rate in Mbps and assigns a scheduler profile. Allowed range for maximum transmit rate is 1-100 Mbps.	—	—
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Aruba APs are attached directly to the managed device, set the port to be trusted.	—	enabled

Parameter	Description	Range	Default
`vlan <word>`	Sets the supplied range of VLANs as trusted. All remaining become untrusted automatically. For example, If you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the **no trusted vlan** command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set. However, if you execute the **trusted vlan <word>** command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs. A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.	1-4094	—
`tunneled-node-port`	Enable tunneled node capability on the interface.	—	disabled
`xsec`	Enables and configures the Extreme Security (xSec) protocol. **NOTE:** You must purchase and install the xSec software module license in the Mobility Master.	—	—

Parameter	Description	Range	Default
`point-to-point`	MAC address of the managed device that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the managed device to each other. The key must be the same on both managed device.	—	—
`allowed vlan`	VLANs that are allowed on the xSec tunnel.	—	—
`mtu`	(Optional) MTU size for the xSec tunnel.	—	—
`vlan`	xSec VLAN ID. For managed device-to-managed device communications, both managed device must belong to the same VLAN.	1-4094	—

Usage Guidelines

Use this command to configure settings for Mobility Master interface, including duplex, LLDP and switchport settings. You can issue the **show port status** command to obtain information about the interfaces currently available on the Mobility Master.

Interface Bandwidth Contracts

7000 Series controllers have the ability to classify and identify applications on the network.You can create bandwidth contracts to limit traffic for individual applications (or categories of applications) either sent from or received by a selected interface. There are two basic models for using this feature.

- **Limiting lower-priority traffic**: If there is a lower-priority application or application type that you want to limit, apply a bandwidth contract just to that application, and allow all other application traffic to pass without any limits.
- **Protecting higher-priority traffic**: If you want to guarantee bandwidth for a company-critical application or application group, you can add that application to an exception list, then apply a bandwidth contract to all remaining traffic.

You can apply bandwidth contracts using one or both of these models. Each interface supports up to 64 bandwidth contracts.

Interface contract Precedence

An interface bandwidth contract is applied to downstream traffic before a user-role bandwidth contract is applied, and for upstream traffic, the user-role bandwidth contract is applied before the interface bandwidth contract. For all traffic using compression and encryption, bandwidth contracts are applied after that traffic is compressed and encrypted. If you apply more than one bandwidth contract to any specific category type, then the bandwidth contracts are applied in the following order.

1. A contract that explicitly excludes an application

2. A contract that explicitly excludes an application category
3. A contract that applies to a specific application
4. A contract that applies to a specific application category
5. A generic bandwidth contract, not specific to any application or application category

Example

The following commands configure an interface as a trunk port for a set of VLANs:

```
(host) [mynode] (config) # interface gigabitethernet 0/0/0
(host) [mynode] (config-range)# switchport mode trunk
(host) [mynode] (config-range)# switchport trunk native vlan 10
(host) [mynode] (config-range)# switchport trunk allowed vlan 1,10,100
```

The following commands configure trunk port 0/0/0 with test-acl session for VLAN 2.

```
(host) [mynode] (config) # interface range gigabitethernet 0/0/0
(host) [mynode] (config-range)# switchport mode trunk
(host) [mynode] (config-range)# ip access-group
(host) [mynode] (config-range)# ip access-group test session vlan 2
```

The following commands configure a interface bandwidth contract for a high-priority application.

```
(host) [mynode] (config) # interface gigabitethernet 0/0/1
(host) [mynode] (config) # bw-contract protectskype4b exclude app alg-skype4b-voice downstream
```

Related Commands

Command	Description
show interface gigabitethernet	Displays information about a specified Gigabit Ethernet port.

Command History

Release	Modification
ArubaOS 8.3.0.0	A new parameter, **speed-mode**, was added.
ArubaOS 8.2.0.0	The following changes were introduced: ■ Updated the new syntax as **ip access-group {in|out|session {vlan <vlanId>}} <name>** ■ A new sub parameter **<WORD>** was added under **switchport trunk allowed** parameter. You can specify **none** to remove all the VLANs from the list of allowed VLANs configured on the trunk port. ■ A new parameter, **sfp-alternate-detection**, was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system. The **ip access-group** parameter requires the PEFNG license. The **xsec** parameter requires the xSec license.	Config mode on Mobility Master.

interface loopback

```
interface loopback
   ip address <ipaddr>
   ipv6 address <ipv6-prefix>
   no ...
```

Description

This command configures the loopback address on Mobility Master.

Syntax

Parameter	Description
`ip address`	Host IP address in dotted-decimal format. This address is routed from all external networks.
`ipv6 address`	Host IPv6 address that can be routed from all external networks.
`no`	Negates any configured parameter.

Usage Guidelines

If configured, the loopback address is used as Mobility Master's IP address. If you do not configure a loopback address for Mobility Master, the IP address assigned to VLAN 1 is used as Mobility Master's IP address. After you configure or modify a loopback address, you need to reboot Mobility Master.

Example

The following command configures a loopback address:

```
(host) [mynode] (config) #interface loopback
(host) [mynode] (config-submode)#ip address 10.2.22.220
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system.	Config mode on Mobility Master.

interface mgmt

```
interface mgmt
   dhcp
               ip address <ipaddr> <ipmask>  [vlan-tag <vlanid>]
   ipv6 address <ipaddr>/<prefix-length> [vlan-tag <vlanid>]
   no ...
   shutdown
```

Description

This command configures the out-of-band Ethernet management port on controller.

Syntax

Parameter	Description
`dhcp`	Enables DHCP on the interface.
`ip address`	Configures an IP address and netmask on the interface.
`vlan-tag <vlanid>`	(Optional) Tags the management interface with the specified VLAN ID.
`ipv6 address <ipaddr>`	Configures an IPv6 address on the interface.
`vlan-tag <vlanid>`	(Optional) Tags the management interface with the specified VLAN ID.
`no`	Negates any configured parameter.
`shutdown`	Causes a hard shutdown of the interface.

Usage Guidelines

Execute this command on the device level from the Mobility Master. This command is applicable only for the 7000 Series platforms.

Use the **show interface mgmt** command to view the current status of the management port.

Example

The following command configures an IP address on the management interface:

```
(host) [mynode] (config) #interface mgmt
   (host) [mynode] (config-submode) #ip address 10.1.1.1 255.255.255.0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	**vlan-tag** optional sub-parameter was introduced under the **ip address** and **ipv6 address** parameters.

Command Information

Platforms	License	Command Mode
7000 Series controllers	Base operating system	Config mode on Mobility Master.

interface port-channel

```
interface port-channel <id>
   description <LINE>
   gigabitethernet <slot/module/port>
   ip access-group {in <name>|out <name>|session <name>|vlan <vlanId> {session <name>}}
   jumbo
   no ...
   openflow-disable
   shutdown
   spanning-tree [bpduguard|cost <value>|point-to-point|port-priority <value>|portfast [trunk]
   |vlan  {range <WORD>|<vlanid>}]
   switchport {access vlan <vlan>|mode {access|trunk}|trunk {allowed vlan {<vlans>|add
   <vlans>|all|except <vlans>|remove <vlans>| native vlan <vlan>}
   trusted {vlan [add|remove] <word>}
   xsec {{point-to-point <macaddr> <key> allowed vlan <vlans> [<mtu>]}|vlan <vlan>}
```

Description

This command configures an Ethernet port channel.

Syntax

Parameter	Description	Range	Default
`<id>`	ID number for this port channel.	0-7	—
`description <LINE>`	A character string describing this port-channel.	up to 60 characters	—
`gigabitethernet <slot/module/port>`	Adds the specified GigabitEthernet interface to the port channel.	—	—
`ip <access-group>`	Applies the specified ACL to the interface. Use the **ip access-list** command to configure an ACL. This command requires the PEFNG license.	—	—
`in <name>`	Applies ACL to interface's inbound traffic.	—	—
`out <name>`	Applies ACL to interface's outbound traffic.	—	—
`session <name>`	Applies session ACL to interface and optionally to a selected VLAN associated with this port.	—	—
`vlan <vlanId> {session <name>}`	Applies session ACL to VLAN.	1-4094	–

Parameter	Description	Range	Default
jumbo	Enables or disables jumbo frame MTU configured via firewall on a port channel.		Disabled
no	Negates any configured parameter.	—	—
openflow-disable	Enables or disables Openflow on the port channel.	—	disabled
shutdown	Causes a hard shutdown of the interface.	—	—
spanning-tree	Enables spanning tree.	—	—
bpduguard	Enables BPDU guard on the port channel.	—	Disabled
cost <value>	Specify the cost value of the spanning tree path for an interface.	1 - 65535	—
point-to-point	Configures the interface as a point to point link.	—	—
port-priority <value>	Specify the spanning tree priority for the interface.	0 - 255	—
portfast [trunk}	Enables forwarding of traffic from the interface. Optionally you can choose a trunk port for forwarding the traffic.	—	—
vlan {range <WORD> | <vlanid>}]	Configure a VLAN instance or a range of VLAN IDs for the	—	—
switchport	Sets switching mode parameters for the interface.	—	—
access vlan <vlanId>	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	—
mode {access | trunk}	Sets the mode of the interface to access or trunk mode only.	—	—
port-security maximum <num>	Sets the maximum number of MAC addresses that can be configured on the port channel.	16-32768	—

Parameter	Description	Range	Default
`trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans> |remove <vlans>}|native vlan <vlan>}}`	Sets the interface as a trunk port for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the managed device, or add or remove specified VLANs. Optionally you can specify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Aruba APs are attached directly to a managed device, set the port to be trusted.	—	disabled

Parameter	Description	Range	Default
`vlan [add|remove] <word>`	Sets the specified range of VLANs as trusted. All remaining become untrusted automatically. For example, if you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the **no trusted vlan** command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set. However, if you execute the **trusted vlan** <**word**>command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs. A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.	1-4094	—
`xsec`	Enables and configures the Extreme Security (xSec) protocol. You must purchase and install the xSec software module license in the managed device.	—	—
`point-to-point`	MAC address of the device that is the xSec tunnel termination point, and the 16-byte shared key used to authenticate the device to each other. The key must be the same on both devices.	—	—
`allowed vlan`	VLANs that are allowed on the xSec tunnel.	—	—
`mtu`	(Optional) MTU size for the xSec tunnel.	—	—

Parameter	Description	Range	Default
`vlan`	xSec VLAN ID. For managed device-to-managed device communications, both managed devices must belong to the same VLAN.	1-4094	—

Usage Guidelines

A port channel allows you to aggregate ports on a managed device. You can configure a maximum of 8 port channels per supported managed device with a maximum of 8 interfaces per port channel.

Note the following when setting up a port channel between a managed device and a Cisco switch (such as a Catalyst 6500 Series Switch):

- There must be no negotiation of the link parameters.
- The port-channel mode on the Cisco switch must be “on”.

Example

The following command configures a port channel:

```
(host) (config) #interface port channel 7
(host) [mynode] (config-submode)#gigabitethernet 0/0/1
(host) [mynode] (config-submode)#gigabitethernet 0/0/2
```

Command History

Release	Modification
ArubaOS 8.2.0.0.	Updated the new syntax as **ip access-group {in <name>|out <name>|session <name>|vlan <vlanId> {session <name>}}**.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system. The **ipaccess-group** parameter requires the PEFNG license. The **xsec** parameter requires the xSec license.	Config mode on Mobility Master.

interface range

```
interface range gigabitethernet <slot>/<module-start>/<port-start>-<module-end>/<port-end>
   ip access-group {in|out|session {vlan <vlanId>}} <acl)_name>
   lacp
   lldp
   no
   shutdown
   switchport {access vlan <vlan>|mode {access|trunk}|trunk {allowed vlan {<vlans>|add
   <vlans>|all|except <vlans>|remove <vlans>}|
    native vlan <vlan>}}
   trusted {vlan <word>}
```

Description

This command configures a range of GigabitEthernet interfaces on the managed device.

Syntax

Parameter	Description	Range	Default
`range`	Range of Ethernet ports in the format <slot>/<module>/<port>-<port>. where <slot>/<module>/<port> is the interface.	—	—
`duplex`	Transmission mode on the interface: full- or half-duplex or auto to automatically adjust transmission.	auto/full/half	auto
`ip access-group`	Applies the specified ACL to the interface. Use the ip access-list command to configure an ACL.	—	—
`in`	Applies ACL to interface's inbound traffic.	—	—
`out`	Applies ACL to interface's outbound traffic.	—	—
`session`	Applies session ACL to interface and optionally to a selected VLAN associated with this range of ports.	—	—
`lacp`	Configure an LACP group to the interface.	—	—

Parameter	Description	Range	Default
group <id> mode [active|passive]	Enter the LAG number (0-7) and specify the mode (**active** or **passive**). ■ Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets. ■ Passive mode—the interface is not in an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.	—	—
port-priority <value>	Enter the port-priority value. The higher the value, the lower the priority.	1-65535	255
timeout	Enter the keyword **long** to set the LACP session to 90 seconds. Enter the keyword **short** to set the LACP session to 3 seconds.	—	90
lldp	Configures an LLDP functionality on an interface.	—	—
fast-transmit-counter	Set the number of the LLDP data units sent each time fast LLDP data unit transmission is triggered	1-8	4
fast-transmit-interval	Set the LLDP fast transmission interval in seconds.	1-3600	1
med	Enables the LLDP MED protocol.	—	disabled

Parameter	Description	Range	Default
`receive`	Enables processing of LLDP PDU received.	—	disabled
`transmit`	Enables LLDP PDU transmit.	—	disabled
`transmit-hold <1-100>`	Set the transmit hold multiplier.	1-100	4
`transmit-interval <1-3600>`	Sets the transmit interval in seconds.	1-3600	30
`no`	Negates any configured parameter.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`switchport`	Sets switching mode parameters for the interface.	—	—
`access vlan`	Sets the interface as an access port for the specified VLAN. The interface carries traffic only for the specified VLAN.	—	—
`mode`	Sets the mode of the interface to access or trunk mode only.	—	—
`trunk {allowed vlan {<vlans>|add <vlans>|all|except <vlans> |remove <vlans>}|native vlan <vlan>}}`	Sets the interfaces as trunk ports for the specified VLANs. A trunk port carries traffic for multiple VLANs using 802.1q tagging to mark frames for specific VLANs. You can include all VLANs configured on the managed device, or add or remove specified VLANs. Optionally you can specify the native VLAN for the trunk mode interface. Frames on the native VLAN are not 802.1q tagged.	—	—

Parameter	Description	Range	Default
`trusted`	Set this interface and range of VLANs to be trusted. VLANs not included in the trusted range of VLANs will be, by default, untrusted. Trusted ports and VLANs are typically connected to internal controlled networks, while untrusted ports connect to third-party APs, public areas, or other networks to which access controls should be applied. When Aruba APs are attached directly to the managed device, set the port to be trusted.	—	enabled
`vlan <word>`	Sets the specified range of VLANs as trusted. All remaining become untrusted automatically. For example, If you set a VLAN range as: vlan 1-10, 100-300, 301, 305-400, 501-4094 Then all VLANs in this range are trusted and all others become untrusted by default. You can also use the **no trusted vlan** command to explicitly make an individual VLAN untrusted. The no trusted vlan command is additive and adds given vlans to the existing untrusted vlan set. However, if you execute the **trusted vlan** <**word**> command, it overrides any earlier untrusted VLANs or a range of untrusted VLANs and creates a new set of trusted VLANs. **NOTE:** A port supports a user VLAN range from 1-4094. If you want to set all VLANs (1-4094) on a port as untrusted then mark the port itself as untrusted. By default the port and all its associated VLANs are trusted.	1-4094	—

Usage Guidelines

Use the show port status command to obtain information about the interfaces available on the managed device. You can execute this command only on a hardware platform that acts as a managed device or as a stand-alone controller.

Example

The following command configures a range of interface as a trunk port for a set of VLANs:

```
(host) [00:0b:86:99:88:17] (config) #interface range gigabitethernet 0/0/0-0/17
(host) [00:0b:86:99:88:17] (config-submode)#switchport mode trunk
(host) [00:0b:86:99:88:17] (config-submode)#switchport trunk native vlan 10
(host) [00:0b:86:99:88:17] (config-submode)#switchport trunk allowed vlan 1,10,100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	Updated the new syntax as **ip access-group {in|out|session {vlan <vlanId>}} <acl)_name>**.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

interface tunnel

```
interface tunnel <number>
   autogenerate peer <peer-mac-address>
   description <string>
   inter-tunnel-flooding
   ip
      access group in <acl-name>
      address {internal | pool tunnel-pool <pool-name> |{<ipaddr> <netmask>}}
      ospf
         area <area-id>
         authentication message-digest
         cost <value>
         dead-interval <value>
         hello-interval <value>
         message-digest-key <id> <pwd>
         priority <value>
         retransmit-interval <value>
         transmit-delay <value>
   ipv6 address X:X:X:X::X
   mtu <mtu>
   no ...
   openflow-enable
   shutdown
   trusted
   tunnel
      destination <ip-addr>|{ipv6 <ipv6-addr>}
      keepalive cisco |{<interval> <retries>}
      mode gre {<num>|ip|ipv6}
      source
         controller-ip
         ipv6 {<ipv6-addr>|loopback|controller-ip|{vlan <vlan id>}}
         loopback
         {vlan <vlan-id>}
         <ip-addr>
      vlan {<vlan id>|add|remove}
```

Description

This command configures a Layer-2 or Layer-3 GRE tunnel between a managed device and another GRE-capable device.

Syntax

Parameter	Description	Range	Default
`tunnel <number>`	Tunnel Identification number. The tunnel ID used here does not have to match the tunnel ID used in the other managed device.	1-16777215	—
`autogenerate peer <peer-mac-address>`	Auto generates the tunnel endpoint for the specified peer device.	—	—

Parameter	Description	Range	Default
`description`	String that describes this tunnel.	—	—
`inter-tunnel-flooding`	Enables inter-tunnel flooding.	—	Enabled
`ip access group in <acl-name>`	Attach a route ACL to a L3 GRE tunnel interface. When you associate a routing ACL to inbound traffic on a managed device terminating a L3 GRE tunnel, that ACL can forward traffic as normal, route traffic to a nexthop router on a nexthop list, or redirect traffic over an L3 GRE tunnel or tunnel group. For more information on creating a routing ACL, see ip access-list route.	—	—
`ip address {internal | pool tunnel-pool <pool-name> |{<ipaddr> <netmask>}}`	IP address of the Layer 3 tunnel. This represents the entrance to the tunnel. **NOTE:** This address should be a unique, non-routable IP address. Enter one of the following values: ■ internal: IP address is allocated from the Remote-Node pool. ■ pool tunnel-pool <pool-name>: IP address is allocated from the specified tunnel pool. ■ <ipaddr>: An IPv4 address. **NOTE:** The IP address should not be part of any subnet in your network, nor does it have to be routable in your network. It is used as a gateway for routing your private subnets (i.e., non-routable VLANs) within the GRE tunnel. ■ <netmask>: IP subnet mask.	—	—

Parameter	Description	Range	Default
`ipv6`	IPv6 address of the Layer-3 GRE tunnel. **NOTE:** This IP address can be configured only for a Layer-3 GRE tunnel (refer to the "*mode gre*" parameter below for details).	—	—
`mtu`	MTU size for the interface.	1024 - 9216	Enabled IPv4: 1100 IPv6: 1500
`no`	Negates any configured parameter.	—	—
`openflow-enable`	Enables OpenFlow on the tunnel.	—	disabled
`shutdown`	Causes a hard shutdown of the interface.	—	—
`trusted`	■ **When Trusted is enabled**: Any device can send any traffic through the GRE tunnel without having to be authenticated. ■ **When Trusted is disabled**: Any device that is a source of traffic and is sent through the tunnel must be authenticated to be able to send the traffic. If the device is not authenticated, traffic from that device will be subject to the restrictions of the Initial Role specified in the Wired Access AAA Profile. This is the default. For related information, see aaa authentication wired.	—	Disabled
`tunnel`	Configures tunneling. The default is an IPv4 Layer-3 GRE tunnel.	—	mode gre ip
`destination <ip-addr> |ipv6 <ipv6-addr>`	The destination IP address (v4 or v6) for the GRE tunnel endpoint.	—	—

Parameter	Description	Range	Default
`keepalive {cisco | {<interval> <retries>}}`	Enables sending of periodic keepalive frames on the tunnel to determine the tunnel status (up or down). You can optionally set the interval at which keepalive frames are sent, and the number of times the frames are resent before a tunnel is considered to be down. **NOTE:** Executing the **no tunnel keepalive** command disables the keepalive frames, but retains the configured interval and retry values.	—	Disabled
`cisco`	The <**cisco**> option enables keepalive interoperability for Layer-3 tunnels between managed devices and Cisco network devices. Aruba sets the keepalive packet's GRE protocol field to 0x801; however, Cisco sets the GRE protocol field to 0. When this option is enabled, the Aruba managed device automatically sets the GRE protocol value to 0.		Disabled
`<interval>`	Number of seconds at which keepalive frames are sent.	1-86400	10 seconds
`<retries>`	Number of consecutive times that the keepalives fail before the tunnel is considered to be down.	0-1024	3

Parameter	Description	Range	Default
`mode gre {ip|ipv6|<num>}`	This parameter a) specifies the tunnel encapsulation method as **GRE** and b) allows you to specify whether it is a Layer-2 or Layer-3 GRE tunnel. ■ **ip**: Specifies an IPv4 Layer-3 GRE tunnel. The protocol number is set to **0x0800** and is not configurable. Traffic is redirected into the tunnel using a static route or a session ACL policy. The managed device encapsulates the Layer-3 packet only. ■ **ipv6**: Specifies an IPv6 Layer-3 GRE tunnel. The protocol number is set to **0x86DD** and is not configurable. Traffic is redirected into the tunnel using a static route or a session ACL policy. The managed device encapsulates the Layer-3 packet only. ■ **<num>**: A 16-bit protocol number that uniquely identifies a GRE tunnel. The number format is numeric. The managed devices at both endpoints of the tunnel must be configured with the same protocol number. The protocol number does not necessarily have to match the protocol number of the encapsulated frame. The managed device encapsulates the entire frame, including the Layer-2 header.	—	—

Parameter	Description	Range	Default
`source`	The local endpoint of the tunnel on the controller. This can be one of the following: ■ controller-ip: IPv4 address of the managed device. ■ ipv6: Specify one of the following IPv6 options: ● <X:X:X:X::X>: Specify the IPv6 address. ● controller-ip: IPv4 address of the managed device. ● loopback: IPv6 loopback inter-face configured on the managed device. ● vlan <vlan id>: Specify the VLAN interface ID. ■ loopback: Loopback interface configured on the managed device. ■ vlan <vlanid>: Specify the VLAN interface ID. ■ <A.B.C.D>: Specify an IPv4 address.	—	—

Parameter	Description	Range	Default
`vlan <id>`	Specify the VLANs to be included in this tunnel. ■ add: The VLANs to be added to the current list. ■ remove: The VLANs to be removed from the current list. **NOTE:** You can configure a VLAN only if the tunnel mode is set to Layer-2 (**mode gre <16-bit protocol number>**). If the tunnel mode is not set to Layer-2 mode, the system displays an error message: *Tunnel is an IP [v6] GRE Tunnel. Change the mode before adding this*.	—	—

Usage Guidelines

You can configure a Layer-2 or Layer-3 GRE tunnel between an Aruba managed device and another GRE-capable device. The default is an IPv4 Layer-3 GRE tunnel (**tunnel mode gre ip**).

In Layer-3 GRE tunnels, IPv6 encapsulated in IPv4 and IPv4 encapsulated in IPv6 are not supported. The only Layer-3 GRE modes supported are IPv4 encapsulated in IPv4 and IPv6 encapsulated in IPv6.

You can direct traffic into the tunnel using a static route (by specifying the tunnel as the next hop for a static route) or a session-based ACL.

Configuration Examples

Layer-2 GRE Tunnel

The following CLI command configures a Layer-2 GRE tunnel:

MN-1 Configuration

```
(host) [mynode] (config)# interface tunnel 101
  description "IPv4 Layer-2 GRE 101"
  tunnel mode gre 1
  tunnel source vlan 10
  tunnel destination 20.20.20.249
  tunnel keepalive
  trusted
  tunnel vlan 101
```

MN-2 Configuration

```
(host) [mynode] (config)# interface tunnel 101
  description "IPv4 Layer-2 GRE 101"
  tunnel mode gre 1
  tunnel source vlan 20
  tunnel destination 10.10.10.249
  tunnel keepalive
  trusted
```

```
   tunnel vlan 101
```

IPv4 Layer-3 GRE Tunnel

The following CLI command examples configure a Layer-3 GRE tunnel for IPv4 between two managed devices.

MN-1 Configuration

```
(MN-1) (host) [mynode] (config) #interface tunnel 202
   (host) [mynode] (config-submode) #description "IPv4 L3 GRE 101"
   (host) [mynode] (config-submode) #tunnel mode gre ip
   (host) [mynode] (config-submode) #ip address 1.1.1.1 255.255.255.255
   (host) [mynode] (config-submode) #tunnel source vlan 10
   (host) [mynode] (config-submode) #tunnel destination 20.20.20.249
   (host) [mynode] (config-submode) #trusted
```

MN-2 Configuration

```
(MN-2) (host) [mynode] (config) #interface tunnel 202
   (host) [mynode] (config-submode) #description "IPv4 L3 GRE 202"
   (host) [mynode] (config-submode) #tunnel mode gre ip
   (host) [mynode] (config-submode) #ip address 1.1.1.2 255.255.255.255
   (host) [mynode] (config-submode) #tunnel source vlan 20
   (host) [mynode] (config-submode) #tunnel destination 10.10.10.249
   (host) [mynode] (config-submode) #trusted
```

IPv6 Layer-3 GRE Tunnel

The following CLI command examples configure a Layer-3 GRE tunnel for IPv6 between two managed devices.

MN-1 Configuration

```
(MN-1) (host) [mynode] (config) #interface tunnel 106
   (host) [mynode] (config-submode) #description "IPv6 Layer-3 GRE 106"
   (host) [mynode] (config-submode) #tunnel mode gre ipv6
   (host) [mynode] (config-submode) #ip address 2001:1:2:1::1
   (host) [mynode] (config-submode) #tunnel source vlan 10
   (host) [mynode] (config-submode) #tunnel destination 2001:1:2:2020::1
   (host) [mynode] (config-submode) #trusted
```

MN-2 Configuration

```
(MN-2) (host) [mynode] (config) #interface tunnel 206
   (host) [mynode] (config-submode) #description "IPv6 Layer-3 GRE 206"
   (host) [mynode] (config-submode) #tunnel mode gre ipv6
   (host) [mynode] (config-submode) #ip address 2001:1:2:1::2
   (host) [mynode] (config-submode) #tunnel source vlan 20
   (host) [mynode] (config-submode) #tunnel destination 2001:1:2:1010::1
   (host) [mynode] (config-submode) #trusted
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Updated the new syntax as **access group in <acl-name>**.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master

interface vlan

```
interface vlan <vlan>
   bandwidth-contract <name>
   bcmc-optimization
   description <string>
   filter-broadcast-on-helper
   filter-broadcast-on-ipv6-helper
   ip
      access-group in <acl_name>
      address {<ipaddr> <ipmask>|dhcp-client client-id<cid>|internal|pppoe}
      helper-address <address>
      igmp {proxy {gigabitethernet <slot/module/port> | port-chanel <id>}}|snooping
      local-proxy-arp
      nat {inside|outside}
      ospf
         area
         authentication message-digest
         cost <value>
         dead-interval <1-65535>
         hello-interval <1-65535>
         message-digest-key  <1 - 255> <passwd>
         priority <0-255>
         retransmit-interval <1-65535>
         transmit-delay <1-65535>
      pppoe-max-segment-size <mss>
      pppoe-password <password>
      pppoe-service-name <service-name>
      pppoe-username <username>
      routing
   ipv6
      address {dhcp6-client|link-local  <ipv6-address>|pd <pd-name> ::X:X:X:X:X|<ipv6-pre-
      fix>/<prefix-length> eui-64}
      dhcp {pdclient <pd_name>|server <pool name>}
      helper-address <address>
      mld {proxy {gigabitethernet <slot/module/port>|port-chanel <id>}}|snooping
      nd
         ra {dns <ipv6_address>|enable|hop-limit <value>|interval <value>|life-time <value>|-
         managed-config-flag|mtu <value>|other-config-flag|preference {high|low|medium}|prefix
         X:X:X:X::X/<0-128>}
         reachable-time <value>
         retransmit-time <value>
   mtu <1280-1500>
   multimode-auth lease-time <5-3600>
   no ...
   operstate up
   option-82 {ap-name essid}|{mac [essid]}
   shutdown
   suppress-arp
```

Description

This command configures a VLAN interface.

Syntax

Parameter	Description	Range	Default
`vlan`	VLAN ID number.	1-4094	—
`bandwidth-contract <name>`	Name of the bandwidth contract to be applied to this VLAN interface. When applied to a VLAN, the contract limits both broadcast and multicast traffic. Use the **aaa bandwidth-contract** command to configure a bandwidth contract.	—	—
`bcmc-optimization`	Enables broadcast and multicast traffic optimization to prevent flooding of broadcast and multicast traffic on VLANs. If this feature is enabled on uplink ports, any managed device-generated Layer-2 packets will be dropped.	—	disabled
`description`	String that describes this interface.	—	802.1q VLAN
`filter-broadcast-on-helper`	Filters DHCP discover broadcast when the helper is configured.	—	—
`filter-broadcast-on-ipv6-helper`	Filters DHCPv6 client multicast packets when the helper is configured.	—	—
`ip`	Configures IPv4 for this interface.		
`access-group in <acl_name>`	Assigns an access list to inbound traffic on the interface, where <name> is the name of an access list.		
`address`	Configures the IP address for this interface, which can be one of the following: <ipaddr> <netmask> ■ dhcp-client: use DHCP to obtain the IP address ■ internal: IP address allocated from the branch group config. ■ pppoe: use PPPoE to obtain the IP address	—	—
`helper-address <address>`	IP address of the DHCP server for relaying DHCP requests for this interface. If the DHCP server is on the same subnetwork as this VLAN interface, you do not need to configure this parameter.	—	—
`igmp`	Enables IGMP proxy or IGMP snooping on this interface. See interface vlan ip igmp for complete details on this parameter.	—	—
`local-proxy-arp`	Enables local proxy ARP.	—	—

Parameter	Description	Range	Default
`nat {inside|outside}`	Enables source NAT for all traffic routed from or to this VLAN. **CAUTION:** All ports on the managed device are assigned to VLAN 1 by default. Do not enable the **nat inside** option for VLAN 1, as this will prevent IPsec connectivity between the managed device and its IPsec peers.	—	—
`ospf`	Define an OSPF area. See interface vlan ip ospf for complete details on this parameter.	—	—
`pppoe-max-segment-site`	Configures the TCP MSS in bytes.	128	—
`pppoe-password`	Configures the PAP password on the PPPoE Access Concentrator for the switch.	1–80	—
`pppoe-service-name`	Configures the PPPoE service name.	1–80	—
`pppoe-username`	Configures the PAP username on the PPPoE Access Concentrator for the switch.	1–80	—
`routing`	Enables layer-3 forwarding on the VLAN interface. To disable layer-3 forwarding, you must configure the IP address for the interface and specify **no ip routing**.	—	(enabled)
`ipv6`	Configures IPv6 for this interface.	—	—
`address`	Configures the IPv6 address of interface. ■ **dhcp6-client** - The DHCPv6 is used to obtain an IPv6 address. ■ **link-local** - The link local address ■ **pd** - The prefix obtained by PD client on uplink. ■ **X:X:X:X::X/<0-128>** - The IPv6 prefix/prefix-length used to configure the global unicast address for this interface.	—	—
`dhcp`	Configures DHCP for IPv6. **pdclient** - The IPv6 prefix from a DHCPv6 Prefix delegation server. **server** - Configures the DHCPv6 pool for the vlan.	—	—
`helper-address <address>`	IPv6 address of the DHCP server for relaying DHCP requests for this interface. If the DHCP server is on the same subnetwork as this VLAN interface, you do not need to configure this parameter.	—	—

Parameter	Description	Range	Default
`mld`	Enables MLD on this interface. **proxy** - Configures MLD proxy on the following interfaces. ■ fastethernet ■ gigabitethernet <slot/module/port> ■ port-channel **snooping** - Configures the MLD snooping on this interface.	—	—
`nd {ra | reachable-time |retransmit-time}`	Configures the IPv6 neighbor discovery options. **ra** - configures the following router advertizement options: ■ **dns** - Configures IPv6 recursive DNS server ■ **enable** - Enables IPv6 RA ■ **hop-limit** - Configures RA hop-limit ■ **interval** - Configures RA interval ■ **life-time** - Configures RA lifetime ■ **managed-config-flag** - Enables hosts to use DHCP server for stateful address autoconfiguration ■ **mtu** - Configures MTU for RA ■ **other-config-flag** - Enables hosts to use DHCP server for other non-address stateful autoconfiguration ■ **preference** - Configures a router preference of high/low/medium ■ **prefix** - Configures IPv6 RA prefix **reachable-time** - Configures neighbor discovery reachable time. By default this field is set to 0. Valid value - 0-3, 600,000 msec. **retransmit-time** - Configures neighbor discovery retransmit time. By default this field is set to 0. Valid value - 0-3, 600,000 msec.	—	—
`no`	Negates any configured parameter.	—	—
`mtu`	MTU setting for the VLAN.	1024-1500	—
`multimode-auth`	MultiMode Authentication Support on VLAN	—	—
`operstate up`	Set the state of the interface to be up.	—	—

Parameter	Description	Range	Default
`option-82 {ap-name [essid] |mac [essid]}`	Allows a DHCP relay agent to insert circuit specific information into a request that is being forwarded to a DHCP server. The managed device, when acting as a DHCP relay agent, needs to be able to insert information about the AP and SSID through which a client is connecting into the DHCP request. Many service providers use this mechanism to make access control decisions. You can include: ■ AP name or AP name and ESSID. ■ MAC address or MAC address and ESSID.	—	—
`shutdown`	Causes a hard shutdown of the interface.	—	—
`suppress-arp`	Prevents flooding of ARP broadcasts on all the untrusted interfaces.	—	—

Usage Guidelines

All ports on the managed device are assigned to VLAN 1 by default. Use the **interface gigabitethernet** command to assign a port to a configured VLAN. Use the **show interface vlan** and **show user** commands to view DHCP option-82 related output.

Example

The following command configures a VLAN interface:

```
(host) [mynode] (config) #interface vlan 16
   (host) [mynode] (config-submode) #ip address 10.26.1.1 255.255.255.0
   (host) [mynode] (config-submode) #ip helper-address 10.4.1.22
```

The following example displays the use of extended scope of address range:

```
(host)[mynode](config) #interface vlan 214
   (host) [mynode] (config-submode) #ipv6 address 2014::2/64
   (host) [mynode] (config-submode) #ipv6 nd reachable-time 1000
   (host) [mynode] (config-submode) #ipv6 nd retransmit-time 1000
   (host) [mynode] (config-submode) #ipv6 nd ra enable
   (host) [mynode] (config-submode) #ipv6 nd ra preference high
   (host) [mynode] (config-submode) #ipv6 nd ra prefix 2014::/64
   (host) [mynode] (config-submode) #operstate up
   (host) [mynode] (config-submode) #ipv6 mld snooping
```

Related Commands

Command	Description
ip access-list route	This command configures an ACL for PBR.
ip nexthop-list	Use this command to define a next-hop list for a routing policy.

Command History

Release	Modification
ArubaOS 8.2.0.0.	The following changes were introduced: ■ Updated the new syntax as **access-group in <acl_name>**. ■ Added the following sub-parameters: • **filter-broadcast-on-helper** • **filter-broadcast-on-ipv6-helper** • **ipv6 <helper-address>**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

interface vlan ip igmp

```
interface vlan <vlan>
   ip igmp {proxy {gigabitethernet <slot/module/port>} | port-channel <id>} | snooping
```

Description

This command enables IGMP or IGMP snooping on this interface, or configures a VLAN interface for uninterrupted streaming of multicast traffic.

Syntax

Parameter	Description
`proxy`	Enable IGMP proxy for this interface.
`gigabitethernet <slot/module/port>`	Enable IGMP proxy on the specified GigabitEthernet (IEEE 802.3) interface.
`port-channel <id>`	Enable IGMP proxy on the specified port channel.
`snooping`	Enable IGMP snooping. The IGMP protocol enables an router to discover the presence of multicast listeners on directly-attached links. Enable IGMP snooping to limit the sending of multicast frames to only those nodes that need to receive them.

Usage Guidelines

The newer IGMP proxy feature and the older IGMP snooping feature cannot be enabled at the same time, as both features add membership information to multicast group table. For most multicast deployments, you should enable the IGMP Proxy feature on all VLAN interfaces to manage all the multicast membership requirements on the managed device. If IGMP snooping is configured on some of the interfaces, there is a greater chance that multicast information transfers may be interrupted.

This release of ArubaOS supports version 1 of the MLD protocol (MLDv1). MLDv1, defined in RFC 2710, is derived from version 2 of the IPv4 IGMPv2. You can use the command **interface vlan <vlan> ipv6 mld** to enable the MLD protocol and allow an IPv6 router to discover the presence of multicast listeners on directly-attached links. Use the CLI command **interface vlan <vlan> ipv6 mld snooping** for the Pv6 router to send multicast frames to only those nodes that need to receive them.

Example

The following example configures IGMP proxy for vlan 2. IGMP reports from the managed device would be sent to the upstream router on gigabitethernet port 0/0/3.

```
(host) (conf)# interface vlan 2
   (conf-subif)# ip igmp proxy gigabitethernet 0/0/3
```

Related Commands

Command	Description
interface vlan	Configure interface VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration VLAN Interface Mode (config-submode)

iot transportProfile

```
iot transportProfile <profile>
   clone
   endpointID <id>
   endpointToken <token>
   endpointType {Meridian-Asset-Tracking | Meridian-Beacon-Management | ZF}
   endpointURL <url>
   password <password>
   payloadContent {managed-beacons | managed-tags | zf-tags | all-ble-data}
   transportInterval <interval>
   username <user>
   no…
```

Description

This command configures an IoT transport profile.

Syntax

Parameter	Description	Range	Default
`clone`	Copy data from another IoT data profile.	—	—
`endpointID <id>`	Endpoint ID of the IoT management server.	—	—
`endpointToken <token>`	Endpoint token of the IoT management server.	—	—
`endpointType`	Endpoint type of the IoT management server.	—	—
`Meridian-Asset-Tracking`	Stream data to meridian WebSocket server.	—	—
`Virgin-Cruises`	Virgin cruises at the backend of the premise beacons.	—	—
`ZF`	ZF deTagtive server.	—	—
`endpointURL <url>`	Endpoint URL of the IoT management server.	—	—
`password <password>`	Endpoint password.	—	—
`payloadContent`	Content of the messages sent to the IoT management server.	—	—
`managed-beacons`	Beacon management data.	—	—
`managed-tags`	Asset tag RSSI data	—	—
`zf-tags`	ZF tag data.	—	—
`all-ble-data`	All the BLE device data.	—	—

Parameter	Description	Range	Default
`transportInterval <interval>`	Instant AP IoT data interval in seconds.	5 to 3600 seconds	—
`username <user>`	Endpoint user name.	—	—
`no...`	Removes any existing configuration.	—	—

Usage Guidelines

Use this command to create or modify an IoT transport profile. An IoT transport profile is a global profile that is used to transport BLE information to an endpoint server.

Example

The following example configures the IoT transport profile.

```
(host) [mynode] (config)# iot transportProfile sample
(host) [mynode] (IoT Data Profile "sample")# endpointURL
https://edit.meridianapps.com/api/beacons/manage
(host) [mynode] (IoT Transport Profile "sample")# endpointType Meridian-Beacon-Management
(host) [mynode] (IoT Transport Profile "sample")# payloadContent managed-beacons
(host) [mynode] (IoT Transport Profile "sample")# transportInterval 300
(host) [mynode] (IoT Transport Profile "sample")# endpointToken
MzkxMTZlMWYtYTgzYS00YWUxLTkzYWEtYjQyNzE1MGMyMjAxOjBiZWJjYWViLTRjNjItNGEwNC1hMGIyLWYzZTM5ZDFlNGVkNg==
```

Related Commands

Command	Description
iot usetransportProfile	Sets an IoT management server profile.
show iot transportProfile	Shows the IoT profile status.

Command History

Version	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration IoT Data Profile Mode (config-submode)

iot usetransportProfile

```
iot usetransportProfile <iot-profile-name>
```

Description

This command sets an IoT management server profile. You can set up to four management server profiles.

Example

Execute the following command to set an IoT transport profile:

```
(host) [mynode] (config)# iot usetransportProfile sample
```

Related Commands

Command	Description
iot transportProfile	Configures an IoT transport profile.
show iot transportProfile	Shows the IoT profile status.

Command History

Version	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

ip access-list eth

```
ip access-list eth <accname>
   deny {<ethtype> [<bits>]|any} [mirror] [position <prio>]
   no ...
   permit {<ethtype> [<bits>]|any} [mirror][position <prio>]
```

Description

This command configures an Ethertype ACL.

Syntax

Parameter	Description	Range
`<accname>`	Define an access list, where <accname> is a name, or a number in the specified range.	200-299
`deny`	Reject the specified packets, which can be one of the following: ■ Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535) ■ any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination, or set the position of the ACL. The default position is last, a position of 1 puts the ACL at the top of the list.	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets, which can be one of the following: ■ Ethertype in decimal or hexadecimal (0-65535) and optional wildcard (0-65535) ■ any: match any Ethertype Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination, or set the position of the ACL. The default position is last, a position of 1 puts the ACL at the top of the list.	—

Usage Guidelines

The Ethertype field in an Ethernet frame indicates the protocol being transported in the frame. This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. This ACL can be used to permit IP frames while blocking other non-IP protocols such as IPX or Appletalk.

If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see firewall on page 459.

Example

The following command configures an Ethertype ACL:

```
(host) [mynode] (config) #ip access-list eth 200
(host) [mynode] (config-submode)#permit any mirror position 3
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master

ip access-list extended

```
ip access-list extended <accname>
   deny <protocol> <source> <dest>
   ipv6 <protocol> <source> <dest>
   no ...
   permit <protocol> <source> <dest>
```

Description

This command configures an extended ACL. To configure IPv6 specific rules, use the **ipv6** keyword for each rule.

Syntax

Parameter	Description	Range
`extended <accname>`	Define an access list, where <accname> is a name, or a number in the specified range.	100-199, 2000-2699
`deny`	Reject the specified packets.	—
`<protocol>`	Protocol, which can be one of the following: ■ **any**: any protocol ■ **icmp**: Internet Control Message Protocol ■ **igmp**: Internet Gateway Message Protocol ■ **tcp**: Transmission Control Protocol ■ **udp**: User Datagram Protocol ■ **<0-255>**: An IP protocol number between 0-255	—
`<source>`	Source, which can be one of the following: ■ **any**: any source ■ **host**: specify a single host IP address ■ **A.B.C.D**: IPv4 source address and wildcard	—
`<dest>`	Destination, which can be one of the following: ■ **any**: any destination ■ **host**: specify a single host IP address ■ **A.B.C.D**: IPv4 destination address and wildcard	—
`ipv6 <deny | permit>`	Use the ipv6 keyword to add IPv6 specific rules.	—
`<protocol>`	Protocol, which can be one of the following: ■ **any**: any protocol ■ **icmpv6**: Internet Control Message Protocol ■ **tcp**: Transmission Control Protocol ■ **udp**: User Datagram Protocol ■ **<0-255>**: An IP protocol number between 0-255	—
`<source>`	Source, which can be one of the following: ■ **any**: any source ■ **host**: specify a single host IP address ■ **X:X:X:X::X/<0-128>**: IPv6 source address and wildcard	—

Parameter	Description	Range
`<dest>`	Destination, which can be one of the following: ■ **any**: any destination ■ **host**: specify a single host IP address ■ **X:X:X:X::X/<0-128>**: IPv6 destination address and wildcard	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets.	
`<protocol>`	Protocol, which can be one of the following: ■ **any**: any protocol ■ **icmp**: Internet Control Message Protocol ■ **igmp**: Internet Gateway Message Protocol ■ **tcp**: Transmission Control Protocol ■ **udp**: User Datagram Protocol ■ **<0-255>**: An IP protocol number between 0-255	—
`<source>`	Source, which can be one of the following: ■ **any**: any source ■ **host**: specify a single host IP address ■ **A.B.C.D**: IPv4 source address and wildcard	—
`<dest>`	Destination, which can be one of the following: ■ **any**: any destination ■ **host**: specify a single host IP address ■ **A.B.C.D**: IPv4 destination address and wildcard	—

Usage Guidelines

Extended ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source or destination IP address or IP protocol.

Example

The following command configures an extended ACL:

```
(host) [mynode] (config) #ip access-list extended 100
(host) [mynode] (config-submode) #deny any host 1.1.21.245 any
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforma	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master

ip access-list geolocation

```
ip access-list geolocation <accname>
   deny
   {[<from>|<to> {anonymous_proxy [log|mirror|position]|any [log|mirror|position]}|country
   <STRING>|region <STRING>]}
   no ...
   permit
   {[<from>|<to> {anonymous_proxy [log|mirror|position]|any [log|mirror|position]}|country
   <STRING>|region <STRING>]}
```

Description

This command configures a geolocation ACL.

Syntax

Parameter	Description
`<accname>`	Define an access list, where <accname> is a name, or a number in the specified range.
`deny <from|to>`	Reject the specified packets, which can be one of the following: ■ Packets coming from the source. ■ Packets meant for the destination.
`anonymous_proxy <log|mirror|position>`	Match packets from or to an anonymous proxy. It has the following options: ■ Log if the ACL is applied. ■ Mirror all session packets to datapath or remote destination. ■ Filter position. The position number is in the range of <1-2000>. The default is last, and 1 is first position.
`any <log|mirror|position>`	Match any location. It has the following options: ■ Log if the ACL is applied. ■ Mirror all session packets to datapath or remote destination. ■ Filter position. The position number is in the range of <1-2000>. The default is last, and 1 is first position.
`country <STRING>`	Match packets from or to a country. The <STRING> denotes country name. **NOTE:** Use double quotes to specify country names with spaces in the name.
`region <STRING>`	Match packets from or to a region. The <STRING> denotes region name. **NOTE:** Use double quotes to specify region names with spaces in the name.
`no`	Negates any configured parameter.

Parameter	Description
`permit <from|to>`	Allow the specified packets, which can be one of the following: ■ Packets coming from the source. ■ Packets meant for the destination.
`anonymous_proxy <log|mirror|position>`	Match packets from or to an anonymous proxy. It has the following options: ■ Log if the ACL is applied. ■ Mirror all session packets to datapath or remote destination. ■ Filter position. The position number is in the range of <1-2000>. The default is last, and 1 is first position.
`any <log|mirror|position>`	Match any location. It has the following options: ■ Log if the ACL is applied. ■ Mirror all session packets to datapath or remote destination. ■ Filter position. The position number is in the range of <1-2000>. The default is last, and 1 is first position.
`country <STRING>`	Match packets from or to a country. The <STRING> denotes country name. **NOTE:** Use double quotes to specify country names with spaces in the name.
`region <STRING>`	Match packets from or to a region. The <STRING> denotes region name. **NOTE:** Use double quotes to specify region names with spaces in the name.

Example

The following command configures a geolocation ACL:

```
(host) [mynode] (config) #ip access-list geolocation global-geolocation-acl
(host) [mynode] (config-submode)#permit from any mirror position 3
```

Command History

Version	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master

ip access-list mac

```
ip access-list mac <accname>
   deny {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
   no ...
   permit {<macaddr>[<wildcard>]|any|host <macaddr>} [mirror]
```

Description

This command configures a MAC ACL.

Syntax

Parameter	Description	Range
`mac <accname>`	Configures a MAC access list, where <accname> is a name, or a number in the specified range.	700-799, 1200-1299
`deny`	Reject the specified packets, which can be the following: ■ **any**: any packets ■ **host**: specify a MAC address ■ **A:B:C:D:E:F**: MAC address and optional wildcard Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets, which can be the following: ■ **any**: any packets ■ **host**: specify a MAC address ■ **A:B:C:D:E:F**: MAC address and optional wildcard Optionally, you can configure the mirror parameter, which mirrors packets to a datapath or remote destination.	—

Usage Guidelines

MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses. If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see firewall on page 459.

Example

The following command configures a MAC ACL:

```
(host) [mynode] (config) #ip access-list mac 700
(host) [mynode] (config-submode) #deny 11:11:11:00:00:00
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master

ip access-list route

```
ip access-list route <accname>
   <source> <dest> <service> <action> forward|route {ipsec-map <ipsec-map-name>}|{next-hop-
   list <next-hop-list-name>}|{tunnel <tunnel-id>}|{tunnel-group <tunnelgroupname>} [position
   <position>]
```

Description

This command configures an ACL for PBR.

Syntax

Parameter	Description
`rout <accname>`	Define a route access list, where <accname> is an access list name
`<source>`	The traffic source, which can be one of the following: ■ **alias<name>**: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) ■ **any**: match any traffic ■ **host <ip-addr>**: specify a single host IP address ■ **localip**: specify the local IP address to match traffic ■ **network <ip-addr> <netmask>**: specify the IP address and netmask ■ **no**: negate a command ■ **user**: represents the IP address of the user
`<dest>`	The traffic destination, which can be one of the following: ■ **alias<name>**: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) ■ **any**: match any traffic ■ **host <ip-addr>**: specify a single host IP address ■ **localip**: specify the local IP address to match traffic ■ **network <ip-addr> <netmask>**: specify the IP address and netmask ■ **user**: represents the IP address of the user
`<service>`	Network service to which the ACL is applied. The service can be one of the following: ■ ■ **any**: match any traffic ■ **app<string>**: application name. (For a complete list of supported applications, issue the command **show dpi application all**.) ■ **appcategory <string>**: application category name. (For a complete list of supported applications, issue the command **show dpi application all**.) ■ **icmp**: Internet Control Message Protocol ■ **tcp <0-65535>:** specify the TCP destination port number (0-65535) ■ **tcp source<0-65535>**: TCP source port number ■ **udp <0-65535>:** UDP destination port number (0-65535) ■ **udp source<0-65535>**: UDP source port number ■ **<0-255>**: IP protocol number (0-255) ■ **<string>**: name of a network service (use the show netservice command to see configured services)

Parameter	Description
<action>	Action if rule is applied, which can be one of the following: ■ **forward**: Explicitly define an ACL with a forward action to skip PBR for traffic which would otherwise match another PBR rule. ■ **route ipsec-map <ipsec-map-name>**: Redirected over a VPN tunnel by specifying the ipsec-map name. For more information on IPsec maps, see crypto-local ipsec-map. ■ **route next-hop-list <next-hop-list-name>**: Packets can be routed to a nexthop router on a nexthop list by specifying the nexthop list name. For more information on nexthop lists, see ip nexthop-list. ■ **route tunnel <tunnel-id>**: Packets can be redirected over an L3 GRE tunnel. ■ **route tunnel-group <tunnelgroupname>**: Packets can be redirected over an L3 GRE tunnel group. For more information on tunnel groups, see tunnel-group. ■ **[position <position>]**: (Optional) Specify the position of the forwarding or routing rule. (1 is first, default is last)

Usage Guidelines

PBR is an optional feature that allows packets to be routed based on ACLs configured by the administrator. By default, when a managed device receives a packet for routing, it looks up the destination IP in the routing table and forwards the packet to the nexthop router. If PBR is configured, the nexthop device can be chosen based on a defined ACL.

In a typical deployment scenario with multiple uplinks, the default route only uses one of the uplink next-hops for forwarding packets. If a nexthop becomes unreachable, the packets will not reach their destination. If your deployment uses PBR based on a nexthop list, any of the uplink nexthops could be used for forwarding traffic. This requires a valid ARP entry (Route-cache) in the system for all the PBR nexthops.

Example

The following command configures a routing access list using an IPsec map.

```
(host) [mynode] (config) #ip access-list route pbr1
(host) [mynode] (config-submode) #any any udp 100 route ipsec-map VPN1
```

Related Commands

Command	Description
interface vlan	This command associates a routing ACL with a specific VLAN.
ip nexthop-list	Use this command to define a next-hop list for a routing policy

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master

ip access-list session

```
ip access-list session <accname>
   <source> <dest> <service> <action> [<extended action>]
   ipv6 <source> <dest> <service> <action> [<extended action>]
   no ...
```

Description

This command configures an ACL session. To create IPv6 specific rules, use the **ipv6** keyword.

Syntax

Parameter	Description
`session <accname>`	Define a session ACL, where <accname> is an access list name, or an access list number in the specified range.
`ipv6`	Use the ipv6 keyword to create IPv6 specific rules.
`<source>`	The traffic source, which can be one of the following: ■ **alias**: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) ■ **any**: match any traffic ■ **host**: specify a single host IP address ■ **localip**: specify the local IP address to match traffic ■ **network**: specify the IP address and netmask ■ **user**: represents the IP address of the user ■ **userrole**: represents the traffic based on user role
`<dest>`	The traffic destination, which can be one of the following: ■ **alias**: specify the network resource (use the **netdestination** command to configure aliases; use the **show netdestination** command to see configured aliases) ■ **any**: match any traffic ■ **host**: specify a single host IP address ■ **localip**: specify the local IP address to match traffic ■ **network**: specify the IP address and netmask ■ **user**: represents the IP address of the user ■ **userrole**: represents the traffic based on userrole

Parameter	Description
`<service>`	Network service, which can be one of the following: ■ **IP protocol number** (0-255) ■ **name of a network service** (use the show netservice command to see configured services) ■ **any**: match any traffic ■ **app**: application name. (For a complete list of supported applications, issue the command **show dpi application all**.) ■ **appcategory**: application category name. (For a complete list of supported applications, issue the command **show dpi application all**.) ■ **icmp:** Internet Control Message Protocol ■ **tcp destination port number**: specify the TCP port number (0-65535) ■ **tcp source**: TCP/UDP source port number ■ **udp**: specify the UDP port number (0-65535) ■ web-cc-category: name of an a web content category. For the full list of available web content categories, issue the command **show web-cc categories**. ■ **web-cc-reputation**: any of the predefined web content reputation levels. • high-risk • low-risk • moderate-risk • suspicious • trustworthy

Parameter	Description
<action>	Action if rule is applied, which can be one of the following: **deny**: Reject packets. Applicable to both IPv4 and IPv6. **dst-nat**: Performs destination NAT on packets. Forward packets from source network to destination; re-mark them with destination IP of the target network. This action functions in tunnel/decrypt-tunnel forwarding mode. User should configure the NAT pool in the managed device. **dual-nat**: Performs both source and destination NAT on packets. Source IP and destination IP is changed as per the NAT pool configured. This action functions in tunnel/decrypt-tunnel forwarding mode. User should configure the NAT pool in the managed device. **permit:** Forward packets. Applicable to both IPv4 and IPv6. **redirect**: Specify the location to which packets are redirected. The following are applicable only to IPv4: ■ Datapath destination ID (**0-65535**). ■ **esi-group**: Specify the ESI server group configured with the esi group command. ■ **tunnel**: Specify the ID of the tunnel configured with the interface tunnel command. **webcc-reputation**: Assign one of the predefined web content reputation levels to the packets. The following are applicable only to IPv6: ■ **tunnel**: Specify the ID of the tunnel configured with the interface tunnel command. ■ **tunnel-group**: Specify the tunnel-group configured with the interface tunnel command. **route:** Specify the next hop to which packets are routed, which can be one of the following: ■ **dst-nat:** Destination IP changes to the IP configured from the NAT pool. This action functions in bridge/split-tunnel forwarding mode. User should configure the NAT pool in the managed device. ■ **src-nat:** Source IP changes to the external IP of the Remote AP. This action functions in bridge/split-tunnel forwarding mode and uses implied NAT pool. **src-nat**: Performs source NAT on packets. Source IP changes to the outgoing interface IP address (implied NAT pool) or from the pool configured (manual NAT pool). This action functions in tunnel/decrypt-tunnel forwarding mode.
<extended action>	Optional action if rule is applied, which can be one of the following: ■ **blacklist**: blacklist user if ACL gets applied. ■ **disable-scanning**: pause ARM scanning while traffic is present. Note that you must enable "VoIP Aware Scanning" in the ARM profile for this feature to work. ■ **dot1p-priority**: specify 802.1p priority (0-7), where 0 is the lowest priority, and 7 is the highest. ■ **log**: generate a log message ■ **mirror**: mirror all session packets to datapath or remote destination ■ If you configure the mirror option, define the destination to which mirrored packets are sent in the firewall policy. For more information, see firewall on page 459. ■ **next-hop-list**: Route packet to the next hop in the list. ■ **position**: specify the position of the rule (1 is first, default is last) ■ **queue**: assign flow to priority queue (high/low) ■ **send-deny-response**: if <action> is deny, send an ICMP notification to the source ■ **time-range**: specify time range for this rule (configured with time-range command) ■ **tos**: specify ToS value (0-63)
no	Negates any configured parameter.

Usage Guidelines

Session ACLs define traffic and firewall policies on the managed device. You can configure multiple rules for each policy, with rules evaluated from top (1 is first) to bottom. The first match terminates further evaluation. Generally, you should order more specific rules at the top of the list and place less specific rules at the bottom of the list. The ACL ends with an implicit deny all. To configure IPv6 rules, use the `ipv6` keyword followed by the regular ACL keywords.

Example

The following CLI configuration shows how pre-classification and post-classification occurs during enforcement.

Each application has an implicit set of ports that are used for communication. In phase 1, if an application ACE entry is hit, the traffic matching this application's implicit port is allowed (as governed by the application ACE). The DPI engine can monitor the exchange on these ports and determine the application. Once the application is determined, phase 2 occurs when an evaluation is done to determine the final outcome for the session.

The following CLI configuration example is a user role with both the global and role session ACLs:

```
(host) [mynode] (config) #ip access-list session global-sacl
(host) [mynode] (config) #ip access-list session apprf-employee-sacl
(host) [mynode] (config) #ip access-list session control
   any any app gmail-chat permit
   any any app youtube permit
   any any any deny
```

This example shows a DPI rule along with a L3/L4 rule with forwarding action in the same ACL.

```
(host) [mynode] (config) #ip access-list session AppRules
   any any app Facebook permit tos 45
   any any app YouTube deny
   any any appcategory peer-to-peer deny
   any any tcp 23 permit
   network 40.1.0.0/16 any tcp 80 permit tos 60
   network 20.1.0.0/16 any tcp 80 src-nat
!
(host) [mynode] (config) #ip access-list session NetRules
   network 80.0.0.0/24 any tcp 80 deny
   network 60.0.0.0/24 any tcp 80 dual-nat pool <pool1>
   network 10.0.0.0/24 any tcp 80 dst-nat
!
(host) [mynode] (config) #user-role Role1
   session-acl AppRules
   session-acl NetRules
!
```

The following command configures a session ACL with IPv4 and IPv6 address:

```
(host) [mynode] (config) #ip access-list session common
(host) [mynode] (config-sess-common)#host 10.12.13.14 any any permit
(host) [mynode] (config-sess-common)#ipv6 host 11:12:11:11::2 any any permit
```

The following example displays information for an ACL called mylist:

```
(host) [mynode] (config) #show ip access-list mylist
ip access-list session mylist
mylist
---------
Priority  Source  Destination  Service  Application  Action  TimeRange  Log  Expired  Queue
TOS  8021P  Blacklist  Mirror  DisScan  IPv4/6  Contract
```

```
--------  ------  -----------  -------  -----------  ------  ---------  ---  -------  -----  -
--  -----  ---------  ------  -------  ------  --------
1         any     any                   app gmail    deny                                 Low
                                    4
```

The following example shows how this local-override netdestination alias is used in the controller:

```
(host) [mynode] (config) #ip access-list  session store-override
(host) [mynode] (config-sess-store-override)#any alias store any permit
(host) [mynode] (config-sess-store-override)#alias store any any deny
(host) [mynode] (config-sess-store-override)#!
(host) [mynode] (config) #show ip interface brief
   Interface                   IP Address / IP Netmask        Admin    Protocol
   vlan 1                  172.72.10.254 / 255.255.255.0     up       up
   vlan 55                    55.55.55.1 / 255.255.255.0     up       up
   loopback                   unassigned / unassigned        up       up

(host) [md] #show acl acl-table | include dummy-acl
75   session      620        2           3          dummy-acl                    0

(host) [md] #show acl ace-table acl 75

620: any netdest-id: 34  0  0-0  0-0  f1000080001:permit  alias-dst  hits-table-index 24578
621: netdest-id: 34 any  0  0-0  0-0  f800080001:permit  alias-src  hits-table-index 24579
622: any any  0  0-0  0-0  f180000:deny
```

The following examples display the use of extended scope of address range:

```
(host) [mynode] (config) #ip access-list session v6-logon-control
   ipv6 user any udp 546  deny
   ipv6 any any svc-v6-icmp  permit
   ipv6 any any svc-v6-dhcp  permit
   ipv6 any any svc-dns  permit
   ipv6 any  network fc00::/7 any  permit
   ipv6 any  network fe80::/64 any  permit

(host) [mynode] (config) #ip access-list session validuser
   network 127.0.0.0 255.0.0.0 any any  deny
   network 169.254.0.0 255.255.0.0 any any  deny
   network 224.0.0.0 240.0.0.0 any any  deny
   host 255.255.255.255 any any  deny
   network 240.0.0.0 240.0.0.0 any any  deny
   any any any  permit
   ipv6 host fe80:: any any  deny
   ipv6 network fc00::/7 any any  permit
   ipv6 network fe80::/64 any any  permit
   ipv6 alias ipv6-reserved-range any any  deny
   ipv6 any any any  permit
   !
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master

ip access-list standard

```
ip access-list standard <accname>
   deny {<ipaddr> <wildcard>|any|host <ipaddr>}
   ipv6 <ipaddr>
   no ...
   permit {<ipaddr> <wildcard>|any|host <ipaddr>}
```

Description

This command configures a standard ACL.

Syntax

Parameter	Description	Range
`standard <accname>`	Define an access list, where <accname> is an access list name, or an access list number in the specified range.	1-99, 1300-1399
`deny`	Reject the specified packets, which can be the following: ■ **any**: any source ■ **host**: specify a single host IP address ■ **A.B.C.D**: IPv4 source address and wildcard	—
`ipv6 <deny | permit>`	Reject or allow the specified packets, which can be the following: ■ **any**: any source/destination IPv6 address ■ **host**: specify a single host IPv6 address ■ **X:X:X:X::X/<1-128>**: IPv6 source/destination IPv6 address and wildcard	—
`no`	Negates any configured parameter.	—
`permit`	Allow the specified packets, which can be the following: IP address and optional wildcard any: any packets host: specify a host IP address	—

Usage Guidelines

Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.

Example

The following command configures a standard ACL:

```
(host) [mynode] (config) #ip access-list standard 1
(host) [mynode] (config-submode) #permit host 10.1.1.244
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master

ip cp-redirect-address

```
ip cp-redirect-address {disable | <A.B.C.D>}
```

Description

This command configures a redirect address for captive portal.

Syntax

Parameter	Description
`disable`	Disables automatic DNS resolution for captive portal.
`<A.B.C.D>`	Redirect unauthenticated user to this IP address. This address should be routable from all external networks.

Usage Guidelines

This command redirects wireless clients that are on different VLANs (from the managed device's IP address) to the captive portal on the managed device.

If you have the Next Generation Policy Enforcement Firewall (PEFNG) license installed in the managed device, modify the captive portal session ACL to permit HTTP/S traffic to the destination **cp-redirect-address <A.B.C.D>** instead of **mswitch**. If you do not have the PEFNG license installed in the managed device, the implicit captive-portal-profile ACL is automatically modified when you issue this command.

Example

The following command configures a captive portal redirect address:

```
(host) ^[mynode] (config) #ip cp-redirect-address disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip default-gateway

```
ip default-gateway
   import {cell|cell-cost <cost>|dhcp|dhcp-cost <cost>|pppoe|pppoe-cost <cost>}
   mgmt <nexthop>
   <nexthop> [<cost>]
```

Description

This command configures the default gateway for Mobility Master or the managed device.

Syntax

Parameter	Description
`import`	Use a gateway IP address obtained through the cell interface, DHCP or PPPoE. The default gateway is imported into the routing table and removed when the uplink is no longer active.
`cell`	Use a gateway IP address obtained through the cell interface.
`cell-cost <cost>`	Use the cost for cell interface.
`dhcp`	Use a gateway IP address obtained DHCP.
`dhcp-cost <cost>`	Use the cost for DHCP interface.
`pppoe`	Use a gateway IP address obtained through PPPoE.
`pppoe-cost <cost>`	Use the cost for PPPoE interface
`mgmt <nexthop>`	Set the default gateway IP address as the management interface IP address.
`<nexthop> [<cost>]`	IP address of the default gateway and the distance metric of this route.

Usage Guidelines

You can use this command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect Mobility Master or the managed device. If you define more than one dynamic gateway type, you must also define a cost for the route to each gateway. Mobility Master or the managed device will first attempt to obtain a gateway IP address using the option with the lowest cost. If Mobility Master and the managed device are unable to obtain a gateway IP address, they will then attempt to obtain a gateway IP address using the option with the next-lowest path cost.

Example

The following command configures the default gateway for the Mobility Master:

```
(host) [mynode] (config) #ip default-gateway 10.1.1.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip dhcp adaptive

```
ip dhcp adaptive
```

Description

This command enables adaptive VLAN assignment based on the DHCP server.

Syntax

No parameters.

Example

The following command enables adaptive VLAN assignment based on the DHCP server:

```
(host) [mynode] (config) #ip dhcp adaptive
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip dhcp default-pool

```
ip dhcp default-pool
   private
   public
```

Description

This command configures the DHCP pool type.

Syntax

Parameter	Description
`private`	Configure a private DHCP pool.
`public`	Configure a public DHCP pool.

Example

The following command configures a private DHCP pool:

```
(host) [mynode] (config) #ip dhcp default-pool private
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip dhcp excluded-address

```
ip dhcp excluded-address <low-address> [<high-address>]
```

Description

This command configures an excluded address range for the DHCP server on Mobility Master.

Syntax

Parameter	Description
`<low-address>`	Low range excluded IP addresses. For example, you can enter the IP address of the Mobility Master so that this address is not assigned.
`<high-address>`	High range excluded IP addresses.

Usage Guidelines

Use this command to specifically exclude certain addresses from being assigned by the DHCP server. Ensure that the statically assigned IP addresses are excluded.

Example

The following command configures an excluded address range:

```
(host) [mynode] (config) #ip dhcp excluded-address 192.168.1.1 192.168.1.255
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip dhcp increase-increase-limit

```
ip dhcp increase-increase-limit
```

Description

This command configures additional DHCP scope that is twice the user limit on specific controller platforms.

Syntax

No parameter.

Usage Guidelines

This feature is disabled by default. This command can be used only in any of the following controller platforms: 7005 Controller, 7008 Controller, or 7010 Controller.

Example

To enable the additional DHCP scope on a controller, execute the following command:

```
(host) (config) #ip dhcp increase-increase-limit
```

Related Commands

Command	Description
show ip dhcp	Shows the DHCP pool statistics.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platform	License	Command Mode
7005 Controller, 7008 Controller, and 7010 Controller platforms	Base operating system	Config mode on the Managed Device or controller

ip dhcp load-balance

```
ip dhcp load-balance priority
   round-robin {ipupsell | private | public}
   strict {ipupsell | private | public}
```

Description

This command configures the DHCP pool load balancing priority.

Syntax

Parameter	Description
`round-robin`	Enable a round-robin priority.
`ipupsell`	Configure the DHCP pool as an IP upsell pool.
`private`	Configure the DHCP pool as private.
`public`	Configure the DHCP pool as public.
`strict`	Enable a strict priority.
`ipupsell`	Configure the DHCP pool as an IP upsell pool.
`private`	Configure the DHCP pool as private.
`public`	Configure the DHCP pool as public.

Example

The following command DHCP pool load balancing priority:

```
(host) [mynode] (config) #ip dhcp load-balance priority round-robin private
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip dhcp ping-check

```
ip dhcp ping-check
   disable
```

Description

This command disables the ping-check option on the DHCP server of the Mobility Master.

Syntax

Parameter	Description
`disable`	Disables the ping-check option on the DHCP server of the Mobility Master.

Example

The following example disables the ping-check option on the DHCP server of the Mobility Master:

```
(host) [mynode] (config) #ip dhcp ping-check disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip dhcp pool

```
ip dhcp pool <name>
   default-router <address> [<address2> <address3> <address4> <address5> <address6> <address7>
   <address8>]
   distributed range <startip> <endip> <hosts>
   dns-server {import | <address> [<address2> <address3> <address4> <address5> <address6>
   <address7> <address8>]}
   domain-name <domain>
   lease <days> <hours> <minutes> <seconds>
   netbios-name-server {import | <address> [<address2> <address3> <address4> <address5>
   <address6> <address7> <address8>]}
   network <network-number> {</prefix(1-30)>|<mask>}
   no ...
   option <code> {hex <hex string> | ip <ipaddr> | text <option-string>}
   pooltype {ipupsell | private | public}
   vendor-class-identifier
```

Description

This command configures a DHCP pool on the Mobility Master.

Syntax

Parameter	Description
`default-router <address>`	IP address of the default router for the DHCP client. The client should be on the same subnetwork as the default router. You can specify up to 8 IP addresses.
`distributed range`	IP address range for the distributed pool.
`<startip>`	Starting IP address of the address pool.
`<endip>`	Ending IP address of the address pool.
`<hosts>`	Number of clients.
`dns-server`	Configure DHCP DNS server.
`import`	Use the DNS server address obtained through DHCP or PPPoE.
`<address>`	IP address of the DHCP DNS server. You can specify up to 8 IP addresses.
`domain-name <domain>`	Domain name to which the client belongs.
`lease`	The amount of time that the assigned IP address is valid for the client. Specify the lease in <days> <hours> <minutes> <seconds>.
`netbios-name-server`	IP address of the NetBIOS Windows Internet Naming Service (WINS) server, which can be one of the following:
`import`	Use the NetBIOS name server address obtained through PPPoE or DHCP.
`<address>`	IP address of the WINS server. You can specify up to 8 IP addresses.

Parameter	Description
network	Range of addresses that the DHCP server may assign to clients, in the form of <ipaddr> and <netmask> or <ipaddr> and <prefix>.
</prefix(1-30)>	Network prefix.
<mask>	Network mask.
no	Negates any configured parameter.
option	Client-specific option code and IP address. See RFC 2132, "DHCP Options and BOOTP Vendor Extensions".
hex <hex string>	Specify the Hex string. Maximum hex characters allowed is 22.
ip <ipaddr>	Specify IP address.
text <option-string>	Specify optional string.
pooltype	Configure the DHCP Pool types.
ipupsell	Configure the DHCP pool as an IP upsell pool.
private	Configure the DHCP pool as private.
public	Configure the DHCP pool as public.
vendor-class-identifier	Send or suppress the Aruba AP vendor ID to clients.

Usage Guidelines

A DHCP pool should be created for each IP subnetwork for which DHCP services should be provided. DHCP pools are not specifically tied to VLANs, as the DHCP server exists on every VLAN. When Mobility Master receives a DHCP request from a client, it examines the origin of the request to determine if it should respond. If the IP address of the VLAN matches a configured DHCP pool, Mobility Master answers the request.

Example

The following command configures a DHCP pool:

```
(host) [mynode] (config) #ip dhcp pool floor1
(host) [mynode] (config-submode) #default-router 10.26.1.1
(host) [mynode] (config-submode) #dns-server 192.168.1.10
(host) [mynode] (config-submode) #domain-name floor1.test.com
(host) [mynode] (config-submode) #lease 0 8 0
(host) [mynode] (config-submode) #network 10.26.1.0 255.255.255.0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

ip domain lookup

```
ip domain lookup
```

Description

This command enables Domain Name System (DNS) hostname to address translation.

Syntax

No parameters.

Usage Guidelines

This command is enabled by default. Use the **no** form of this command to disable.

Example

The following command enables DNS hostname translation:

```
(host) [mynode] (config) #ip domain lookup
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip domain-name

```
ip domain-name <name>
```

Description

This command configures the default domain name.

Syntax

Parameter	Description
`<name>`	Name used to complete unqualified host names. Do not specify the leading dot (.).

Usage Guidelines

Mobility Master uses the default domain name to complete hostnames that do not contain domain names. You must have at least one domain name server configured on the controller (see ip name-server on page 626).

Example

The following command configures the default domain name:

```
(host) [mynode] (config) #ip domain-name yourdomain.com
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip igmp

```
ip igmp
   last-member-query-count <val>
   last-member-query-interval <last-member-query-interval>
   max-members-per-group <val>
   no
   query-interval <query-interval>
   query-response-interval <query-response-interval>
   quick-client-convergence
   robustness-variable <robustness-variable>
   ssm-range <startip> <maskip>
   startup-query-count <startup-query-count>
   startup-query-interval <startup-query-interval>
   version-1-router-present-timeout <version-1-router-present-timeout>
   version-2-router-present-timeout <version-2-router-present-timeout>
```

Description

This command configures the Internet Group Management Protocol (IGMP) timers and counters.

Syntax

Parameter	Description	Range	Default
`last-member-query-count`	Number of group-specific queries that Mobility Master sends before assuming that there are no local group members.	1-65535	2
`last-member-query-interval`	Maximum time, in seconds, that can elapse between group-specific query messages.	1-65535	10
`max-members-per-group`	Configure maximum members per group.	1-65535	300
`query-interval`	Interval, in seconds, at which the Mobility Master sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information.	1-65535	125
`query-response-interval`	Maximum time, in 1/10th seconds, that can elapse between when the Mobility Master sends a host-query message and when it receives a response. This must be less than the query-interval.	1-65535	100
`quick-client-convergence`	Trigger IGMP reports from client during roaming.	—	—
`robustness-variable`	Increase this value to allow for expected packet loss on a subnetwork.	2-10	2
`ssm-range`	Configure the start IP address and mask IP address for source-specific multicast range.	—	—

Parameter	Description	Range	Default
`startup-query-count`	Number of queries that the Mobility Master sends out at start up, separated by **startup-query-interval**.	1-65535	2
`startup-query-interval`	Interval, in seconds, at which the Mobility Master sends general queries on start up.	1-65535	31
`version-1-router-present-timeout`	Timeout, in seconds, if a version 1 IGMP router is detected.	1-65535	400
`version-2-router-present-timeout`	Timeout, in seconds, if a version 2 IGMP router is detected.	1-65535	400

Usage Guidelines

IGMP establishes and manages IP multicast group membership. See RFC 3376, “Internet Group Management Protocol, version 3” for more information.

Example

The following command configures IGMP:

```
(host) [mynode] (config) #ip igmp
(host) ^[mynode] (config-submode)#query-interval 130
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip local

```
ip local pool <pool_name> <pool_start_address> [<pool_end_address>]
```

Description

This command configures a local IP pool for Layer-2 Tunnel Protocol (L2TP).

Syntax

Parameter	Description
`pool <pool_name>`	Name for the address pool.
`<pool_start_address>`	Starting IP address for the pool.
`<pool_end_address>`	(Optional) Ending IP address for the pool.

Usage Guidelines

VPN clients can be assigned IP addresses from the L2TP pool.

Example

The following command configures an L2TP pool:

```
(host) [mynode] (config) #ip local pool pool-l2tp 10.1.1.1 10.1.1.99
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip mobile active-domain

```
ip mobile active-domain <name>
```

Description

This command configures the mobility domain that is active on Mobility Master.

Syntax

Parameter	Description
`<name>`	Name of the mobility domain.

Usage Guidelines

All managed devices are initially part of the “default” mobility domain. If you use the “default” mobility domain, you do not need to specify this domain as the active domain on Mobility Master. However, once you assign a managed device to a user-defined domain, the “default” mobility domain is no longer an active domain on the Mobility Master.

Example

The following command assigns Mobility Master to a user-defined mobility domain:

```
(host) [mynode] (config) #ip mobile active-domain campus1
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip mobile domain

```
ip mobile domain <name>
   anchor <subnet> <netmask> <1-4094> <controller-ip> description <dscr>
   description <descr>
   hat <home-agent> [description <dscr>]
   no
```

Description

This command configures the mobility domain on the managed devices.

Syntax

Parameter	Description
`<name>`	Name of the mobility domain.
`anchor`	Configures the anchor managed device. The **no ip mobile proxy auth-sta-roam-only** command has to be configured for this to work. Supported only for IPv4 clients
`<subnet>`	VLAN subnet IP of the anchored managed device.
`<netmask>`	Subnet mask of the anchored managed device.
`<1-4094>`	VLAN ID of the anchored managed device.
`<controller-ip>`	The IP address of the anchored managed device.
`description`	Description of the anchored managed device.
`description`	Description of the mobility domain. The description can be a maximum of 30 characters (including spaces).
`hat`	Configures a home agent table (HAT) entry.
`<home-agent>`	The IP address of the home agent managed device that requires mobility service.
`description`	Description of the HAT entry. The description can be a maximum of 30 characters (including spaces).
`no`	Negates any configured parameter.

Usage Guidelines

You configure the HAT on Mobility Master; the mobility domain information is pushed to all managed devices that are managed by the same Mobility Master.

HAT entries map subnetworks or VLANs and the home agents. The home agent is typically the managed device's IP address. The home agent's IP address must be routable; that is, all managed devices that belong to the same mobility domain must be able to reach the home agent's IP address.

The maximum number of mobility datapath tunnels supported is 32. A maximum of 32 hat entries can be configured if the hat entries are not VRRP IP addresses. If VRRP IP addresses are configured in the HAT table

the maximum number of HAT entries supported is less than 32 as for each VRRP entry in HAT more than two datapath tunnels are considered.

The managed device looks up information in the HAT to obtain the IP address of the home agent for a mobile client. Because there can be multiple home agents on a subnetwork, the HAT can contain more than one entry for the same subnetwork.

Example

The following command configures HAT entries:

```
(host) [mynode] (config) #ip mobile domain east_building
(host) ^[mynode] (config-submode)#hat 192.0.2.1 description "East building entries"
(host) ^[mynode] (config-submode)#show ip mobile domain east_building

Mobility Domains:, 1 domain(s)
------------------------------
Domain name east_building

Home Agent Table
Home Agent      Description
--------------- -------------------------
192.0.2.1       East building entries
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip mobile foreign-agent

```
ip mobile foreign-agent
   lifetime <40-65534>
   max-visitors <0-5000>
   registrations {interval <100-10000> | retransmits <0-5>}
```

Description

This command configures the foreign agent for IP mobility.

Syntax

Parameter	Description	Range	Default
`lifetime`	Requested lifetime, in seconds, as per RFC 3344, “IP Mobility Support for IPv4”.	40-65534	40
`max-visitors`	Maximum number of active visitors.	0-5000	5000
`registrations`	Frequency at which re-registration messages are sent to the home agent:		
`interval`	Retransmission interval, in milliseconds	100-10000	1000
`retransmits`	Maximum number of times the foreign agent attempts mobile IP registration message exchanges before giving up.	0-5	3

Usage Guidelines

A foreign agent is the managed device which handles all mobile IP communication with a home agent on behalf of a roaming client.

Example

The following command configures the foreign agent:

```
(host) [mynode] (config) #ip mobile foreign-agent registration interval 10000
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip mobile home-agent

```
ip mobile home-agent
   max-bindings <0-5000>
   replay <0-300>
```

Description

This command configures the home agent for IP mobility.

Syntax

Parameter	Description	Range	Default
`max-bindings`	Maximum number of mobile IP bindings. This option is an additional limitation to control the maximum number of roaming users. When the limit is reached, registration requests from the foreign agent fail which causes a mobile client to set a new session on the visited managed device, which will become its home managed device.	0-5000	5000
`replay`	Time difference, in seconds, for time stamp-based replay protection, as described by RFC 3344, “IP Mobility Support for IPv4”. 0 disables replay.	0-300	7

Usage Guidelines

A home agent for a mobile client is the managed device where the client first appears when it joins the mobility domain. The home agent is the single point of contact for the client when it roams.

Example

The following command configures the home agent:

```
(host) [mynode] (config) #ip mobile home-agent replay 100
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip mobile packet-trace

```
ip mobile packet-trace <A:B:C:D:E:F>
```

Description

This command enables packet tracing for the given mac address.

Use this command with caution. It replaces the existing users with user entries from the imported file.

Syntax

Platform	License
<A:B:C:D:E:F>	The MAC address of the host

Usage Guidelines

Executing this command enables packet tracing for the given mac address. This is used for troubleshooting purposes only.

Example

The following command enables packet tracing for the host:

```
(host) [mynode] (config) #ip mobile packet-trace 00:40:96:a6:a1:a4
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ip mobile proxy

```
ip mobile proxy
   auth-sta-roam-only
   block-dhcp-release
   event-threshold <1-100>
   log-trail
   no-service-timeout <30-300>
   on-association
   refresh-stale-ip
   stale-timeout <30-3600>
   stand-alone-AP
   trail-length <1-30>
   trail-timeout <120-3600>
```

Description

This command configures the proxy mobile IP module in a mobility-enabled managed device.

Syntax

Parameter	Description	Range	Default
`auth-sta-roam-only`	Allows a client to roam only if has been authenticated. If a client has not been authenticated, no mobility service is offered if it roams to a different VLAN or managed device.	—	enabled
`block-dhcp-release`	Filters out DHCP release from stations.	—	—
`event-threshold`	Maximum number of mobility events (events that can trigger mobility) handled per second. Mobility events above this threshold are ignored. This helps to control frequent mobility state changes when the client bounces back and forth on APs before settling down.	1-100	25
`log-trail`	Enables logging at the notification level for mobile client moves.	—	enabled
`no-service-timeout`	Time, in seconds, after which mobility service expires. If nothing has changed from the previous state, the client is given another bridge entry but it will have limited connectivity.	30-300	180
`on-association`	Enabling this option triggers mobility on station association. Mobility move detection is performed when the client associates with the managed device and not when the client sends packets. Mobility on association can speed up roaming and improve connectivity for devices that can trigger mobility if they do not send many uplink packets. Downside is security; an association is all it takes to trigger mobility. This option is applicable only if layer-2 security is enforced. It is recommended to retain the default settings as this option causes more load in the system due to exchange of extra messages between managed device in the mobility domain.	—	disabled

Parameter	Description	Range	Default
`refresh-stale-ip`	Mobility forces station to renew its stale IP (assuming its DHCP) by deauthorizing the station.		
`stale-timeout`	Number of seconds the mobility state is retained after the loss of connectivity. This allows authentication state and mobility information to be preserved on the home agent managed device. The default is 60 seconds but can be safely increased. Note that in many case a station state is deleted without waiting for the stale timeout; user delete from management, foreign agent to foreign agent hand-off, etc. (This is different from the no-service-timeout; no-service-timeout occurs up front while the stale-timeout begins when mobility service is provided but the connection is disrupted for some reason.)	30-3600	60
`stand-alone-AP`	Enables support for third party or stand-alone APs. When this is enabled, broadcast packets are not used to trigger mobility and packets from untrusted interfaces are accepted. If mobility is enabled, you must also enable stand-alone AP for the client to connect to the managed device's untrusted port. If the managed device learns wired users via the following methods, enable stand-alone AP: ■ Third party AP connected to the managed device through the untrusted port. ■ Clients connected to ENET1 on APs with two ethernet ports. ■ Wired user connected directly to the managed device's untrusted port. **NOTE:** When IP mobility is enabled, you must also enable the stand-alone AP Support option so that a Multiplexer (MUX) server can perform properly and display all wired users who are connected to a MUX port.	—	disabled
`trail-length`	Specifies the maximum number of entries (client moves) stored in the user mobility trail.	1-30	30
`trail-timeout`	Specifies the maximum interval, in seconds, an inactive mobility trail is held.	120-3600	600

Usage Guidelines

The *proxy mobile IP module* in a mobility-enabled managed device detects when a mobile client has moved to a foreign network and determines the home agent for a roaming client. The proxy mobile IP module performs the following functions:

- Derives the address of the home agent for a mobile client from the HAT using the mobile client's IP address. If there is more than one possible home agent for a mobile client in the HAT, the proxy mobile IP module uses a discovery mechanism to find the current home agent for the client.
- Detects when a mobile client has moved. Client moves are detected based on ingress port and VLAN changes and mobility is triggered accordingly. For faster roaming convergence between AP(s) on the same managed device, it is recommended that you keep the **on-association** option enabled. This helps trigger mobility as soon as 802.11 association packets are received from the mobile client.

Example

The following command triggers mobility on station association:

```
(host) [mynode] (config) #ip mobile proxy on-association
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip mobile revocation

```
ip mobile revocation
   interval <100-10000>
   retransmits <0-5>
```

Description

This command configures the frequency at which registration revocation messages are sent.

Syntax

Parameter	Description	Range	Default
`interval`	Retransmission interval, in milliseconds.	100-10000	1000
`retransmits`	Maximum number of times the home agent or foreign agent attempts mobile IP registration or revocation message exchanges before giving up.	0-5	3

Usage Guidelines

A home agent or foreign agent can send a registration revocation message, which revokes registration service for the mobile client. For example, when a mobile client roams from one foreign agent to another, the home agent can send a registration revocation message to the first foreign agent so that the foreign agent can free any resources held for the client.

Example

The following command configures registration revocation messages:

```
(host) [mynode] (config) #ip mobile revocation interval 2000
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip name-server

```
ip name-server <A.B.C.D>
```

Description

This command configures servers for name and address resolution.

Syntax

Parameter	Description
`<A.B.C.D>`	IP address of the server.

Usage Guidelines

You can configure up to six servers using separate commands. Specify one or more servers when you configure a default domain name (see ip domain-name on page 612).

Example

The following command configures a name server:

```
(host) [mynode] (config) #ip name-server 10.1.1.245
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip nat

```
ip nat pool <name> <start-ipaddr> <end-ipaddr> [<dest-ipaddr> <static>]
```

Description

This command configures a pool of IP addresses for network address translation (NAT).

Syntax

Parameter	Description
`<name>`	Name of the NAT pool.
`<start-ipaddr>`	IP address that defines the beginning of the range of source NAT addresses in the pool.
`<end-ipaddr>`	IP address that defines the end of the range of source NAT addresses in the pool.
`<dest-ipaddr>`	Destination NAT IP address.
`<static>`	Map the NAT pool on a one-to-one basis.

Usage Guidelines

This command configures a NAT pool which you can reference in a session ACL rule (see ip access-list session on page 592).

Example

The following command configures a NAT pool:

```
(host) [mynode] (config) #ip nat pool 2net 2.1.1.1 2.1.1.125
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Next Generation Policy Enforcement Firewall (PEFNG) license	Config mode on Mobility Master

ip nexthop-list

```
ip nexthop-list <STRING>
   ip {dhcp vlan <id> [priority <number>]|<A.B.C.D> [priority <number>]}
   ipsec-map <map_name> [priority <number>]
   no
   preemptive-failover
```

Description

Define a next hop list for policy-based routing.

Syntax

Parameter	Description
`<STRING>`	Name of the next hop list.
`ip`	Next hop IP address.
`dhcp vlan <id>`	VLAN ID of the VLAN used by the next hop device. If the VLAN gets an IP address using DHCP, and the default gateway is determined by the VLAN interface, the gateway IP is used as the next hop IP address.
`<A.B.D.C>`	IP address of the next hop device.
`ipsec-map <map_name>`	Packets can be redirected over a VPN tunnel by specifying the IPsec map name.
`preemptive-failover`	Enable or disable preemptive failover. If preemption is enabled and a higher priority next hop becomes reachable again, packets are again forwarded to the higher priority next hop.

Usage Guidelines

A next hop IP is the IP address of a adjacent router or device with layer-2 connectivity to the managed device. If the managed device uses policy-based routing to forwards packets to a next hop device and that device becomes unreachable, the packets matching the policy will not reach their destination. The next hop list provides redundancy for the next hop devices by forwarding the traffic to a backup next hop device in case of failures. If active next hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next hop on the list.

A maximum of 4 next hops can be added to a next hop list. Each next hop can be assigned a priority, which decides the order of selection of the next hop. If a higher priority next hop goes down, the next higher priority next hop which is active is chosen for forwarding. If all the next hops are configured with same priority, the order is determined based on the order in which they are configured. If all the next hops are down, traffic is passed regular destination based forwarding.

In a typical deployment scenario with multiple up-links, the default route only uses one of the uplink next-hops for forwarding packets. If a next hop becomes unreachable, the packets will not reach their destination. If your deployment uses policy-based routing based on a next hop list, any of the uplink next hops could be used for forwarding traffic. This requires a valid ARP entry (route-cache) in the system for all the policy-based routing next hops.

In a branch office managed device deployment, the site up-links can obtain their IP addresses and default gateway using DHCP. In such deployments, the next hop-list configuration can use the VLAN IDs of uplink VLANs. If the VLAN gets an IP address using DHCP, and the default gateway is determined by the VLAN

interface, the gateway IP is used as the next hop IP address. Branch deployments may also require policy-based redirection of traffic to different VPN tunnels. The next hop list allows you to select an IPsec map to redirect traffic through IPsec tunnels.

Example

The following command configures a list of next hops:

```
(host) [mynode] (config) #ip nexthop-list list1
(host) ^[mynode] (config-submode)#ip 10.1.1.41 priority 1
(host) ^[mynode] (config-submode)#ip 172.21.18.170 priority 2
(host) ^[mynode] (config-submode)#ip 192.18.140.20 priority 3
```

Related Commands

Command	Description
show ip nexthop-list	Display next hop list settings for policy-based routing.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

interface vlan ip ospf

```
interface vlan <vlan>
   ip ospf
      area
      authentication message-digest
      cost <cost>
      dead-interval <seconds>
      hello-interval <seconds>
      message-digest-key <keyid> <passwd>
      priority <number>
      retransmit-interval <seconds>
      transmit-delay <seconds>
```

Description

Configure OSPF on the VLAN interface.

Syntax

Parameter	Description	Range	Default
`area`	Enable OSPF on a specific interface by entering the IP address of the router that will use OSPF.	—	—
`authentication message-digest`	Set the OSPF authentication mode to message digest.	—	disabled
`cost <cost>`	Set the cost associated with the OSPF traffic on an interface.	1 to 65535	1
`dead-interval <seconds>`	Set the elapse interval (seconds) since the last hello-packet was received from the router. After the interval elapses, the neighboring routers declare the router dead.	1 to 65535 seconds	40
`hello-interval <seconds>`	Set the elapse interval (seconds) between hello packets sent on the interface.	1 to 65535 seconds	10
`message-digest-key <keyid> <passwd>`	Enable OSPF MD5 authentication and set the key identification and a character string password.	<keyid> = 1 to 256	No default
`priority <number>`	Set the priority number of the interface to determine the designated router.	0 to 255	0

Parameter	Description	Range	Default
`retransmit-interval <seconds>`	Set the retransmission time between link state advertisements for adjacencies belonging to the interface. Set the time interval long enough to prevent unnecessary retransmissions.	1 to 65535 seconds	5
`transmit-delay <seconds>`	Set the elapse time before retransmitting link state update packets on the interface.	1 to 65535 seconds	1

Usage Guidelines

When configuring OSPF over multiple vendors, use this command to ensure that all routers use the same cost. Otherwise, OSPF may route improperly.

Related Commands

Command	Description
interface vlan	Configure interface VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Parameter introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration VLAN Interface Mode (config-submode)

ip probe default

```
ip probe default
   burst-size <size>
   frequency <seconds>
   mode ping
   no
   retries <count>
```

Description

This command configures IP probes for the policy-based routing using a next-hop list.

Syntax

Parameter	Description	Range	Default
`burst-size <size>`	Number of probes to be sent during the probe frequency interval defined by the **frequency** parameter of this profile.	1-16	5
`frequency <seconds>`	Probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the **burst-size** parameter during each frequency interval defined by this **frequency** parameter.	10-3600	10
`mode ping`	Enable this feature by issuing the **mode ping** command. Ping is the only mode currently supported by this feature.	—	—
`no`	Remove or negate any configured parameter.	—	—
`retries <count>`	Number of times the managed device attempts to resend a probe.	1-255	3

Usage Guidelines

The health-check feature uses ping-probes to check reachability and latency from the managed device to data center though each of the managed device's WAN up-links. Latency is calculated based on the round-trip time (RTT) of ping responses. Ping settings are configured globally using the **ip probe default** command.

Examples

The following commands enable this feature, and reduce the default probe frequency interval and probe burst size:

```
(host) [mynode] (config) #ip probe default
(host) ^[mynode] (config-submode)#burst-size 3
(host) ^[mynode] (config-submode)#frequency 5
(host) ^[mynode] (config-submode)#mode ping
```

Related Commands

Command	Description
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device up-links.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip probe health-check

```
ip probe health-check
   burst-size <size>
   frequency <frequency>
   mode {ping|udp}
   jitter
   no
   retries <count>
```

Description

This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device up-links.

Syntax

Parameter	Description	Range	Default
`burst-size <size>`	Number of probes to be sent during the probe frequency interval defined by the **frequency** parameter of this profile.	1-16	5
`frequency <seconds>`	Probe interval, in seconds. The WAN health-check feature sends the number of probes defined by the **burst-size** parameter during each frequency interval defined by this **frequency** parameter.	10-3600	10
`jitter`	Jitter is a variation in the delay of received packets, which can be worsened by network congestion, improper queuing and configuration errors. The WAN health-check feature measures jitter on the connection to the remote host by sending and measuring packets at fixed intervals. Jitter measurements are only available if the health-check feature is set to send UDP packets.	—	—
`mode {ping|udp}`	Enable this feature by issuing the mode command and choosing the type of probe packets to be sent, **ping** or **udp**.	—	—
`no`	Remove or negate any configured parameter.	—	—
`retries <count>`	Number of times the managed device attempts to resend a probe.	1-255	3

Usage Guidelines

The health-check feature uses ping-probes to check reachability and latency from the managed device to data center though each of the managed device's WAN up-links. Latency is calculated based on the delay of ping responses.

Examples

The following commands enable this feature, and reduce the default probe frequency interval and probe burst size.

```
(host) [mynode] (config) #ip probe health-check
(host) ^[mynode] (config-submode)#burst-size 3
(host) ^[mynode] (config-submode)#frequency 5
(host) ^[mynode] (config-submode)#mode udp
(host) ^[mynode] (config-submode)#jitter
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip radius

```
ip radius
   nas-ip {nas-vlan <nasvlan>|<A.B.C.D>}
   rfc-3576-server udp-port <0-65535>
   source-interface {loopback|vlan <1-4094>}
```

Description

This command configures global parameters for RADIUS servers.

Syntax

Parameter	Description	Range	Default
`nas-ip`	A global Network Access Server (NAS) IP address to send in RADIUS packets. This configuration supersedes the server-specific NAS IP configured with the **aaa authentication-server radius** command.	—	—
`nas-vlan`	Configure the NAS VLAN to be used as the NAS IP address.	—	—
`A.B.C.D`	Configure the NAS IP address.	—	—
`rfc-3576-server udp-port <0-65535>`	Configures the UDP port to receive requests from a RADIUS server that can send user disconnect and change-of-authorization messages, as described in RFC 3576, “Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS)”. See the **aaa rfc-3576-server** command to configure the server.	0-65535	3799
`source-interface`	Interface for all outgoing RADIUS packets. The IP address of the specified interface is included in the IP header of RADIUS packets. The interface can be one of the following:	—	—
`loopback`	Use the IP address of the loopback interface.	—	—
`vlan`	Use the IP address of the VLAN.	1-4094	—

Usage Guidelines

This command configures global RADIUS server parameters. If the **aaa authentication-server radius** command configures a server-specific NAS IP, the server-specific IP address is used instead.

Example

The following command configures a global NAS IP address sent in RADIUS packets:

```
(host) [mynode] (config) #ip radius nas-ip 192.168.1.245
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	The **ip radius rfc-3576-server udp-port** command requires the PEFNG license. Other commands are available in the base operating system.	Config mode on Mobility Master

ip route

```
ip route <destip> <destmask> {ipsec <name> [<cost>]|null <0-0>|<nexthop> [<cost>]}
```

Description

This command configures a static route on Mobility Master or the managed device.

Syntax

Parameter	Description
`<destip>`	Enter the destination IP address prefix in dotted decimal format (A.B.C.D).
`<destmask>`	Enter the destination netmask in dotted decimal format (A.B.C.D).
`ipsec <name>`	Enter the IPsec map name to use a static IPsec route map.
`null <0-0>`	Enter the key word **null 0** to designate a null interface.
`<nexthop> [<cost>]`	Enter the forwarding router address in dotted decimal format (A.B.C.D). Optionally, enter the distance metric (cost) for this route. The cost prioritizes routing to the destination. The lower the cost, the higher the priority.

Usage Guidelines

This command configures a static route on Mobility Master or the managed device other than the default gateway. Use the **ip default-gateway** command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect Mobility Master or the managed device.

Example

The following command configures a static route:

```
(host) [mynode] (config) #ip route 172.16.0.0 255.255.0.0 10.1.1.1
```

Related Commands

Command	Description
ip nexthop-list	Configure next hop list settings for policy-based routing.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base Operating System	Config mode on Mobility Master

ip tunnel

```
ip tunnel pool <pool-name>
   distributed range <startip> <endip>
   no
```

Description

This command configures the DHCP address pool for remote IP address distribution. This command should be configured from the **/md** node hierarchy.

Syntax

Parameter	Description
`distributed range <startip> <endip>`	Configures the DHCP address pool for remote IP address distribution.
`no`	Remove or negate any configured parameter.

Example

The following command configures the DHCP address pool for remote IP address distribution:

```
(host) [md] (config) #ip tunnel pool corp-tunnel-remote
(host) ^[md] (config-submode)#distributed range 10.0.0.1 10.0.0.100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip vlan

```
ip vlan pool <pool-name>
   distributed range <startip> <endip>
   no
```

Description

This command configures the VLAN address pool for remote IP address distribution. This command should be configured from the **/md** node hierarchy.

Syntax

Parameter	Description	Range	Default
`distributed range <startip> <endip>`	Configures the VLAN address pool for remote IP address distribution.	—	—
`no`	Remove or negate any configured parameter.	—	—

Example

The following command configures the VLAN address pool for remote IP address distribution:

```
(host) [md] (config) #ip VLAN pool corp-vlan-remote
(host) ^[md] (config-submode)#distributed range 10.0.0.1 10.0.0.100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master

ip-flow-export-profile

```
ip-flow-export-profile
   collector-ip <collector-ip>
   enable
   flow-cache-size <flow-cache-size>
   no
   observation-domain <observation-domain>
   port <port>
   transport-protocol {tcp | udp}
   upload-all-interval <upload-all-interval>
   upload-snapshot-interval <upload-snapshot-interval>
   upload-template-interval <upload-template-interval>
   wireless-export
```

Description

This command configures the IP flow collector profile. This command should be configured under **/md**.

Syntax

Parameter	Description	Range	Default
`collector-ip <collector-ip>`	Assigns a managed device as the IP Flow Collector within its node.		
`enable`	Enables the IP Flow Collector.		
`flow-cache-size <flow-cache-size>`	Determines the maximum number of entries a managed device can cache before the log is exported to the IP Flow Collector.	5000–25000	
`no`	Negates the prior configuration.		
`observation-domain <observation-domain>`	Allows the IP Flow Collector to group managed devices when receiving data sessions.		Switch IP as 32 Bit number
`port <port>`	Assigns the port to which the exported caches are sent on the IP Flow Collector.		
`transport-protocol`	Determines the transport protocol when a cache is exported.		
`tcp`	Assigns TCP as the transfer protocol .		
`udp`	Assigns UDP as the transfer protocol.		
`upload-all-interval <upload-all-interval>`	Determines the maximum time interval allowed before a managed device must export its cache to the IP Flow Collector.	0–30 minutes 0 to disable	
`upload-snapshot-interval <upload-snapshot-interval>`	Determines the maximum time interval cache for an inactive flow is exported.	0–30 minutes 0 to diable	

Parameter	Description	Range	Default
`upload-template-interval <upload-template-interval>`	Determines the maximum time interval to upload IPFIX templates.	0–30 minutes 0 to disable	0
`wireless-export`	Enables wireless export.		Disabled

Example

The following command configures a DHCP pool:

```
(host) [mynode] (config) #ip-flow-export-profile
(host) [mynode] (IP Flow Collector Profile) #enable
(host) [mynode] (IP Flow Collector Profile) #collector-ip 192.0.2.1
(host) [mynode] (IP Flow Collector Profile) #write memory
```

Related Commands

Command	Description
show ip-flow-export wireless-cache	Displays the cache for WLAN information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The **wireless-export** parameter was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on the Mobility Master

ipv6 cp-redirect-address

```
ipv6 cp-redirect-address <ip6addr> | disable
```

Description

This command configures a redirect address for captive portal.

Syntax

Parameter	Description
`<ip6addr>`	This address should be routable from all external networks.
`disable`	Disables automatic DNS resolution for captive portal.

Usage Guidelines

This command redirects wireless clients that are on different VLANs (from the managed device's IP address) to the captive portal on the managed device.

If you have the Next Generation PEFNG license installed in the managed device, modify the captive portal session ACL to permit HTTPS traffic to the destination **cp-redirect-address <ip6addr>** instead of **mswitch**. If you do not have the PEFNG license installed in the managed device, the implicit captive-portal-profile ACL is automatically modified when you issue this command.

Example

The following command configures a captive portal redirect address:

```
(host) [/md] (config) #ipv6 cp-redirect-address
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 default-gateway

```
ipv6 default-gateway mgmt <ipv6-address> <cost>
```

Description

This command configures an IPv6 default gateway.

Syntax

Parameter	Description
`mgmt`	Specify the Management Interface.
`<ipv6-address>`	Specify the IPv6 address of the default gateway.
`cost`	Specify the distance metric to select the routing protocol that determines the way to learn the route.

Usage Guidelines

This command configures an IPv6 default gateway.

Example

The following command configures an IPv6 default gateway:

```
(host) [/md] (config) #ipv6 default-gateway 2cce:205:160:100::fe 1
```

The following example displays the use of extended scope of address range:

```
(host) [/md] (config) #ipv6 default-gateway 2014::1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 dhcp excluded-address

```
ipv6 dhcp excluded-address <low-address> [<high-address>]
```

Description

This command configures an excluded IPv6 address range for the DHCPv6 server on the Mobility Master.

Syntax

Parameter	Description
`<low-ipaddr>`	Low end of range of IPv6 addresses. For example, you can enter an IPv6 address that should not be assigned.
`<high-ipaddr>`	High end of the range of IPv6 addresses.

Usage Guidelines

Use this command to specifically exclude certain IPv6 addresses from being assigned by the DHCPv6 server. Ensure that the statically assigned IPv6 addresses are excluded.

Example

The following command configures an excluded IPv6 address range:

```
(host) [/md/X.X.X.X.X.X] (config-dhcpv6)#ipv6 dhcp excluded-address 2002:570:20::2
2002:570:20::25
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in base operating system.	Config mode on Mobility Master

ipv6 dhcp pool

```
ipv6 dhcp pool <pool-name>
   dns-server <ipv6-address>
   domain-name <domain>
   lease <days> <hours> <minutes> <seconds>
   network <network prefix>
   no ...
   option <code> {ip <ipv6-addr> | text <string>}
   preference <1-255>
```

Description

This command configures a DHCPv6 pool on the Mobility Master.

Syntax

Parameter	Description
`dns-server`	IPv6 address of the DNS server.
`domain-name`	Domain name to which the client belongs.
`lease`	The amount of time that the assigned IPv6 address is valid for the client. Specify the lease in <days> <hours> <minutes> <seconds>. The default value is 12 hours.
`network`	The DHCPv6 network prefix.
`no`	Negates any configured parameter.
`option`	Client-specific option code and IPv6 address or text. See RFC 3315, DHCPv6.
`preference`	The DHCPv6 server preference.

Usage Guidelines

A DHCPv6 pool should be created for each IPv6 subnetwork for which DHCPv6 services should be provided. DHCPv6 pools are not specifically tied to VLANs, as the DHCPv6 server exists on every VLAN. When the Mobility Master receives a DHCPv6 request from a client, it examines the origin of the request to determine if it should respond. If the IPv6 address of the VLAN matches a configured DHCPv6 pool, the Mobility Master answers the request.

Example

The following command configures a DHCPv6 pool:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 dhcp pool DHCPv6
   (host) [/md/X.X.X.X.X.X] (config-submode) #dns-server 2001:470:20::2
   (host) [/md/X.X.X.X.X.X] (config-submode) #domain-name test.org
   (host) [/md/X.X.X.X.X.X] (config-submode) #lease 0 12 0 0
   (host) [/md/X.X.X.X.X.X] (config-submode) #network 2001:470:20::/64
   (host) [/md/X.X.X.X.X.X] (config-submode) #option 24 text "Domain Search List"
   (host) [/md/X.X.X.X.X.X] (config-submode) #preference 25
```

The following example displays the use of extended scope of address range, which is restricted only to DHCP pool configuration:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 dhcp pool sparta
   network 2012::/120
```

!

If the DHCP pool configuration on the managed device, that acts as a DHCP server has the address pool configured in the reserved range, then the APs gets an IP address from the server. If the address pool is not in the reserved range, then the AP cannot get an IP from the server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 domain lookup

```
ipv6 domain lookup
```

Description

This command enables IPv6 Domain Name System hostname translation for clients.

Syntax

No parameters.

Example

The following command enables IPv6 Domain Name System hostname translation:

```
(host) [mynode] (config) #ipv6 domain lookup
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **lookup** parameter was added.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 enable

```
ipv6 enable
```

Description

This command enables IPv6 packet processing globally. This option is disabled by default.

Syntax

No parameters.

Usage Guidelines

This command enables IPv6 packet processing globally.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 firewall

```
ipv6 firewall
   attack-rate {ping <number>|session <number>|tcp-syn <number>}
   deny-inter-user-bridging |
   drop-ip-fragments |
   enable-per-packet-logging |
   enable-stateful-icmp |
   enforce-tcp-handshake |
   ext-hdr-parse-len |
   no
   prohibit-ip-spoofing |
   prohibit-rst-replay |
   session-idle-timeout <seconds>
```

Description

This command configures firewall options on the Mobility Master for IPv6 traffic.

Syntax

Parameter	Description	Range	Default
`attack-rate`	Sets rates which, if exceeded, can indicate a denial of service attack.		
`ping`	Number of ICMP pings per 30 seconds, which if exceeded, can indicate a denial of service attack. Recommended value is 120.	1-16384	—
`session`	Number of TCP or UDP connection requests per 30 seconds, which if exceeded, can indicate a denial of service attack. Recommended value is 960.	1-16384	—
`tcp-syn`	Number of TCP SYN messages per 30 seconds, which if exceeded, can indicate a denial of service attack. Recommended value is 960.	1-16384	—
`deny-inter-user-bridging`	Prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic. This option can be used to prevent Appletalk or IPX traffic from being forwarded.	—	disabled
`drop-ip-fragments`	When enabled, all IP fragments are dropped. You should not enable this option unless instructed to do so by a customer support representative.	—	disabled
`enable-per-pac ket-logging`	Enables logging of every packet if logging is enabled for the corresponding session rule. Normally, one event is logged per session. If you enable this option, each packet in the session is logged. You should not enable this option unless instructed to do so by a customer support representative, as doing so may create unnecessary overhead on the Mobility Master.	—	disabled

Parameter	Description	Range	Default
`enforce-stateful-icmp`	Enables stateful ICMP processing and create sessions for ICMP errors and denies unidirectional response.	—	disabled
`enforce-tcp-handshake`	Prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.	—	disabled
`ext-hdr-parse-len`	Set the threshold value beyond which the IPv6 header will not be parsed and the packet will be dropped.	—	100 bytes
`prohibit-ip-spoofing`	Detects IP spoofing (where an intruder sends messages using the IP address of a trusted client). When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.	—	disabled
`prohibit-rst-replay`	Closes a TCP connection in both directions if a TCP RST is received from either direction. You should not enable this option unless instructed to do so by a customer support representative.	—	disabled
`session-idle-timeout`	Time, in seconds, that a non-TCP session can be idle before it is removed from the session table. You should not modify this option unless instructed to do so by a customer support representative.	16-300	16 seconds

Usage Guidelines

This command configures global firewall options on the Mobility Master for IPv6 traffic.

Example

The following command does not allow forwarding of non-IP frames between IPv6 clients:

```
(host) [/md] (config) #ipv6 firewall deny-inter-user-bridging
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system, except for noted parameters.	Config mode on Mobility Master

ipv6 helper-address

```
ipv6 helper-address
   helper-address <address>
      source <srcaddr>
```

Description

This command configures the DHCPv6 server relay agent. .

Syntax

Parameter	Description
`helper-address`	Configures DHCPv6 server relay agent.
`source`	Configure DHCPv6 relay source address if the interface has more than one IPv6 address.

Example

The following command configures a helper address:

```
(host) [00:0c:29:3c:f7:d3] (config-submode)#ipv6 helper-address 2017::2 source 2016::2
```

Command History

Version	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 local

```
ipv6 local
   pool <pool_name_v6> <pool_start_addressv6> <pool_end_addressv6>
```

Description

This command configures a local IPv6 pool for Layer-2 Tunnel Protocol (L2TP).

Syntax

Parameter	Description
`pool`	Name for the address pool.
`<pool_start_addressv6>`	Starting IPv6 address for the pool.
`<pool_end_addressv6>`	(Optional) Ending IPv6 address for the pool.

Usage Guidelines

VPN clients can be assigned IPv6 addresses from the L2TP pool.

Example

The following command configures a local IPv6 pool:

```
(host) [mynode] (config) #ipv6 local pool 2001:0000:0eab:DEAD:0000:OOAO:ABCD:004E
2002:0000:0eab:DEAD:0000:OOAO:ABCD:004E
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Master

ipv6 name-server

```
ipv6 name-server
   X:X:X:X::X
```

Description

This command configures the IPv6 address of the domain name server.

Syntax

Parameter	Description
`X:X:X:X::X`	Domain server IPv6 address (maximum of 6).

Example

The following command adds IPv6 name server (DNS server):

```
(host) [mynode] (config) #ipv6 name-server 2020::abcd:abcd
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The domain server IPv6 address was added.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config mode on Mobility Master

ipv6 neighbor

```
ipv6 neighbor <ipv6addr> vlan <vlan#> <mac>
```

Description

This command configures an IPv6 static neighbor on a VLAN interface.

Syntax

Parameter	Description
`<ipv6addr>`	Specify the IPv6 address of the neighbor entry.
`vlan <vlan#>`	Specify the VLAN ID.
`<mac>`	Specify the 48-bit hardware address of the neighbor entry.

Usage Guidelines

You can configure an IPv6 static neighbor on a VLAN interface.

Example

The following command configures an IPv6 static neighbor on VLAN 1:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 neighbor 2cce:205:160:100::fe vlan 1 00:0b:86:61:13:28
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Master

ipv6 mld

```
ipv6 mld
   max-members-per-group <val>
   no
   query-interval <query-interval>
   query-response-interval <query-response-interval>
   robustness-variable <robustness-variable>
   ssm-range <startip> <maskip>
```

Description

This command configures the IPv6 MLD (Multi-listener discovery) parameters.

Syntax

Parameter	Description
`max-members-per-group`	Configure maximum members per group (1-65535). The default value is 300.
`query-interval`	Specify the time interval in seconds (1-65535) between general queries. The default value is 125 seconds. By varying this value, you can tune the number of MLD messages on the link; larger values cause MLD queries to be sent less often.
`query-response-interval`	Specify the maximum response delay in deciseconds (1/10 seconds) that can be inserted into the periodic general queries. The default value is 100 deciseconds. By varying this value, you can tune the burstiness of MLD messages on the link; larger values make the traffic less bursty, as node responses are spread out over a larger interval. The number of seconds represented by this value must be less than the query interval.
`robustness-variable`	Specify a value between 2 to 10. The default value is 2. The robustness variable allows you to tune for the expected packet loss on a link. If a link is expected to be lossy, you can increase this value. You must not configure the robustness variable as 0 or 1.
`ssm-range`	Specify the source specific multicast IPv6 range. This variable allows you to configure a valid multicast IPv6 address range for which SSM semantics needs to be applied. The default IPv6 SSM address range is FF3X::4000:1 – FF3X::FFFF:FFFF.

Usage Guidelines

You can modify the default values of the MLD parameters for IPv6 MLD snooping. You must enable IPv6 MLD snooping for these values to take effect. For more information on enabling IPv6 MLD snooping, see interface vlan on page 571.

Example

The following command configures the query interval of 200 seconds for IPv6 MLD snooping:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 mld
(host) [/md/X.X.X.X.X.X] (config-mld) # query-interval 200
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **max-members-per-group** parameter was added.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on managed devices

ipv6 proxy-ra

```
ipv6 proxy-ra
   interval <value>
```

Description

This command configures an interval for proxy RA.

Syntax

Parameter	Description
`interval`	Configures the proxy RA interval (180-1800 sec). This overrides interface RA interval value if it is lesser.

Usage Guidelines

This command configures interval for proxy RA.

Example

The following command enables proxy RA:

```
(host) [md] (config) #ipv6 proxy-ra
IPv6 RA proxy already enabled.
```

The following command configures a global NAS IPv6 address sent in RADIUS packets:

```
(host) [md] (config) #ipv6 proxy-ra interval 200
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **proxy-ra** parameter was modified to enable proxy RA.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Master

ipv6 radius

```
ipv6 radius
   nas-ip6 { nas-vlan <nasvlan>|<ipv6-addr>}
   source-interface {loopback|vlan <vlan> <ip6addr>}
```

Description

This command configures global parameters for configured IPv6 RADIUS servers.

Syntax

Parameter	Description
`nas-ip6`	A global NAS IPv6 address to send in RADIUS packets. This configuration supercedes the server-specific NAS IPv6 configured with the **aaa authentication-server radius** command.
`nas-vlan <nasvlan>`	The NAS VLAN to be used as NAS IP.
`ipv6-addr`	The NAS IPv6 address.
`source-interface`	Interface for all outgoing RADIUS packets. The IPv6 address of the specified interface is included in the IP header of RADIUS packets. The interface can be one of the following:
`loopback`	The loopback interface.
`vlan`	The specified VLAN.

Usage Guidelines

This command configures global IPv6 RADIUS server parameters. If the `aaa authentication-server radius` command configures a server-specific NAS IPv6 address, the server-specific IPv6 address is used instead.

Example

The following command configures a global NAS IPv6 address sent in RADIUS packets:

```
(host) [md] (config) #ipv6 radius nas-ip6 2001:470:20::2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system.	Config mode on Mobility Master

ipv6 route

```
ipv6 route {X:X:X:X::X/<0-128>}|ipv6-next-hop|null|vlan[vlanid]|link-local-next-hop}|cost
```

Description

This command configures static IPv6 routes on the managed device.

Syntax

Parameter	Description
`X:X:X:X::X/<0-128>`	Specify the IPv6 address and the prefix length of the destination.
`<ipv6-next-hop>`	Specify the next-hop IPv6 address or null 0 to terminate or discard the packets. Listed below are the following options: ■ X:X:X:X::X-IPv6 address of next-hop. The address should only be a Global IPv6 address. ■ null-Null interface ■ vlan-Vlan for link local for next-hop ■ <vlanid>-Vlan-id for link local next-hop ■ X:X:X:X::X-IPv6 link local address of next-hop
`<cost>`	Specify the distance metric to select the routing protocol that determines the way to learn the route.

Usage Guidelines

You can configure static IPv6 routes on the managed device.

Example

The following command configures a static IPv6 route on the managed device:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 route 2cce:205:160:100::/<64> 2001:205:160:100::ff 1
(host) [/md/X.X.X.X.X.X] (config) #ipv6 route 2000:eab::/64 vlan 1 fe80::1a:1e00:a00:9f0
```

The following example displays the use of extended scope of address range:

```
(host) [/md/X.X.X.X.X.X] (config) #ipv6 route 2002::/64 2004::2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

kernel coredump

```
[no] kernel coredump
```

Use this command under the supervision of Aruba Global Technical Support.

Description

This command enables the controller to capture the snapshot of the working memory of the control plane when the control plane has terminated abnormally.

An additional flash memory available check is imposed on core dump. If less than 100 MB of space is left on the flash, the extra core dump chunks get discarded.

Syntax

Parameter	Description	Range	Default
`coredump`	Enable kernel core dump on the controller.	—	Disabled

Usage Guidelines

After issuing this command, you may run the **write memory** command to save the configuration. This will enable the kernel core dumps across reboots.

Example

The following example enables kernel core dump on the controller:

```
(host) (config) #kernel coredump
```

Use the following command to save the configuration change using the CLI:

```
(host) (config) #write memory
```

Use the following command to view the kernel core dump status using the CLI:

```
(host) (config) #show running-config | include kernel
Building Configuration...
kernel coredump
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

lb-group

```
<name>
   gre-standby
   hold-time <number>
   no {gre-standby|hold-time|preemption|primary|randomize-time|secondary}
   preemption
   primary
   randomize-time <number>
   secondary
```

Description

Manage and configure the load balancing group.

Syntax

Parameter	Description	Range
`name`	Name of load balancing group	—
`gre-standby`	Enable GRE standby	—
`hold-time <number>`	Hold time after which failover occurs	—
`no`	Disable load balancing group features	—
`preemption`	Enable preemptive failover	—
`primary`	Configure primary map	—
`randomize-time <number>`	Random time after hold-time when failover occurs	—
`secondary`	Configure secondary map	—

Usage Guidelines

Configure the load balance properties using the load-balance group command.

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on managed device.

lc-cluster exclude-vlan

```
lc-cluster exclude-vlan <excludevlan>
```

Description

This command is used to exclude certain VLANs for the VLAN probing algorithm on the managed devices.

Syntax

Parameter	Description
`<excludevlan>`	List of exception VLANs separated by comma (,), range by (-). Max string length: 256.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system	Config mode on managed devices

lc-cluster initiate Upgrade

```
lc-cluster <cluster_name> initiate upgrade version <img_version> partition <partition_id>
```

Description

This command is used to trigger the cluster upgrade in the Mobility Master:

Syntax

Parameter	Description
`upgrade`	Upgrade using information in configured upgrade-profile
`version`	Target image version, for example, 8.1.0.0_XXXXX
`partition`	The partition on the managed device to which the new image is to be copied, valid values are 0 or 1 and this is optional. If the partition not specified, it will automatically pick the alternate boot partition.

Example

```
(host) [mm] [cluster1] #lc-cluster <cluster_name> initiate upgrade version <img_version>
partition <partition_id>
```

- cluster_name: The configured cluster profile name, the managed devices and APs associated to the cluster that needs to be upgraded.

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system	Config mode on Mobility Master

lc-cluster group-membership

`lc-cluster group-membership`

Description

Configure the group-membership in each node. This command is used to enable the cluster membership on the managed devices.

Syntax

Parameter	Description
`<profile>`	Enter the cluster profile name.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system	Config mode on managed devices.

lc-cluster group-profile

```
lc-cluster group-profile <profile>
   active-ap-lb
   active-ap-rebalance-ap-count <active-ap-rebalance-ap-count>
   active-ap-rebalance-threshold-percentage <active-ap-rebalance-threshold-percentage>
   active-ap-rebalance-timer <active-ap-rebalance-timer>
   active-ap-unbalance-threshold-percentage <active-ap-unbalance-threshold-percentage>
   active-client-rebalance-threshold
   clone <source>
   controller <ip> [priority <prio>] [mcast-vlan <mcast_vlan>] [vrrp-ip <vrrp_ip> vrrp-vlan
   <vrrp_vlan> group <group number>]
   controller-v6 <ipv6>
   heartbeat-threshold <heartbeat-threshold>
   redundancy
   standby-client-rebalance-threshold <standby-client-rebalance-threshold>
   unbalance-threshold<unbalance-threshold>
```

Description

This command is used to configure the cluster group profile in the Mobility Master.

Syntax

Parameter	Description
`<profile>`	Enter the cluster profile name you want to create.
`active-ap-lb`	Enable load balancing of APs by load sharing active AACs among cluster members.
`active-ap-rebalance-ap-count <active-ap-rebalance-ap-count>`	Specify the number of APs when active AP rebalance is initiated.
`active-ap-rebalance-threshold-percentage <active-ap-rebalance-threshold-percentage>`	Redistribute active AP load when active load on any cluster is beyond this configured percentage.
`active-ap-rebalance-timer <active-ap-rebalance-timer>`	Time, in minutes, to initiate the active AP rebalancing operation.

Parameter	Description
`active-ap-unbalance-threshold-percentage <active-ap-unbalance-threshold-percentage>`	Redistribute active AP load when the controllerreaches the rebalance threshold and the difference between the maximum and minimum load on the controller is more than this threshold percentage.
`active-client-rebalance-threshold`	Redistribute active client load when active load on any cluster node is beyond this configured percentage
`clone <source>`	Copy data from another controller cluster profile.
`controller <ip>`	Managed device to be made part of this cluster. The IPv4 Address is the value of the **controller-ip**
`priority <prio>`	Defines the priority level for the managed devices
`mcast-vlan <mcast_vlan>`	Enter the multicast vlan
`vrrp-ip <vrrp_ip>`	Configure the VIP address that will be owned by the elected VRRP master.

Parameter	Description
`vrrp-vlan <vrrp_vlan>`	Specifies the VLAN ID of the VLAN on which VRRP will run.
`group <group_id>`	The value of the parameter is an integer and the range is 1-12. The value 0 is the unset value if you do not want to group the managed devices.
`controller-v6 <ipv6>`	Controller to be made part of this cluster. The IPv6 address is the value of the **controller-ip**.
`group <group_id>`	The value of the parameter is an integer and the range is 1-12. The value 0 is the unset value if you do not want to group the managed devices.
`mcast-vlan <mcast_vlan>`	Enter the multicast VLAN to be used for forwarding multicast traffic to upstream router.
`priority <prio>`	Define the priority level for the managed devices. The value of this parameter is in the range of 1-255. The default value is 128.

Parameter	Description
vrrp-ip-v6 <vrrp_ip_v6>	Configure the IPv6 address that is owned by the elected VRRP master.
heartbeat-threshold	Cluster has an adaptive heartbeat mechanism that adjusts the frequency of heartbeats based on RTD data. This mechanism waits for a period of time, determined based on maximum RTD observed during the last 100 successful heartbeats, before declaring a peer cluster node to be dead. The configured value, if greater, overrides the time taken for the heartbeat algorithm to declare peer dead. When not configured, the failure detection is purely based on the cluster heartbeat algorithm.
redundancy	Enable load sharing redundancy among cluster members.

Parameter	Description
standby-client-rebalance-threshold	Redistribute standby client load when total load on any cluster node is beyond this configured percentage
unbalance-threshold	Indicates the minimum difference in load percentage between max loaded cluster node and min loaded cluster node to let load balancing algorithm kick in.

Example

The following command adds the managed devices to a group profile:

```
(host) [md] (config)lc-cluster group-profile cluster6
(host) [md] (Classic Controller Cluster Profile "cluster6") controller 192.168.28.22 priority
128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 1
(host) [md] (Classic Controller Cluster Profile "cluster6") controller 192.168.28.23 priority
128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 1
(host) [md] (Classic Controller Cluster Profile "cluster6") controller 192.168.28.24 priority
128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 2
(host) [md] (Classic Controller Cluster Profile "cluster6") controller 192.168.28.26 priority
128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 2
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: ■ **active-ap-lb** ■ **active-ap-rebalance-ap-count** ■ **active-ap-rebalance-threshold-percentage** ■ **active-ap-rebalance-timer** ■ **active-ap-unbalance-threshold-percentage** ■ **controller-v6** ■ **redundancy**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system	Config mode on Mobility Master

lc-cluster start-vlan-probe

```
lc-cluster start-vlan-probe
```

Description

This command is used to trigger a VLAN probe on the managed devices.

Syntax

No syntax.

Usage Guidelines

After removing the VLANs using the command, **lc-cluster exclude-vlan**, execute this command to re-run the VLAN probing algorithm.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Managed Device

lacp group

```
lacp group <group_number> mode {active | passive}
```

Description

Enable LACP and configure LACP on the interface.

Parameter	Description
`<group_number>`	Enter the LAG number. Range: 0-7
`mode {active | passive}`	Enter the keyword **mode** followed by either the keyword **active** or **passive**. ■ Active mode—the interface is in active negotiating state. LACP runs on any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets. ■ Passive mode—the interface is *not* in an active negotiating state. LACP runs on any link that is configured in a passive state. The port in a passive mode responds to negotiations requests from other ports that are in an active state. Ports in passive state respond to LACP packets.

Usage Guidelines

LACP is disabled by default; this command enables LACP. If the group number assigned contains static port members, the command is rejected.

Related Command

Command	Description
show lacp	View the LACP configuration status
show interface port-channel	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

lacp port-priority

```
lacp port-priority <priority_value>
```

Description

Configure the LACP port priority.

Syntax

Parameter	Description
`<priority value>`	Enter the port-priority value. The higher the value number the lower the priority. Range: 1 to 65535 Default: 255

Usage Guidelines

Set the port priority for LACP.

Related Commands

Command	Description
lacp group	Enable LACP and configure on the interface
show lacp	View the LACP configuration status
show interface port-channel	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platform	License	Command Mode
All Platforms	Base operating system	Configuration Interface Mode (config-if) for Mobility Master

lacp system-priority

```
lacp system-priority <priority_value>
```

Description

This command configures the LACP system priority.

Syntax

Parameter	Description	Range	Default
`<priority_value>`	Enter the system priority value. The higher the value number the lower the priority.	1-65535	32768

Related Commands

Command	Description
lacp group	Enable LACP and configure on the interface
show lacp	View the LACP configuration status
show interface port-channel	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

lacp timeout

```
lacp timeout {long | short}
```

Description

Configure the timeout period for the LACP session.

Syntax

Parameter	Description
`long`	Enter the keyword **long** to set the LACP session to 90 seconds. This is the default.
`short`	Enter the keyword **short** to set the LACP session to 3 seconds.

Usage Guidelines

The timeout value is the amount of time that a port-channel interface waits for a LACP data units from the remote system before terminating the LACP session. The default time out value is 90 seconds (long).

Related Commands

Command	Description
lacp group	Enable LACP and configure on the interface
show lacp	View the LACP configuration status
show interface port-channel	View information on a specified port channel interface

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

lc-rap-pool

```
lc-rap-pool <pool_name>
```

Description

This command is used to configure the Remote AP inner IP pool for cluster deployment.

Syntax

Parameter	Description
`pool_name`	Specify the name of the local IP pool.
`pool_start_address`	Configure the start address of the local pool.
`pool_end_address`	Configure the end address of the local pool.

Example

To configure a Remote AP inner pool for cluster deployment, execute the command

```
(host) [mynode] (config) #lc-rap-pool rap-cluster 3.1.1.3 3.1.1.10
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

lcd-menu

```
lcd-menu
   [no] disable menu [maintenance [factory-default| media-eject| qui-quick-setup | media-eject
   | system-halt | system-reboot | upgrade-image [parition0 | partition1]| upload-config]]
```

Description

This command allows you to enable or disable the LCD menu either completely or for specific operations.

Syntax

Parameter	Description	Default
`lcd-menu`	Enters the LCD menu configuration mode.	—
`no`	Delete the specified LCD menu option.	—
`disable`	Disables (or enables) the complete LCD menu.	—
`maintenance`	Disables (or enables) the maintenance LCD menu.	Enabled
`factory-default`	Disables (or enables) the return to factory default option in the LCD menu.	Enabled
`media-eject`	Disables (or enables) the media eject option in the LCD menu.	Enabled
`system-halt`	Disables (or enables) the system halt option in the LCD menu.	Enabled
`system-reboot`	Disables (or enables) the system reboot in the LCD menu.	Enabled
`upgrade-image`	Disables (or enables) the upgrade image option in the LCD menu.	Enabled
`partition 0` `partition 1`	Disables (or enables) image upgrade on the specified partition (0 or 1).	Enabled
`upload-config`	Disables (or enables) the upload config option in the LCD menu.	Enabled

Usage Guidelines

You can use this command to disable executing the maintenance operations using the LCD menu. You can use the no form of these commands to enable the specific LCD menu. For example, the following commands enable system halt and system reboot options:

```
(host) [mynode] (config) #lcd-menu
(host) [mynode] (lcd-menu) #no disable menu maintenance system-halt
(host) [mynode] (lcd-menu) #no disable menu maintenance system-reboot
```

You can use the following show command to display the current LCD settings:

```
(host) [mynode]#show lcd-menu
lcd-menu
--------
Menu                                          Value
----                                          -----
menu maintenance upgrade-image partition0     enabled
menu maintenance upgrade-image partition1     enabled
menu maintenance system-reboot reboot-stack   enabled
menu maintenance system-reboot reboot-local   enabled
```

```
menu maintenance system-halt halt-stack      enabled
menu maintenance system-halt halt-local      enabled
menu maintenance upgrade-image               enabled
menu maintenance upload-config               enabled
menu maintenance factory-default             enabled
menu maintenance media-eject                 enabled
menu maintenance system-reboot               enabled
menu maintenance system-halt                 enabled
menu maintenance gui-quick-setup             enabled
menu maintenance                             enabled
menu                                         enabled
```

Example

The following example disables the LCD menu completely:

```
(host) [mynode] (config) #lcd-menu
(host) [mynode] (lcd-menu) #disable menu
```

The following example disables executing the specified maintenance operation using the LCD menu:

```
(host) [mynode] (config) #lcd-menu
(host) [mynode] (lcd-menu) #disable menu maintenance ?
factory-default          Disable factory default menu
gui-quick-setup          Disable quick setup menu on LCD
media-eject              Disable media eject menu on LCD
system-halt              Disable system halt menu on LCD
system-reboot            Disable system reboot menu on LCD
upgrade-image            Disable image upgrade menu on LCD
upload-config            Disable config upload menu on LCD
(host) (lcd-menu) #disable menu maintenance upgrade-image ?
partition0               Disable image upgrade on partition 0
partition1               Disable image upgrade on partition 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
7200 Series controllers	Base operating system	Config mode on Mobility Master

license

```
license
   add <key>
   del <key>
   export <filename>
   import <filename>
   remote remote-ip-addr <ip-addr> add <key>
   report <filename>}
   server-ip  <ip-addr>
```

Description

This command allows you to install, delete, and manage software licenses on Mobility Master.

Syntax

Parameter	Description
`add`	Installs the software license key in Mobility Master. The key is normally sent to you via email.
`del`	Removes the software license key from Mobility Master. The key is normally sent to you via email. This parameter is available in enable mode.
`export`	Exports the license database on Mobility Master to the specified file in flash.
`import`	Replaces the license database on Mobility Master with the specified file in flash. The system serial numbers referenced in the imported file must match the numbers on the Mobility Master.
`remote remote-ip-addr <ip-addr> add <key>`	Use this command to associate a non-sharable license installed on the Mobility Master with the managed device for which that license key was generated. The <ip-addr> parameter is the IP address of the managed device, and <key> is the license key for the non-sharable license.
`report`	Saves a license report to the specified file in flash.
`server-ip  <ip-addr>`	Enter the IP address of the licensing server on a standalone controller or a Mobility Master to configure that controller as a licensing client. This command must be configured from the Mobility Master configuration node.

Usage Guidelines

ArubaOS supports a centralized licensing architecture, which allows a group of managed devices to share a pool of licenses. A primary and backup Mobility Master can share a single set of licenses, eliminating the need for a redundant license set on the backup server. Managed devices maintain information sent from the Mobility Master, even if the managed device and the Mobility Master can no longer communicate.

A Mobility Master uses licensing pools to distribute licenses to a large number of managed devices across geographic locations. By default, all managed devices associated to a Mobility Master share a single global pool of all the sharable licenses added to that Mobility Master. However, ArubaOS also allows you to create additional licensing pools at a configuration node, allowing a groups of managed devices at or below that configuration level to share licenses among themselves, but not with other groups. For information on creating license pools using the Mobility Master CLI, see license-pool-profile.

New licenses and license pools can only be added through the Mobility Master WebUI. Licenses cannot be added directly to a managed devices. If a controller had previously installed sharable licenses before it was added to a Mobility Master as a managed devices, those licenses are no longer usable on that device. Those license keys must be regenerated and assigned to the **managed device** or licensing pool using the Mobility Master WebUI.

For complete information on the centralized licensing feature, refer to the *Aruba Mobility Master Licensing Guide.*

Examples

From any configuration node , issue the command **license add <key>**.

```
(host)[mynode] #license add lnZSpC2vkLMlJw8KVYdgj2
```

Related Commands

Command	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license-pool-profile	Use this command to create a local licensing pool and allocate licenses for that licensing pool.

Command History

Release	Modification
ArubaOS 8.2.0	The **server-ip** parameter can now associated multiple Mobility Masters to a licensing server. In previous releases, this command was supported on standalone controllers only.
ArubaOS 8.0.1.0	The **server-ip** and **remote remote-ip-addr** parameters are introduced, and the **remote ip-addr** parameter is deprecated.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

license-pool-profile

```
license-pool-profile <profile>
   acr-licenses {eval key <key> <num>}|<num>
   ap-licenses {eval key <key> <num>}|<num>
   clone <source>
   license-pool-path <license-pool-path>
   mc-va-licenses-eg {eval key <key> <num>}|<num>}
   mc-va-licenses-il {eval key <key> <num>}|<num>}
   mc-va-licenses-jp {eval key <key> <num>}|<num>}
   mc-va-licenses-rw {eval key <key> <num>}|<num>}
   mc-va-licenses-us {eval key <key> <num>}|<num>}
   mm-license {eval key <key> <num>}|<num}
   no
   pefng-licenses {eval key <key> <num>}|<num>}
   rfp-licenses {eval key <key> <num>}|<num>}
   via-licenses {eval key <key> <num>}|<num>}
   webcc-licenses {eval key <key> <num>}|{subscript key <key> <num>}
```

Description

Use this command to create a local licensing pool and allocate licenses for that licensing pool.

Syntax

Parameter	Description
`<profile>`	The name of the profile for which you are creating a local license pool, for example, Northwest. The profile name is limited to 63 characters. **NOTE:** In ArubaOS 8.0.x releases, the licensing pool profile name was required to be the license pool configuration path. Starting in ArubaOS 8.1, the **license-pool-path** parameter is introduced to configure the license pool path, and the profile name can be any string of 63 characters or less.
`acr-licenses`	Add ArubaOS Advanced Cryptography (ACR) licenses to the selected pool. A license is required for each active client termination using Suite-B algorithms or protocols. Use the optional **eval key <key>** parameters to specify an evaluation license key.
`ap-licenses`	Add AP licenses to the selected pool.
`clone`	Copy licenses from another license pool profile.
`license-pool-path <license-pool-path>`	Starting in ArubaOS 8.1.0.0, use this parameter to specify a license pool path, up to 255 characters, for example, /USA/northwest. **NOTE:** If you upgrade a legacy ArubaOS deployment to ArubaOS 8.1 or later, the license-pool-path parameter is automatically derived from the license-pool-profile <profile> name.

`mc-va-licenses-eg`
`mc-va-licenses-il`
`mc-va-licenses-jp`
`mc-va-licenses-rw`
`mc-va-licenses-us`
	Add the following different MC-VA-XX license types enable APs to support regional channels for the following countries:
	■ MC-VA-US: United states
	■ MC-VA-JP: Japan
	■ MC-VA-IL: Israel
	■ MC-VA-EG: Egypt
	■ MC-VA-RW: Rest of the world (all other countries)

Parameter	Description
`mm-licenses`	Add Mobility Master licenses to the selected pool.
`pefng-licenses`	Add PEF licenses to the selected pool to support PEF features, such as intelligent application identification, policy-based traffic management and controls, or stateful user firewalls.
`rfp-licenses`	Add RF Protect licenses to the selected pool, to support features such as spectrum analysis and WIP.
`via-licenses`	VIA licenses support VIA or 3rd party VPN client . VIA licenses are not consumed for site-to-site VPNs. If a managed device or standalone controller has a PEFV license, that device will not consume VIA licenses from a licensing pool, as a single PEFV license supports all VIA and 3rd party VPN clients, up to the full user capacity for that device.
`webcc-licenses`	Add WebCC licenses to the selected pool. The WebCC license is a subscription-based, per-AP license.
`[eval key <key>]`	Use the optional **eval key <key>** parameters to add the specified number of licenses for an evaluation license key.
`<num>`	Number of licenses supported by the license key.

Usage Guidelines

All managed devices associated to the same Mobility Master can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Master. However, ArubaOS also allows you to create individual licensing pools at a configuration node, allowing managed devices below that node to share licenses amongst themselves but not with other managed devices.

You must use the **license add** command to add license keys to the Mobility Master before you can allocate sharable licenses to a license pool, or associate a non-sharable license with an individual managed device.

For complete information on the centralized licensing feature, refer to the *Aruba Mobility Master Licensing Guide.*

Examples

```
(host)[mm] (config) #license-pool-profile Southwest
(host) ^[mm] (License pool profile "Southwest") #license-pool-path /USA/southwest
(host) ^[mm] (License pool profile "Southwest") #ap-licenses 64
(host) ^[mm] (License pool profile "Southwest") #pefng-licenses 64
(host) ^[mm] (License pool profile "Ssouthwest") #rfp-licenses 64
```

Related Commands

Version	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license	This command allows you to install, delete, and manage software licenses on Mobility Master.

Command History

Version	Description
ArubaOS 8.1.0.0	The **license-pool-path** parameter is introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

license-pool-profile-root

```
license-pool-profile-root
   acr-license-enable
   no
   pefng-licenses-enable
   rfp-license-enable
   webcc-license-enable
```

Description

Use this command to enable shared license features within the global licensing pool.

Syntax

Parameter	Description
`acr-license-enable`	Enable ArubaOS Advanced Cryptography features. A license is required for each active client termination using Suite-B algorithms or protocols.
`no ...`	Include the no parameter before any license type to remove that configuration setting and disable licensing features for that license type.
`pefng-licenses-enable`	Enable PEF features, such as intelligent application identification, policy-based traffic management and controls, or stateful user firewalls.
`rfp-license-enable`	Enable RF Protect features, such as spectrum analysis and WIP.
`webcc-license-enable`	The Web Content Classification license is a subscription-based, per-AP license. Issue the **webcc-license-enable** command to enable web content classification features for the duration of the subscription period (up to 10 years per license)

Usage Guidelines

All managed devices associated to the same Mobility Master can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Master.Use this command to enable the functionality for a shared license functionality within these license pools.

Only AP licenses and VIA license are enabled by default when those licenses are added to Mobility Master, all other licenses must be manually enabled.

For complete information on the centralized licensing feature, refer to the *Aruba Mobility Master Licensing Guide.*

Examples

From the SC configuration, issue the command **license-pool-profile-root acr-license-enable**.

```
(host) [MM](config) #license-pool-profile-root
(host) [MM](License root(/) pool profile) #acr-license-enable
```

Related Commands

Version	Description
license-pool-profile	Use this command to create a local licensing pool and allocate licenses for that licensing pool.
license	This command allows you to install, delete, and manage software licenses on Mobility Master.

Command History

Version	Description
ArubaOS 8.2.0.0	The **xsc-license-enable** parameter is deprecated.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode from the MM configuration node on Mobility Master.

local-custom-cert

```
local-custom-cert local-mac <lmac> ca-cert <ca> server-cert <cert> load-balance suite-b <gcm-128 | gcm-256>
```

Description

This command configures the user-installed certificate for secure communication between a managed device and a Mobility Master.

Syntax

Parameter	Description
`<lmac>`	MAC address of the managed device with a local custom certificate.
`ca-cert <ca>`	User-defined name of a trusted CA certificate installed on the managed device. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the managed device.
`server-cert <cert>`	User-defined name of a server certificate installed on the managed device. Use the show **crypto-local pki ServerCert** command to display the server certificates that have been imported into the managed device.
`suite-b`	If you configure your Mobility Master to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: ■ **gcm-128** Use 128-bit AES-GCM Suite-B encryption ■ **gcm-256** Use 256-bit AES-GCM Suite-B encryption

Usage Guidelines

Use this command on a Mobility Master to configure the custom certificate for communication with a managed device. On the managed device, use the **masterip** command to configure the IP address and certificates for the Mobility Master. If your Mobility Master and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

When a managed device communicates with Mobility Master to set up IPsec tunnels, the uplink vlan tag configured via the uplink command will be sent along in vendor-id payload during IKE negotiation. This will uniquely bind the tunnel from a particular uplink on the managed device to a corresponding map on Mobility Master.

Example

The following command configures the managed device with a user-installed certificate:

```
(host) [mynode] (config) #local-custom-cert local-mac 00:16:CF:AF:3E:E1 ca-cert cacert1 server-cert servercert1
```

Related Commands

Command	Description	Mode
show local-cert-mac	Display the IP, MAC address and certificate configuration of managed devices.	Config mode on Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	The **suite-b gcm-128** and **suite-b gcm-256** encryption options for IPsec custom certificates requires the Advanced Cryptography license. All other parameters are available in the base operating system	Config mode on Mobility Master

local-factory-cert

```
local-factory-cert local-mac <lmac> [load-balance]
```

Description

This command configures the factory-installed certificate for communication between a managed device and a Mobility Master.

Syntax

Parameter	Description
`<lmac>`	MAC address of the managed device with a local certificate.

Usage Guidelines

Use this command on a Mobility Master to configure the factory certificate for communication with a managed device. On the managed device, use the **masterip** command to configure the IP address and certificates for the Mobility Master. If your Mobility Master and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

When a managed device communicates with Mobility Master to set up IPsec tunnels, the uplink vlan tag configured via the uplink command will be sent along in vendor-id payload during IKE negotiation. This will uniquely bind the tunnel from a particular uplink on the managed device to a corresponding map on Mobility Master.

Example

The following command configures the managed device with a factory-installed certificate:

```
(host)[node](config) #local-factory-cert local-mac 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description	Mode
show local-cert-mac	Display the IP, MAC address and certificate configuration of managed device.	Config mode on Mobility Master

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Available in the base operating system	Config mode on Mobility Master

localip

```
localip <ipaddr>
   ipsec <key>
```

Description

This command configures the IP address and preshared key for the managed device on a Mobility Master.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the managed device. Use the 0.0.0.0 address to configure a global preshared key for all inter-managed device communications.
`ipsec <key>`	To establish the master-local IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.

Usage Guidelines

Use this command on a Mobility Master to configure the IP address and preshared key or certificates for communication with a managed device. On the managed device, use the **masterip** command to configure the IP address and preshared key for the Mobility Master.

If your Mobility Master and managed devices use a PSK for authentication, they will create the IPsec tunnel using IKEv1.

Example

The following command configures the managed device with a PSK:

```
(host) [mynode] (config) #localip 0.0.0.0 ipsec gw1234xyz
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master.

localipv6

```
localipv6 <local-switch-ipv6>
   ipsec <key>
```

Description

This command configures the IP address and preshared key for the managed device on a Mobility Master.

Syntax

Parameter	Description
`<local-switch-ipv6>`	IP address of the managed device. Use the 0.0.0.0 address to configure a global PSK for communication between managed devices.
`ipsec <key>`	To establish the master-local IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.

Usage Guidelines

Use this command on a Mobility Master to configure the IP address and preshared key or certificates for communication with a managed device. On the managed device, use the **masterip** command to configure the IP address and preshared key for the Mobility Master.

If your Mobility Master and managed devices use a PSK for authentication, they will create the IPsec tunnel using IKEv1.

Example

The following command configures the managed device with a PSK:

```
(host) [mynode] (config) #localipv6 2001:0000:0eab:DEAD:0000:OOAO:ABCD:004E ipsec gw1234xyz
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master

local-peer-mac

```
local-peer-mac <local-mac-addr> ipsec <localkey>
```

Description

This command is used to configure security peer-mac based between Mobility Master and managed devices.

Syntax

Parameter	Description
`local-mac-addr`	Enter the managed device's MAC address.
`ipsec localkey`	Configure the value of the IKE PSK, it must be between 6-64 characters

Example

The following command configures the security peer-mac:

```
(host) [mynode] (config) #local-peer-mac 00:0c:29:00:00:00 ipsec 123456
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master

local-userdb add

```
local-userdb add
   generate-username {generate-password|password <passwd>}
      comments
      email
      expiry
      guest-company
      guest-fullname
      guest-phone
      mode
      opt-field-1
      opt-field-2
      opt-field-3
      opt-field-4
      remote-ip
      role
      sponsor-dept
      sponsor-email
      sponsor-fullname
      sponsor-name
      start-time
   username <name> {generate-password|password <passwd>}
      comments
      email
      expiry
      guest-company
      guest-fullname
      guest-phone
      mode
      opt-field-1
      opt-field-2
      opt-field-3
      opt-field-4
      remote-ip
      role
      sponsor-dept
      sponsor-email
      sponsor-fullname
      sponsor-name
      start-time
```

Description

This command creates a user account entry in Mobility Master's internal database.

Syntax

Parameter	Description	Range	Default
`generate-username`	Automatically generate and add a username.	—	—
`username`	Add the specified username.	1–64 characters	—
`generate-password`	Automatically generate a password for the username.	—	—

Parameter	Description	Range	Default
password	Add the specified password for the username.	6–128 characters	—
comments	Comments added to the user account.	—	—
email	Email address for the user account.	—	—
expiry	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
duration	Duration, in minutes, for the user account.	1–2147483647	—
time	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.	—	—
guest-company	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Aruba wireless network.	—	—
guest-fullname	The guest's full name.	—	—
guest-phone	The guest's phone number.	—	—
mode	Enables or disables the user account.	—	disabled
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
opt-field-2	Same as **opt-field-1**.	—	—
opt-field-3	Same as **opt-field-1**.	—	—
opt-field-4	Same as **opt-field-1**.	—	—
remote-ip	IP address assigned to the remote peer.	—	—
role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.	—	guest
sponsor-dept	The guest sponsor's department name. **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
sponsor-email	The sponsor's email address.	—	—
sponsor-fullname	The sponsor's full name.	—	—
sponsor-name	The sponsor's name.	—	—
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

When you specify the internal database as an authentication server, client information is checked against the user accounts in the internal database. You can modify an existing user account in the internal database with the **local-userdb modify** command, or delete an account with the **local-userdb del** command.

By default, the internal database in Mobility Master is used for authentication. Issue the **aaa authentication-server internal use-local-switch** command to use the internal database in a managed device; you then need to add user accounts to the internal database in the managed device.

Example

The following command adds a user account in the internal database with an automatically-generated username and password:

```
(host) [mynode] #local-userdb add generate-username generate-password expiry duration 480
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest4157
Password: cDFD1675
Expiration: 480 minutes
```

Related Commands

Command	Description
show local-userdb	Use this command to show the parameters displayed in the output of this command.
show local-userdb-guest	Use this command to show the parameters displayed in the output of the local-userdb-guest add command.
mgmt-user	Use the **webui-cacert <certificate name>** command if you want an external authentication server to derive the management user role. This is helpful if there are a large number of users who need to be authenticated. Use the **mgmt-user webui-cacert <certificate_name> serial <number> <username> <role>** command if you want the authentication process to use previously configured certificate name and serial number to derive the user role.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

local-userdb del

```
local-userdb
   del username <name>
         comments
         email
         expiry
         guest-company
         guest-fullname
         guest-phone
         mode
         opt-field-1
         opt-field-2
         opt-field-3
         opt-field-4
         remote-ip
         role
         sponsor-dept
         sponsor-email
         sponsor-fullname
         sponsor-name
         start-time
   del-all
```

Description

This command deletes entries in the Mobility Master's internal database.

Syntax

Parameter	Description	Range	Default
`del username`	Deletes the user account for the specified username.	—	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1–2147483647	—
`time`	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Aruba wireless network.	—	—
`guest-fullname`	The guest's full name.	—	—
`guest-phone`	The guest's phone number.	—	—
`mode`	Enables or disables the user account.	—	disabled

Parameter	Description	Range	Default
opt-field-1	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a “Supervisor.” You can enter username, full name, department and Email information into the optional fields.	—	—
opt-field-2	Same as **opt-field-1**.	—	—
opt-field-3	Same as **opt-field-1**.	—	—
opt-field-4	Same as **opt-field-1**.	—	—
remote-ip	IP address assigned to the remote peer.	—	—
role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.	—	guest
sponsor-dept	The guest sponsor’s department name. **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
sponsor-email	The sponsor’s email address.	—	—
sponsor-fullname	The sponsor’s full name.	—	—
sponsor-name	The sponsor’s name.	—	—
start-time	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.	—	—
del-all	Deletes all entries in the internal database.	—	—

Usage Guidelines

User account entries created with expiration are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Example

The following command deletes a specific user account entry:

```
(host) [mynode] #local-userdb del username guest4157
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master

local-userdb export

```
local-userdb export <filename>
```

Description

This command exports the internal database to a file.

Use this command with caution. It replaces the existing users with user entries from the imported file.

Syntax

Parameter	Description
`export`	Saves the internal database to the specified file in flash.

Usage Guidelines

After using this command, you can use the **copy** command to transfer the file from flash to another location.

Example

The following command saves the internal database to a file:

```
(host) [mynode] #local-userdb export jan-userdb
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform s	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

local-userdb import

```
local-userdb import <filename>
```

Description

This command replaces the internal database with the specified file from flash.

Syntax

Parameter	Description
`import`	Replaces the internal database with the specified file.

Usage Guidelines

This command replaces the contents of the internal database with the contents in the specified file. The file must be a valid internal database file saved with the **local-userdb export** command.

Example

The following command imports the specified file into the internal database:

```
(host) [mynode] #local-userdb import jan-userdb
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

local-userdb modify

```
local-userdb modify username <name>
   comments
   email
   expiry
   guest-company
   guest-fullname
   guest-phone
   mode
   opt-field-1
   opt-field-2
   opt-field-3
   opt-field-4
   remote-ip
   role
   sponsor-dept
   sponsor-email
   sponsor-fullname
   sponsor-name
   start-time
```

Description

This command modifies an existing user account entry in the Mobility Master's internal database.

Syntax

Parameter	Description	Range	Default
`username`	Name of the existing user account entry.	1–64 characters	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1–2147483647	—
`time`	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Aruba wireless network.	—	—
`guest-fullname`	The guest's full name.	—	—
`guest-phone`	The guest's phone number.	—	—
`mode`	Enables or disables the user account.	—	disabled

Parameter	Description	Range	Default
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a “Supervisor.” You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as **opt-field-1**.	—	—
`opt-field-3`	Same as **opt-field-1**.	—	—
`opt-field-4`	Same as **opt-field-1**.	—	—
`remote-ip`	IP address assigned to the remote peer.	—	—
`role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.	—	guest
`sponsor-dept`	The guest sponsor’s department name. **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor’s email address.	—	—
`sponsor-fullname`	The sponsor’s full name.	—	—
`start-time`	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

Use the **show local-userdb** command to view the current user account entries in the internal database.

Example

The following command disables an existing user account in the internal database:

```
(host) [mynode] #local-userdb modify username guest4157 mode disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

local-userdb-guest add

```
local-userdb-guest add
   generate-username {generate-password|password <passwd>}
      comments
      email
      expiry
      guest-company
      guest-fullname
      guest-phone
      mode
      opt-field-1
      opt-field-2
      opt-field-3
      opt-field-4
      remote-ip
      role
      sponsor-dept
      sponsor-email
      sponsor-fullname
      sponsor-name
      start-time
   username <name> {generate-password|password <passwd>}
      comments
      email
      expiry
      guest-company
      guest-fullname
      guest-phone
      mode
      opt-field-1
      opt-field-2
      opt-field-3
      opt-field-4
      remote-ip
      role
      sponsor-dept
      sponsor-email
      sponsor-fullname
      sponsor-name
      start-time
```

Description

This command creates a guest user in a local user database.

Syntax

Parameter	Description	Range	Default
`generate-username`	Automatically generate and add a guest username.	—	—
`username`	Add the specified guest username.	1–64 characters	—

Parameter	Description	Range	Default
`generate-password`	Automatically generate a password for the username.	—	—
`password`	Add the specified password for the username.	6–128 characters	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1–2147483647	—
`time`	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Aruba wireless network.	—	—
`guest-fullname`	The guest's full name.	—	—
`guest-phone`	The guest's phone number.	—	—
`mode`	Enables or disables the user account.	—	disabled
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as **opt-field-1**.	—	—
`opt-field-3`	Same as **opt-field-1**.	—	—
`opt-field-4`	Same as **opt-field-1**.	—	—
`remote-ip`	IP address assigned to the remote peer.	—	—
`role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.	—	guest
`sponsor-dept`	The guest sponsor's department name. **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor's email address.	—	—
`sponsor-fullname`	The sponsor's full name.	—	—

Parameter	Description	Range	Default
`sponsor-name`	The sponsor's name.	—	—
`start-time`	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

When you specify the internal database as an authentication server, client information is checked against the user accounts in the internal database. You can modify an existing user account in the internal database with the **local-userdb-guest modify** command, or delete an account with the **local-userdb-guest del** command.

By default, the internal database in the Mobility Master is used for authentication. Issue the **aaa authentication-server internal use-local-switch** command to use the internal database in a managed device you then need to add user accounts to the internal database in the managed device.

Example

The following command adds a guest user in the internal database with an automatically-generated username and password:

```
(host) [mynode] #local-userdb-guest add generate-username generate-password expiry none
```

The following information is displayed when you enter the command:

```
GuestConnect
Username: guest-5433352
Password: mBgJ6764
Expiration: none
```

Related Commands

Command	Description
show local-userdb-guest	Show the parameter configured using the **local-userdb-guest** command.
show local-userdb	Show the parameters configured using the **local-userdb** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system. The **role** parameter requires the PEFNG license.	Enable mode on Mobility Master

local-userdb-guest del

```
local-userdb-guest {del username <name> | del-all}
```

Description

This command deletes entries in the controller's internal database.

Syntax

Parameter	Description
`del username`	Deletes the user account for the specified username.
`del-all`	Deletes all entries in the internal database.

Usage Guidelines

User account entries created with expiration detail are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Example

The following command deletes a specific user account entry:

```
(host) #local-userdb-guest del username guest4157
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config modes on Mobility Master

local-userdb-guest modify

```
local-userd-guest modify username <name> [comments <g_comments>][email <email>] [expiry
{duration <minutes>|time <mm/dd/yyyy> <hh:mm>}] [guest-company <g_company>][guest-fullname <g_
fullname>][guest-phone <g-phone>][mode disable][opt-field-1 <opt1>][opt-field-2 <opt2>][opt-
field-3 <opt3>][opt-field-4 <opt4>][password <passwd][sponsor-dept <sp_dept>][sponsor-mail
<sp_email>][sponsor-fullname <sp_fullname>][sponsor-name <sp_name>][start-time <mm/dd/yyyy>
<hh.mm>]
```

Description

This command modifies an existing guest user entry in the controller's internal database.

Syntax

Parameter	Description	Range	Default
`username`	Name of the existing user account entry.	1–64 characters	—
`comments`	Comments added to the user account.	—	—
`email`	Email address for the user account.	—	—
`expiry`	Expiration for the user account. If this is not set, the account does not expire.	—	no expiration
`duration`	Duration, in minutes, for the user account.	1–2147483647	—
`time`	Date and time, in mm/dd/yyyy and hh:mm format, that the user account expires.	—	—
`guest-company`	Name of the guest's company. **NOTE:** A guest is the person who needs guest access to the company's Aruba wireless network.	—	—
`guest-fullname`	The guest's full name.	—	—
`guest-phone`	The guest's phone number.	—	—
`mode`	Enables or disables the user account.	—	Disable
`opt-field-1`	This category can be used for some other purpose. For example, the optional category fields can be used for another person, such as a "Supervisor." You can enter username, full name, department and Email information into the optional fields.	—	—
`opt-field-2`	Same as **opt-field-1**.	—	—
`opt-field-3`	Same as **opt-field-1**.	—	—
`opt-field-4`	Same as **opt-field-1**.	—	—
`password`	User's password.	1–6 characters	—

Parameter	Description	Range	Default
`sponsor-dept`	The guest sponsor's department name. **NOTE:** A sponsor is the guest's primary contact for the visit.	—	—
`sponsor-email`	The sponsor's email address.	—	—
`sponsor-fullname`	The sponsor's full name.	—	—
`sponsor-name`	The sponsor's name.	—	—
`start-time`	Date and time, in mm/dd/yyyy and hh:mm format, the guest account begins.	—	—

Usage Guidelines

Use the **show local-userdb-guest** command to view the current user account entries in the internal database.

Example

The following command disables a guest user account in the internal database:

```
(host) #local-userdb-guest modify username guest4157 mode disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and config modes on Mobility Master

local-userdb-guest send-email

```
local-userdb-guest send-email <username> [to-guest][to-sponsor]
```

Description

This command causes the controller to send email to the guest or sponsor any time a guest user is created.

Syntax

Parameter	Description	Range	Default
`<username>`	Name of the guest.	1–64 characters	—
`to-guest`	Allows you to send email to the guest user's address.	—	—
`to-sponsor`	Allows you to send email to the sponsor's email address.	—	—

Usage Guidelines

This command allows the guest provisioning user or network administrator to causes the controller to send email to the guest or sponsor any time a guest user is created.

Example

The following command causes the controller to send an email to the sponsor alerting them that the guest user "Laura" was just created.

```
(host)# local-userdb-guest send-email Laura to-sponsor
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

local-userdb-public-access

```
local-userdb
   del username <name>
   del-all
```

Description

This command deletes guest entries in the Mobility Master's internal database.

Syntax

Parameter	Description	Range	Default
`del username`	Deletes a guest user account for the specified username.	—	—
`del-all`	Deletes all guest entries in the internal database.	—	—

Usage Guidelines

User account entries created with expiration are automatically deleted from the internal database at the specified expiration. Use this command to delete an entry before its expiration or to delete an entry that was created without an expiration.

Example

The following command deletes a specific guest account entry:

```
(host) [mynode] #local-userdb-public-access del username guest4157
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

local-userdb maximum-expiration

```
local-userdb maximum-expiration <expmins>
```

Description

This command configures the maximum time, in minutes, that a guest account in the internal database can remain valid.

Syntax

Parameter	Description	Range
`maximum-expiration`	Maximum time, in minutes, that a guest account in the internal database can remain valid.	1-3000000

Usage Guidelines

The user in the guest-provisioning role cannot create guest accounts that expire beyond the configured maximum time. This command is not available to the user in the guest-provisioning role.

Example

The following command sets the maximum time for guest accounts in the internal database to 8 hours (480 minutes):

```
(host) [/md] (config) #local-userdb maximum-expiration 480
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

local-userdb send-to-guest

```
local-userdb send-to-guest
```

Description

This command automatically sends email to the guest when the guest user is created.

Syntax

No parameters.

Usage Guidelines

A guest is the person who needs guest access to the company's Aruba wireless network. Email is sent directly to the guest after the guest user is created. When configuring the guest provisioning feature, the guest user is generally created by Guest Provisioning user. This is the person who is responsible for signing in guests at your company.

Example

```
(host) [mynode] (config) #local-userdb send-to-guest
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

local-userdb send-to-sponsor

```
local-userdb send-to-sponsor
```

Description

This command automatically sends email to the guest's sponsor when the guest user is created.

Syntax

No parameters.

Usage Guidelines

The sponsor is the guest's primary contact. Email is sent directly to the guest's sponsor after the guest user is created. When configuring the guest provisioning feature, the sponsor is generally created by the Guest Provisioning user. This is the person who responsible for signing in guests at your company.

Example

```
(host) [mynode] (config)#local-userdb send-to-sponsor
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

location

```
location <switchlocation>
```

Description

This command configures the location of the managed device.

Syntax

Parameter	Description
`switchlocation`	A text string that specifies the location of the switch.

Usage Guidelines

Use this command to indicate the location of the managed device. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter "" at the prompt.

Example

The following command configures the location:

```
(host) [mynode] (config) #location "Building 10, second floor, room 21E"
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

location-server-feed

```
enable
disable
```

Description

This command allows sends RSSI information from APs to a location management server.

Syntax

Parameter	Description
`enable`	Enable the feed that sends RSSI information to a location management server. This feature is disabled by default.
`disable`	Disable the feed that sends RSSI information to a location management server. This feature is disabled by default.

Usage Guidelines

This command allows APs to send RSSI information to a location management server, which can use that information to compute the location of stations seen in the network.

Example

The following command configures the location:

```
(host) [mynode] (config) #location-server-feed enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

logging

```
logging [ap-debug|arm|arm-user-debug|facility|network|security|system|user|user-
debug|wireless|<ipv4addr>|<ipv6addr>]
```

Description

Use this command to specify the IP address of the remote logging server, facility, severity, and the type.

Syntax

Parameter	Description	Range	Default
`ap-debug`	AP troubleshooting messages. You must specify a debug value.	–	–
`arm`	ARM messages.	–	–
`arm-user-debug`	ARM user troubleshooting messages. You must specify a MAC address.	–	–
`facility`	Set the facility to be used when logging to the remote syslog server. The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages.	local 0 to local 7	—
`network`	Network messages.	–	–
`security`	Security messages.	–	–
`system`	System messages.	–	–
`user`	User messages.	–	–
`user-debug`	User troubleshooting messages. You must specify a MAC address.	–	–
`wireless`	Wireless messages.	–	–
`<ipv4addr>`	To set the remote logging server IPv4 address.	–	A.B.C.D
`facility`	The facility to be used when logging to a remote syslog server.	local0 to local7	–
`format`	The format of the logs when logging to a remote syslog server. ■ cef - Common Event Fformat ■ bsd-standard - Berkeley Software Distribution standard or RFC-3164 format	–	–

Parameter	Description	Range	Default
severity	Set the remote logging server severity to: ■ alerts - Immediate action required ■ critical - Critical Condition ■ debugging - Debug Messages ■ emergencies - System is unusable ■ errors - Error Conditions in the system ■ informational - Informational Messages ■ notifications - Normal but significant condition ■ warnings - Warning condition	–	–
type	Set the remote logging server message type to: ■ ap-debug - AP Debug Logs ■ arm - ARM logs ■ arm-user-debug - ARM User Debug Logs ■ network - Network logs ■ security - Security logs ■ system - System logs ■ user- User logs ■ user-debug - User Debug Logs ■ wireless - Wireless logs	–	–
<ipv6addr>	To set the remote logging server IPv6 address.	–	X:X:X:X::X
facility	The facility to be used when logging to a remote syslog server.	local0 to local7	–
format	The format of the logs when logging to a remote syslog server. ■ cef - Common Event Fformat ■ bsd-standard - Berkeley Software Distribution standard or RFC-3164 format	–	–
severity	Set the remote logging server severity to: ■ alerts - Immediate action required ■ critical - Critical Condition ■ debugging - Debug Messages ■ emergencies - System is unusable ■ errors - Error Conditions in the system ■ informational - Informational Messages ■ notifications - Normal but significant condition ■ warnings - Warning condition	–	–
type	Set the remote logging server message type to: ■ ap-debug - AP Debug Logs ■ arm - ARM logs ■ arm-user-debug - ARM User Debug Logs ■ network - Network logs ■ security - Security logs ■ system - System logs ■ user- User logs ■ user-debug - User Debug Logs ■ wireless - Wireless logs	–	–

Parameter	Description	Range	Default
`<level>`	The message severity level, which can be one of the following (in order of severity level): ■ alerts - Any condition requiring immediate attention and correction. ■ critical - Any critical conditions, such as hard drive errors. ■ debugging - Messages containing information for debugging purposes. ■ emergencies - Panic conditions that occur when the system becomes unstable. ■ errors - Error conditions. ■ informational - Significant events of a non-critical and normal nature. ■ notifications - Normal but significant condition. ■ warnings - Warning messages.		

Parameter	Description	Range	Default
`process`	Controller process, which can be one of the following: ■ aaa - AAA logging ■ activate - Integration and communication with an Activate server ■ amon_recvr - AMON receiver ■ amon_sender - AMON sender ■ apprf - APPRF feature ■ approc - AP processes ■ armd - ARM processes ■ authmgr - User authentication ■ ble_relay - BLE relay process ■ bocmgr - BOC manager process ■ cert_dwnld - Certificate download process ■ certmgr - Certificate manager ■ cfgdist - Config Distributor ■ cfgm - Configuration Manager ■ cli - Command Line Interface ■ cluster_mgr - Cluster Manager ■ cpsec - Control plane security ■ crypto - VPN (IKE/IPsec) ■ cts - Transport service ■ dbsync - Database synchronization ■ dds - Logging for DDS processes ■ dhcpd - DHCP packets ■ dpagent - DPAGENT process ■ esi - External Services Interface ■ extifmgr - External Interface Manager ■ fpapps - Layer 2 and 3 control ■ fw_visibility - Firewall visibility processes ■ gsmmgr - GSM manager ■ ha_mgr - High availability manager ■ hcm - Health check process ■ httpd - Apache process ■ hwmon - Hardware monitoring ■ iapmgr - Instant AP manager process ■ ip_flow_export - IP Flow Export process ■ ipstm - Instant station manager process ■ l2tp - L2TP ■ lagm - Logging for lagm process ■ licensemgr - License manager ■ lldp - LLDP process ■ localdb - Local database ■ mdns - Multicast DNS proxy ■ mobileip - Mobile IP ■ mon_serv - mon_serv process ■ mon_serv_fwv - mon_serv_fwv process ■ npppd - NPPPD ■ ofa - OpenFlow Agent Process ■ ospf - OSPF logging ■ packetfilter - Packet filtering of messaging and control frames ■ phonehome - PhoneHome ■ pim - Protocol Independent Multicast ■ pppd - PPP ■ pppoed - PPPoE ■ pptp - PPTP ■ processes - Run-time process		

Parameter	Description	Range	Default
	■ profmgr - Profile Manager ■ publisher - Publish subscribe service ■ radvd - RA daemon ■ resolvwrap - Resolve wrap process ■ rfm - RF Troubleshooting Manager ■ rng-mgr - RNG Manager ■ rsync - Rsync ■ rtpa - RTPA process ■ sc_replication_mgr - SC Replication Manager ■ snmp - SNMP ■ spectrum - Spectrum analysis processes ■ stm - Station management ■ survival - Auth survival ■ syslogdwrap - Syslogd wrap ■ traffic - Traffic process ■ ucm - Unified Communication and Collaboration processes ■ upgrademgr - Upgrade Manager ■ util-proc - Util process ■ vrrp - Logging for vrrp process ■ web_cc - Web Content classification ■ webd - Web Daemon. ■ wms - Wireless management		
`subcat`	Message subcategory, which depends upon the message category specified. The following lists the subcategories available for each message category: ■ ap-debug: all, ap-config, ha, sdn ■ arm: all, client-match, radio-mgmt ■ arm-user-debug: all ■ network: all, cluster, dhcp, gp, mobility, packet-dump, sdn ■ security: aaa, all, auth-amon, certinit, certmgr, cluster, cpnw, cpsec, db, 802.1X, firewall, HA, ids, ids-ap, ike, kerberos, mobility, packet-trace, vpn, webserver, wl-sync ■ system: all, amon, amon-ale, amon-amp, ap, ap-config, cluster, configuration, cpnw, gp, ha, mapc, messages, ofc-event-dispatcher, ofc-flow-manager, ofc-packet-dispatcher, ofc-routing-switch, ofc-switch-manager, ofc-topology, ofc-topology-discovery, pan, reg-tbl, snmp, validation, webserver ■ user: all, captive-portal, client-match, cpnw, 802.1X, mapc, pan, radius, vpn ■ user-debug: all, configuration ■ wireless: all		

Usage Guidelines

The local use facilities (local0, local1, local2, local3, local4, local5, local6, and local7) are not reserved for specific message-generating sources, and can be used for sending syslog messages. Use the show logging command to verify that the device sends logging messages.

There are eight logging severity levels, each with its associated types of messages. Each level also includes the levels below it. For example, if you set the logging level to informational (6), all messages from level 0 through level 5 (from emergencies through notifications) are also logged. The warnings severity level is set by default for all message categories.

Only the **logging level warnings security subcat ids** and **logging level warnings security subcat ids-ap** subcategories are enabled by default. Other subcategories are not generated by default even their severity is **warning** or higher. Issue the **logging level** command to enable all other message subcategories.

Example

The following command adds the remote logging server with the IP address 10.1.2.3 with a user log type using local4.

```
(host) [mynode] (config) #logging 10.1.2.3 facility local4
```

Command History

Release	Modification
ArubaOS 8.2.0.0	New system processes called **vrrp** and **lagm** are added to debug issues related to the vrrp process and lagm process.
ArubaOS 8.1.0.0	The **logging level <severity>** was moved to the end of the command string. The **format** parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system.	Config mode on Mobility Master.

logging-trace-files

```
logging-trace-files
```

Description

Use this command to enable or disable the slog_flash application.

Usage Guidelines

The slog_flash application continuously updates log files to the USB storage. An error occurs when the USB storage is removed when the update is in progress. This command is introduced to prompt the user before removing the external USB, to avoid this error.

Example

The following command disables slog_flash app.

```
(host) [mynode] #no logging-trace-files
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
7200 Series, 7030, and 7010	Base operating system.	Config mode on Mobility Master.

loginsession

```
loginsession timeout <minutes>
```

Description

This command configures the time management session (via Telnet or SSH) remains active without user activity.

Syntax

Parameter	Description	Range	Default
`timeout`	Number of seconds or minutes that a management session remains active without any user activity.	5-60 minutes or 1-3600 seconds, 0 to disable	15 minutes

Usage Guidelines

The management user must re-login to the controller after a Telnet or SSH session times out. If you set the timeout value to 0, sessions do not time out. The TCP session timeout for wireless and wired user sessions through the controller is 15 minutes; this timeout for user sessions is not configurable.

Example:

The following command configures management sessions on the controller to not time out:

```
(host) [mynode] (config) #loginsession timeout 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license.	Config mode on Mobility Master.

logon

```
logon <device-ip>
```

Description

This command remotely logs in to the managed device CLI from the Mobility Master CLI.

ArubaOS 8.x does not support this command in the master controller mode.

Syntax

Parameter	Description
`device-ip`	IP address of the managed device.

Usage Guidelines

Ensure that the managed device is reachable from Mobility Master.

Example

This command remotely logs in to the managed device CLI from the Mobility Master CLI.

```
(host) [mynode] (config) #logon 192.0.2.38
Last login: Wed Jun 29 08:23:33 2016 from 192.0.2.34
(host-md) #
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

mac-address-table

```
mac-address-table static <macaddr> gigabitethernet <slot/module/port> vlan <vlan>
```

Description

This command adds a static entry to the MAC address table.

Syntax

Parameter	Description	Range
`<macaddr>`	MAC address, in the format xx:xx:xx:xx:xx:xx.	—
`<slot/module/port>`	Interface in <slot>/<module>/<port> format.	—
`vlan`	ID number of the VLAN.	1-4094

Usage Guidelines

The MAC address table is used to forward traffic between ports on the controller. The table includes addresses learned by the controller. This command allows you to manually enter static addresses that are bound to specific ports and VLANs.

Example

The following command configures a MAC address table entry:

```
(host) [mynode] (config) #mac-address-table static 00:0b:86:f0:05:60 gigabitethernet 0/0/12
vlan 22
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system.	Config mode on Mobility Master.

master-l3redundancy

```
master-l3redundancy
l3-peer-ip-address {<ipaddr> [ipsec <key>] [ipsec-custom-cert <peer-mac> <MAC address>]
[ipsec-factory-cert <peer-mac> <MAC address>]}
l3-sync-state {None|Primary|Secondary}
l3-sync-time <timer>
```

Description

Use this command to configure Layer-3 redundancy for a Mobility Master.

Syntax

Parameter	Description	Default
`l3-peer-ip-address`	Configure L3 peer's ip address.	—
`ipsec`	Configure IPsec secure communication between Mobility Masters.	—
`ipsec-custom-cert`	Customer certificate-based IPsec secure communication between Mobility Masters.	—
`ipsec-factory-cert`	Factory certificate-based IPsec secure communication between Mobility Masters.	—
`l3-sync-state`	Sync state for L3 Redundancy .	—
`None`	No Sync state for L3 Redundancy.	—
`Primary`	Set Sync state for L3 Redundancy as Primary.	—
`Secondary`	Set Sync state for L3 Redundancy as Secondary.	—
`l3-sync-time`	Sync Time for L3 Redundancy.	—
`timer`	Sync time in Hours. Value is between (2-24) hours.	2 hours

Usage Guidelines

This command enables the Layer-3 redundancy. Peer-ip and sync-state functions are required for proper functioning of L3 Redundancy. They have to be individually executed in **/mm/mynode** of all the Mobility Masters involved in the redundancy.

Example

The following command enables you to configure Layer-3 redundancy.

```
(host) *[mynode] (config) #master-l3redundancy
(host) *[mynode] (config-submode)# #l3-peer-ip-address
(host) *[mynode] (config-submode)#l3-sync-state
(host) *[mynode] (config-submode)#l3-sync-time
```

Related Commands

Command	Description
show master-l3redundancy	Displays the current status of Layer-3-domain Mobility Master redundancy.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on managed device.

master-redundancy master-vrrp

```
master-redundancy master-vrrp <id>
```

Description

This command associates a VRRP instance with Mobility Master redundancy.

Syntax

Parameter	Description	Range
<id>	The virtual router ID for the VRRP instance configured with the **vrrp** command.	1-255

Usage Guidelines

To maintain a highly redundant network, you can use a standby for Mobility Master. The underlying protocol used is VRRP which you configure using the **vrrp** command.

Example

The following command configures VRRP for the initially preferred Mobility Master:

```
(host)[mynode](config) #vrrp 22
   vlan 22
   ip address 10.200.22.254
   priority 110
   preempt
   description Preferred-Master
   tracking master-up-time 30 add 20
   no shutdown
master-redundancy
   master-vrrp 22
   peer-ip-address 192.168.2.1 ipsec qwerTY012
```

The following shows the corresponding VRRP configuration for the peer controller.

```
(host)[mynode](config) #vrrp 22
   vlan 22
   ip address 10.200.22.254
   priority 100
   preempt
   description Backup-Master
   tracking master-up-time 30 add 20
   no shutdown
master-redundancy
   master-vrrp 22
peer-ip-address 192.168.22.1 ipsec qwerTY012
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

masterip

```
masterip <ipaddr>
   ipsec <key> [fqdn <local-fqdn>] interface <uplink |{vlan <id>}] peer-mac-1 <peermac1
   ipsec-custom-cert master-mac-1-c <mac-1-c> ca-cert <ca> fqdn <fqdn> [interface uplink|{vlan
   <id>}] [master-mac-2-c <mac-2-c>] server-cert <cert> [suite-b gcm-128|gcm-256]
   ipsec-factory-cert master-mac-1 <mac>
   vpn-ip <vpnip>
```

Description

This command configures the IP address and PSK or certificate for the Mobility Master on a managed device.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the Mobility Master.
`ipsec <key>`	To establish the master-local IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
`fqdn`	Identify a dynamically addressed managed device by entering the FQDN of the controller.
`interface`	Specify the uplink or VLAN interface on the Mobility Master to initiate IKE.
`peer-mac-1`	Specify the peer MAC string. **NOTE:** If the peer device is an x86 server, then configure the MAC address of the management interface of the managed device. However, if the peer device is a hardware platform, you must provide the MAC address of the VLAN interface of the managed device.
`ipsec-custom-cert`	Use a custom-installed certificate on the Mobility Master to establish a master-local IPsec tunnel using IKEv2.
`master-mac-1 <mac-1-c>`	The MAC address of the certificate on the Mobility Master.
`master-mac-2 <mac-2-c>`	(Optional) the MAC address of the certificate on the Mobility Master.
`ca-cert <ca>`	User-defined name of a trusted CA certificate installed on the Mobility Master. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the controller.
`server-cert <cert>`	User-defined name of a server certificate installed on the Mobility Master. Use the show **crypto-local pki ServerCert** command to display the server certificates that have been imported into the controller.
`interface`	Specify the uplink or VLAN interface on the Mobility Master to initiate IKE.
`uplink`	Use the Mobility Master's current active uplink to initiate IKE.

Parameter	Description
vlan <id>	Specify a VLAN interface on the Mobility Master to initiate IKE. If you do not specify a VLAN, the controller IP will be used.
fqdn <fqdn>	Identify a dynamically addressed managed device by entering the FQDN of the controller.
suite-b	If you configure your Mobility Master and managed devices to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: ■ **gcm-128** Use 128-bit AES-GCM Suite-B encryption ■ **gcm-256** Use 256-bit AES-GCM Suite-B encryption
ipsec-factory-cert	Use the factory-installed certificate on the Mobility Master to establish a master-local IPsec tunnel using IKEv2.
master-mac-1 <mac-1-c>	The MAC address of the certificate on the Mobility Master.
master-mac-2 <mac-2-c>	(Optional) the MAC address of the certificate on the backup Mobility Master.
interface	Specify the uplink or VLAN interface on the Mobility Master to initiate IKE.
uplink	Use the Mobility Master's current active uplink to initiate IKE.
vlan <id>	Specify a VLAN interface on the Mobility Master to initiate IKE. If you do not specify a VLAN, the controller IP will be used.
fqdn <fqdn>	Identify a dynamically addressed managed device by entering the FQDN of the controller.
vpn-ip	Specify the IP address of the VPN concentrator.

Usage Guidelines

Use this command on a managed device to configure the IP address and PSK or certificate for secure communication with the Mobility Master. On the Mobility Master, use the **localip** command to configure the IP address and preshared key or certificate for a managed device.

The parameters in this command can also be defined using the initial setup wizard when the managed device is first configured. Best practices is to define masterip settings using this wizard. If the IP address of the Mobility Master on a managed device is changed the managed device should be rebooted.

If your Mobility Master and managed devices use a pre-shared key for authentication, they will create the IPsec tunnel using IKEv1. If your Mobility Master and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

Example

The following command configures the Mobility Master with a PSK:

```
(host) [mynode] (config) #masterip 10.1.1.250 ipsec gw1234567
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	The **suite-b gcm-128** and **suite-b gcm-256** encryption options for IPsec custom certificates requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Config mode on Mobility Master.

masteripv6

```
masteripv6 <masteripv6_val>
   ipsec <key> [fqdn <fqdn>][interface uplink|vlan <id>] masterip4 <masterip4_val> ]
   ipsec-custom-cert master-mac-1-c <mac-1-c> [master-mac2 <mac2>] ca-cert <ca> server-cert
   <cert> [interface uplink|{vlan <id>}] [fqdn <fqdn>] [suite-b gcm-128|gcm-256]
   ipsec-factory-cert master-mac-1 <MAC> [master-mac2 <mac2>] [interface uplink|{vlan <id>}]
   [fqdn <fqdn>]
```

Description

This command configures the IPv6 address and preshared key or certificate for the Mobility Master or a managed device.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the Mobility Master.
`ipsec <key>`	To establish the IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
`ipsec-custom-cert`	Use a custom-installed certificate on the Mobility Master to establish a IPsec tunnel using IKEv2.
`master-mac1 <mac1>`	The MAC address of the certificate on the Mobility Master.
`master-mac2 <mac2>`	(Optional) the MAC address of the certificate on the backup Mobility Master.
`ca-cert <ca>`	User-defined name of a trusted CA certificate installed on the Mobility Master. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the Mobility Master.
`server-cert <cert>`	User-defined name of a server certificate installed on the Mobility Master. Use the show **crypto-local pki ServerCert** command to display the server certificates that have been imported into the Mobility Master.
`interface`	Specify the uplink or VLAN interface on the Mobility Master to initiate IKE.
`uplink`	Use the Mobility Master's current active uplink to initiate IKE.
`vlan <id>`	Specify a VLAN interface on the Mobility Master to initiate IKE. If you do not specify a VLAN, the Mobility Master IP will be used.
`fqdn <fqdn>`	Identify a dynamically addressed managed device by entering the FQDN of the Mobility Master.
`suite-b`	If you configure your master and managed devices to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: ■ **gcm-128** Use 128-bit AES-GCM Suite-B encryption ■ **gcm-256** Use 256-bit AES-GCM Suite-B encryption
`ipsec-factory-cert`	Use the factory-installed certificate on the Mobility Master to establish a master-local IPsec tunnel using IKEv2.

Parameter	Description
`master-mac1 <mac1>`	The MAC address of the certificate on the Master.
`master-mac2 <mac2>`	(Optional) the MAC address of the certificate on the backup Mobility Master.
`interface`	Specify the uplink or VLAN interface on the Mobility Master to initiate IKE.
`uplink`	Use the Mobility Master's current active uplink to initiate IKE.
`vlan <id>`	Specify a VLAN interface on the Mobility Master to initiate IKE. If you do not specify a VLAN, the managed device IP will be used.
`fqdn <fqdn>`	Identify a dynamically addressed managed device by entering the FQDN of the managed device.

Usage Guidelines

Use this command on a managed device to configure the IP address and preshared key or certificate for secure communication with the Mobility Master. On the Mobility Master, use the **localip** command to configure the IP address and pre-shared key or certificate for a managed device.

Changing the IP address of the master on a managed device requires a reboot of the managed device.

If your Mobility Master and managed devices use a pre-shared key for authentication, they will create the IPsec tunnel using IKEv1. If your Mobility Master and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

Example

The following command configures the Mobility Master with a pre-shared key:

```
(host) [00:0b:86:dd:87:00] (config) #masteripv6 2001::1 ipsec Aruba@123 masteripv4 10.20.1.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The **suite-b gcm-128** and **suite-b gcm-256** encryption options for IPsec custom certificates requires the Advanced Cryptography (ACR) license. All other parameters are available in the base operating system.	Available in the config mode on Mobility Master.

master-redundancy peer-ip

```
master-redundancy peer-ip <ipaddr>
   ipsec <key>
   ipsec-custom-cert peer-mac <mac> ca-cert <ca> server-cert <sc> [suite-b gcm128|gcm256]
   ipsec-factory-cert peer-mac <mac>
```

Description

This command configures the IP address and PSK or certificate for a redundant Mobility Master on another Mobility Master.

Syntax

Parameter	Description
`<ipaddr>`	IP address of the redundant controller. Use the 0.0.0.0 address to configure a global preshared key for all inter-controller communications.
`ipsec <key>`	To establish the master-master IPsec tunnel using IKEv1, enter a preshared key between 6-64 characters.
`ipsec-custom-cert`	Use a custom-installed certificate on the controller to establish the master-master IPsec tunnel using IKEv2
`peer-mac <mac>`	The peer MAC address of the certificate on the redundant Mobility Master.
`ca-cert <ca>`	User-defined name of a trusted CA certificate installed on the redundant Mobility Master. Use the **show crypto-local pki TrustedCA** command to display the CA certificates that have been imported into the controller.
`server-cert <cert>`	User-defined name of a server certificate installed on on the redundant Mobility Master. Use the show **crypto-local pki ServerCert** command to display the server certificates that have been imported into the controller.
`suite-b`	If you configure your Mobility Master to use IKEv2 and custom-installed certificates, you can optionally use Suite-B cryptographic algorithms for IPsec encryption. Specify one of the following options: ■ **gcm-128** Use 128-bit AES-GCM Suite-B encryption ■ **gcm-256** Use 256-bit AES-GCM Suite-B encryption
`ipsec-factory-cert`	Use the factory-installed certificate on the Mobility Master to establish a master-local IPsec tunnel using IKEv2.
`peer-mac <mac>`	The MAC address of the certificate on the redundant Mobility Master.

Usage Guidelines

Use this command on a Mobility Master to configure the IP address and preshared key or certificates for communication with a redundant Mobility Master.

If your Mobility Master uses a pre-shared key for authentication, it will create the IPsec tunnel using IKEv1. If your Mobility Master and managed devices use certificates for authentication, the IPsec tunnel will be created using IKEv2.

Example

The following command configures the managed device on a Mobility Master:

```
(host) [mynode] (config) #peer-ip 10.4.62.5 ipsec-custom-cert master-mac 00:02:2D:11:55:4D ca-cert cacert1 server-cert server1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	The **suite-b gcm-128** and **suite-b gcm-256** encryption options for IPsec custom certificates requires the Advanced Cryptography license. All other parameters are available in the base operating system.	Config mode on Mobility Master.

mdconnect

`mdconnect`

Description

This command allows a user to log in to a managed device without a username and password after logging in to a Mobility Master. Change the configuration node to a managed device and execute this command or **mdc**, its short-version to direct the session to the CLI prompt of the managed device. The keyword **MDC** is shown in the CLI prompt to distinguish the managed device and the Mobility Master. On the managed device, a user can exute only show commands.

Syntax

Parameter	Description
`mdconnect`	Log in to a managed device without a username and password.

Usage Guidelines

Use the **mdconnect** command to log in to a managed device without a username and password.

Example

The following command allows a user to log in to a managed device named **VMC** mapped to a device with MAC address 01:02:03:04:05:06:

```
(host) [mynode] #change-config-node VMC
(MM) [01:02:03:04:05:06] #mdconnect

Redirecting to Managed Device Shell
Last login: Wed Nov 2 08:37:48 2016 from X.X.X.X
(VMC) [MDC] #exit

Exiting Managed Device Shell
(MM) [01:02:03:04:05:06] (config) #
```

The following command allows a user to log in to a managed device with MAC address 0a:0b:0c:0d:0e:0f:

```
(host) [mynode] #change-config-node /md/0a:0b:0c:0d:0e:0f
(MM) [0a:0b:0c:0d:0e:0f] #mdconnect

Redirecting to Managed Device Shell
Last login: Wed Nov 2 08:38:48 2016 from X.X.X.X
(test) [MDC] #exit

Exiting Managed Device Shell
(MM) [0a:0b:0c:0d:0e:0f] (config) #
```

Related Commands

Command	Description
change-config-node	Displays the configuration node hierarchy.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

mgmt-server

```
mgmt-server
   primary-server <primary-server-ip> profile <profile-name> [secure] [transport
   {mix|udp|websocket}]
   profile
      default-acp
      default-ale
      default-amp
      default-controller
      <profile-name>
         airgroupinfo-enable
         clone <source>
         inline-ap-stats
         inline-auth-stats
         inline-dhcp-stats
         inline-dns-stats
         location-enable
         misc-enable
         monitored-info-del-enable
         monitored-info-enable
         monitored-info-snapshot-enable
         no
         sessions-enable
         stats-enable
         tag-enable
         uccmonitoring-enable
         wids-event-info-enable
```

Description

This command configures the management server profile.

Syntax

Parameter	Description
`primary-server <primary-server-ip> profile <profile-name> [secure|transport]`	Associate the Mobility Master to ALE server or an AirWave management server by entering the IPv4 or IPv6 address of the server and specifying a management configuration profile.
`secure`	Enabling this specifies that DTLS mode is used.
`transport`	This defines the type of transport mechanism.
`profile`	Configure a new management server profile on the Mobility Master or to edit the default profiles.
`airgroupinfo-enable`	If enabled, the messages related to the AirGroup feature will be sent to the management server.
`clone <source>`	Copy from another management configuration profile.
`inline-ap-stats`	Enable Clarity Live statistics from the AP.

Parameter	Description
inline-auth-stats	Enable Clarity Live statistics related to authentication.
inline-dhcp-stats	Enable Clarity Live statistics of DHCP.
inline-dns-stats	Enable Clarity Live statistics of DNS.
location-enable	If enabled, Station RSSI or AP Neighbor messages will be sent to the management server.
misc-enable	If enabled, the AP system statistics, specifications, and station steer information will be sent to the management server.
monitored-info-del-enable	Information is sent when a monitored AP or client is deleted.
monitored-info-enable	If enabled, the monitored AP or station information will be sent to the management server.
monitored-info-snapshot-enable	If enabled, the managed device sends a periodic snapshot about the state (up or down) of each monitored AP, client, rogue AP, or suspected rogue AP.
no	Negates or removes a parameter.
sessions-enable	If enabled, the firewall DNA, application, and aggregate session messages will be sent to the management server.
stats-enable	If enabled, the statistics for AP radios, virtual APs, and clients are be sent to the management server.
tag-enable	If enabled, tag messages will be sent to the management server.
uccmonitoring-enable	If enabled, the messages about the unified communications manager are be sent to the management server.
wids-event-info-enable	If enabled, the controller sends messages about current IDS events as soon as they are detected.

Usage Guideline

Register a management server with the Mobility Master by specifying the IP address of an AirWave management server or ALE that should receive messages from the Mobility Master using the AMON protocol. You must also specify the management configuration profile in which the AMON message filtering settings can be done. The default profiles provided for the AirWave server (default-amp) and ALE (default-ale) are editable using this command.

The IDS WLAN management system (WMS) on the managed device monitors wireless traffic to detect any new AP or wireless client station that tries to connect to the network. ArubaOS can send Clarity Live and user serviceability statistics from a managed device to a management server, which can use this data to identify the client connectivity issues.

A managed device can also collect information about each step in the use authentication process, and send these records to a management server in the AMON format, the data transport protocol used to communicate basic statistics or state changes to the management servers such as AirWave or ALE.

Example

The following command defines a primary AirWave Management server.

```
(host) [mynode] (config) #mgmt-server primary-server 192.0.2.10 profile default-amp
```

Related Commands

Command	Description
ids management-profile	Manage the events correlation for IDS event traps and syslogs (logs).
ids wms-local-system-profile	This command configures the WLAN management system (WMS) service to terminate on individual managed devices instead of Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The following changes were introduced: ■ The **primary-server** parameter was modified to accept IPv6 address. ■ The Clarity Live parameters such as **inline-ap-stats**, **inline-auth-stats**, **inline-dhcp-stats**, and **inline-dns-stats** were introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master

mgmt-user

```
mgmt-user
   console-blocks
   localauth <username>
   ssh-pubkey
      client-cert <certname> <username>
      <role> [<rcp>]
   webui-cacert <certificate_name> [serial <number>] <username> <role> [<rcp>]
   <username> <rolename> [node <path>] <password>
```

Description

This command configures an administrative user.

Syntax

Parameter	Description	Default
`console-blocks`	Blocks serial console access once the user logs out.	—
`localauth <username>`	Enables the authentication of management users based on the results returned by the authentication server. To disable this setting, use the **no mgmt-user localauth** command. To verify if authentication of local management user accounts is enabled or disabled, use the following command: **show mgmt-user local-authentication-mode**	—
`ssh-pubkey`	Configures certificate authentication of administrative users using the CLI through SSH.	—
`client-cert`	Name of the X.509 client certificate for authenticating administrative users using SSH.	—
`<username>`	Name of the user.	—
`<role>`	Role assigned to the authenticated user.	—
`<rcp>`	Revocation Checkpoint for the ssh user's client certificate. The rcp checks the revocation status of the SSH user's client certificate before permitting access.	—
`webui-cacert`	The client certificate for authenticating administrative users using the WebUI.	—
`<certificate_name>`	The name of the CA certificate. If configured, certificate authentication and authorization are automatically completed using an authentication server.	—
`serial`	Serial number of the client certificate.	—
`<username>`	Name of the user.	—
`<role>`	Role assigned to the authenticated user.	—

Parameter	Description	Default
<rcp>	Revocation Checkpoint for the ssh user's client certificate. The rcp checks the revocation status of the SSH user's client certificate before permitting access.	—
<username>	Name of the user. You can create a maximum of 10 management users. **NOTE:** If you configure a root management user, you can use special characters except for double-byte characters.	—
<rolename>	Role assigned to the user. Predefined roles include: ■ guest-provisioning: Allows the user to create guest accounts on a special WebUI page. ■ location-api-mgmt: Permits access to location API information. You can log into the CLI; however, you cannot use any CLI commands. ■ network-operations: Permits access to Monitoring, Reports, and Events pages in the WebUI. You can log into the CLI; however, you can only use a subset of CLI commands to monitor the controller. ■ read-only: Permits access to CLI show commands or WebUI monitoring pages only. ■ root: Permits access to all management functions on the controller. ■ standard: This role has root privileges but cannot make changes to the management users.	—
node	Configures node level permissions. Use this parameter when you want to configure an authenticated user assigned to a role in the managed device.	—
<path>	Path of the managed device.	—
<password>	**NOTE:** You are prompted for the <password> for this user after you type in <role> and press Enter. The password must have a minimum of six characters. You can use special characters in the management user password. The restrictions are as follows: ■ You cannot use double-byte characters ■ You cannot use the question mark (?) ■ You cannot use white space <space >	—

Usage Guidelines

You can configure client certificate authentication of WebUI or SSH management users (by default, only username/password is used). To configure certificate authentication for the WebUI or SSH, use the web-server mgmt-auth certificate or ssh mgmt-auth public-key commands, respectively.

Use **webui-cacert <certificate name>** command if you want an external authentication server to derive the management user role. This is helpful if there are a large number of users who need to be authenticated.

Use the **mgmt-user webui-cacert <certificate_name> serial <number> <username> <role>** if you want the authentication process to use previously configured certificate name and serial number to derive the user role.

Use the **mgmt-user webui-cacert <certificate_name> serial <number> <username> <role> <rcp>** command if you want to configure an optional RCP for an ssh-pubkey user.

Use the **mgmt-user <username> <rolename> node <path> <password>** to configure an authenticated user assigned to a role in the managed device.

Example

The following command configures a management user and role:

```
(host)[node](config) #mgmt-user testuser1 root
Password: *****
Re-Type password: *****
```

Related Commands

Version	Modification
show mgmt-users	Displays a list of management users on the Mobility Master and details of each management user.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The **node** parameter was introduced in the **mgmt-user <username> <rolename>** command.
ArubaOS 8.1.0.0	The **standard** role was introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master .

mobility-manager

```
mobility-manager <A.B.C.D> [user <word>] <string> [auth-prot {md5 | sha} <srting>] [interval
<secs>] [retrycount <count>] [rtls <rtls-portnumber>] [trap-version {1 | 2c | 3}] [udp-port
<portnumber>]
```

Description

Use the command to allow a managed device to communicate with a mobility manager server (MMS).

Syntax

Parameter	Description	Range	Default
`<A.B.C.D>`	Configures the IP address of the mobility manager server for the managed device to communicate with.	—	—
`user <word> <string>`	Configures the username and password to communicate with MMS.	■ Username: string of length 1–31 ■ Password: string of length 1–31	—
`auth-prot {md5 | sha} <string>`	Configures authentication protocol of the user with password. ■ md5: HMAC-MD5-96 Digest Authentication Protocol ■ sha: HMAC-SHA-96 Digest Authentication Protocol	—	—
`interval <secs>`	Configures the time it takes for a UDP packet to travel to and from the trap server (round-trip time). This value indicates the timeout.	0–65535	0
`priv-prot`	Configures the privacy protocol of the user. ■ AES: CFB128-AES-128 Symmetric Encryption Protocol ■ DES: CBC-DES Symmetric Encryption Protocol	—	—
`retrycount <count>`	Configures the maximum number of retries allowed to authenticate with MMS.	0–256	0
`rtls <rtls-portnumber>`	Configures the UDP port number for RTLS data collection.	string of length 1–256	8000

Parameter	Description	Range	Default
`trap-version {1 | 2c | 3}`	Configures trap server's SNMP version.	1, 2c, or 3	—
`udp-port <portnumber>`	Configures trap server's UDP port number.	1–65535	162

Usage Guidelines

To configure a username and password for the managed device to communicate with MMS, execute the following command:

```
(host) [mm] (config) #mobility-manager 1.1.1.1 user testUN1 testUN1
```

The interval time, retry count, RTLS port number, and UDP port number are optional parameters that can be configured using the **mobility-manager** command.

If you try to configure a third mobility manager server, the following message is displayed:

`Maximum number of 2 MMS servers already configured.`

Example

The following command is an example to configure MMS and allow a managed device to communicate with it:

```
(host) [mm] (config) #mobility-manager 1.1.1.1 user testUN1 testUN1 auth-prot md5 authpswd
interval 250
```

Related Commands

Command	Description
show mobility-managers	This command displays information of MMS.

Command History

Release	Modification
ArubaOS 8.0.0.0	This command was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

mon-serv-toggle-amon-traffic-filter

```
[no] mon-serv-toggle-amon-traffic-filter
```

Description

Enable AMON traffic filter.

Syntax

No parameters.

Usage Guidelines

Issue the **no mon-serv-toggle-amon-traffic-filter** command to disable AMON UDP and re-enable it again using the command **mon-serv-toggle-amon-traffic-filter**

Example

The example below enables AMON traffic filter.

```
(host) [mynode] (config) #mon-serv-toggle-amon-traffic-filter
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

netdestination

```
netdestination <dstname>
   description <description6>
   host <ipaddr> [position <number>] {vlan <vlanID> | offset <offset No>}
   invert
   name <host_name>
   network <ipaddr> <netmask> [position <number>]
   no ...
   range <start-ipaddr> <end-ipaddr> [position <number>]
```

Description

This command configures an alias for an IPv4 network host, subnetwork, or range of addresses.

Syntax

Parameter	Description
`<dstname>`	Name for this host or domain. Maximum length is 63 characters.
`description`	Description about the this destination up to 128 characters long.
`host`	Configures a single IPv4 host and its position in the list. It also provides a sub command, **vlan – offset** to allow local net destination override.
`invert`	Specifies that the inverse of the network addresses configured are used. For example, if a network of 172.16.0.0 255.255.0.0 is configured, this parameter specifies that the alias matches everything except this subnetwork.
`name`	Use the **name** parameter to specify a domain or host name inside the netdestination object. Wildcards are supported through the asterisk (*) symbol, with the limitations described in the examples below. ■ A wildcard '*' is allowed only once and only in the beginning of the host or domain name. (For instance, ***.example.com** is allowed, but **example*.com** and ***example*.com** are not allowed.) ■ If the wildcard is applied to the host, the netdestination matches all hosts ending with that specific domain. (The name ***.example.com** matches all hosts ending with the domain **.example.com**, such as **demo.example.com**.) ■ If the wildcard is applied to the domain, the netdestination matches all hosts ending with that domain string. (The name ***example.com** matches all domains ending with **example.com**, such as **myexample.com** and **domainexample.com**.)
`network`	An IPv4 subnetwork consisting of an IP address and netmask.
`no`	Negates any configured parameter.
`range`	A range of IPv4 addresses consisting of sequential addresses between a lower and an upper value. The maximum number of addresses in the range is 16. If larger ranges are needed, convert the range into a subnetwork and use the **network** parameter.

Usage

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination it in multiple session ACLs. Once you configure an alias, you can use it to manage network

and host destinations from a central configuration point, because all policies that reference the alias will be updated automatically when you change the alias.

When using the **invert** option, use caution when defining multiple aliases, as entries are processed one at a time. As an example, consider a netdestination configured with the following two network hosts:

```
netdestination dest1 invert
network 1.0.0.0 255.0.0.0
network 2.0.0.0 255.0.0.0
```

A frame from http://1.0.0.1 would match the first alias entry, (which allows everything except for 1.0.0.0/8) so the frame would be rejected. However, it would then be compared against the second alias, which allows everything except for 2.0.0.0/8, and the frame would be permitted.

Example

The following command configures an alias for an internal network:

```
(host)[node](config) #netdestination Internal
(host)[node](config-dest) #network 10.1.0.0 255.255.0.0
```

Example

The following command overrides the local network destination:

```
(host)[node](config #netdestination store
(host)[node](config-dest) #host vlan 55 offset 36
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the PEFNG license.	Config mode on Mobility Master .

netdestination6

```
netdestination6 <dstname>
   description <description6>
   host <ipaddr> [position <number>]
   invert
   name <host_name>
   network <ipaddr> <netmask> [position <number>]
   no ...
   range <start-ipaddr> <end-ipaddr> [position <number>]
```

Description

This command configures an alias for an IPv6 network host, subnetwork, or range of addresses.

Syntax

Parameter	Description
`<dstname>`	Name of the IPv6 destination host or subnetwork up to 63 characters long.
`description`	Description about the IPv6 netdestination up to 128 characters long.
`host`	Configures a single IPv6 host and position in the list.
`invert`	Specifies that the inverse of the network addresses configured are used. For example, if a network of fe80:0:0:0:0:0:ac10:0/128 is configured, this parameter specifies that the alias matches everything except this subnetwork.
`name`	Use the **name** parameter to specify a domain or host name inside the netdestination object. Wildcards are supported through the asterisk (*) symbol, with the limitations described in the examples below. ■ A wildcard '*' is allowed only once and only in the beginning of the host or domain name. (For instance, ***.example.com** is allowed, but **example*.com** and ***example*.com** are not allowed). ■ If the wildcard is applied to the host, the netdestination matches all hosts ending with that specific domain. (The name ***.example.com** matches all hosts ending with the domain **.example.com**, such as **demo.example.com**). ■ If the wildcard is applied to the domain, the netdestination matches all hosts ending with that domain string. (The name ***example.com** matches all domains ending with **example.com**, such as **myexample.com** and **domainexample.com**).
`network`	An IPv6 subnetwork consisting of an IP address and netmask.
`no`	Negates any configured parameter.
`range`	A range of IPv6 addresses consisting of sequential addresses between a lower and an upper value. The maximum number of addresses in the range is 16. If larger ranges are needed, convert the range into a sub-network and use the **network** parameter.

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the traffic source and/or destination. Once you configure an alias, you can use it in multiple session ACLs.

When using the **invert** option, use caution when defining multiple aliases, as entries are processed one at a time. As an example, consider a netdestination configured with the following two network hosts:

```
netdestination6 dest1 invert
network 2002:0:0:0:0:0:100:0/128
```

```
network 2002:0:0:0:0:0:200:0/128
```

A frame from http://1.0.0.1 would match the first alias entry, (which allows everything except for 2002:0:0:0:0:0:100:0/128) so the frame would be rejected. However, it would then be compared against the second alias, which allows everything except for 2002:0:0:0:0:0:200:0/128, and the frame would be permitted.

Example

The following command configures an alias for an internal network:

```
(host)[mynode](config) #netdestination6 Internal
(host)[mynode](config-submode) #network fe80:0:0:0:0:0:a01:0/128
```

The following example displays the use of extended scope of address range:

```
(host)[mynode](config) #netdestination6 ipv6-reserved-range
(host)[mynode](config-submode) #invert
(host)[mynode](config-submode) #network 2000::/3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the PEFNG license.	Config mode on Mobility Master

netexthdr

```
netexthdr <name>
   eh <eh-type> deny | permit
```

Description

This command allows you to edit the packet filter options in the extension header (EH).

Syntax

Parameter	Description	Default
`<-name>`	Specify the EH alias name.	default
`eh <eh-type>`	Specify one of the following EH types: ■ **<0-255>**: Matches the IPv6 next header type ■ **authentication**: Matches the IPv6 authentication header ■ **dest-option**: Matches the IPv6 destination-option header ■ **esp**: Matches the IPv6 encapsulation security payload header ■ **fragment**: Matches the IPv6 fragment header ■ **hop-by-hop**: Matches the IPv6 hop-by-hop header ■ **mobility**: Matches the IPv6 mobility header ■ **routing**: Matches the IPv6 routing header	—
`deny`	Denies the IPv6 packets matching the specified extended header type.	—
`permit`	Permits the IPv6 packets matching the specified extended header type. **NOTE:** By default, all the EH types are supported in the default EH.	—

Usage Guidelines

ArubaOS firewall is enhanced to process the IPv6 extension header (EH) to enable IPv6 packet filtering. You can filter the incoming IPv6 packets based on the EH type. You can edit the packet filter options in the default EH, using this command. By default, the default EH alias permits all EH types.

Example

The following command denies the IPv6 packets matching the specified extended header type in the default EH:

```
(host)[node](config #netexthdr default
(host)[node](config-exthdr) #eh authentication deny
```

Related Commands

```
(host) #show netexthdr <alias-name>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master .

netservice

```
netservice <name> <protocol>|tcp|udp {list <port>,<port>}|{<port> [<port>]}
[ALG <service>]
```

Description

This command configures an alias for network protocols.

Syntax

Parameter	Description	Range
`netservice`	Name for this alias.	—
`<protocol>`	IP protocol number.	0-255
`tcp`	Configure an alias for a TCP protocol	
`udp`	Configure an alias for a UDP protocol	
`list <port>,<port>`	Specify a list of non-contiguous port numbers, by entering up to six port numbers, separated by commas.	0-65535
`<port> [<port>]`	TCP or UDP port number. You can specify a single port number, or define a port range by specifying both the lower and upper port numbers.	0-65535
`ALG`	Application-level gateway (ALG) for this alias.	—
`<service>`	Specify one of the following service types: ■ **dhcp**: Service is DHCP ■ **dns**: Service is DNS ■ **facetime**: Service is Facetime ■ **ftp**: Service is FTP ■ **h323**: Service is H323 ■ **jabber**: Service for Jabber ■ **noe**: Service is Alcatel NOE ■ **rtsp**: Service is RTSP ■ **sccp**: Service is SCCP ■ **sip**: Service is SIP ■ **sips**: Service is Secure SIP ■ **svp**: Service is SVP ■ **tftp**: Service is TFTP ■ **vocera**: Service is VOCERA	

Usage Guidelines

Aliases can simplify configuration of session ACLs, as you can use an alias when specifying the network service. Once you configure an alias, you can use it in multiple session ACLs.

Example

The following command configures an alias for a network service:

```
(host)[mynode](config) #netservice HTTP tcp 80
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

no packet-capture

```
no packet-capture
  controlpath
  datapath
  destination
```

Description

This command disables packet capturing for debugging.

Syntax

Parameter	Description	Range	Default
`controlpath {interprocess {all | <ports>} | other | sysmsg {all | <opcodes>} | tcp {all | <ports>} | udp {all | <ports>}}`	Disables capturing following interprocess packets on control path: **interprocess {all | <ports>}**: Disables capturing packets on all or up to 10 comma separated ports. **other**: Disables capturing other types of packets. **sysmsg {all | <opcodes>}**: Disables capturing internal messaging packets on all or up to 10 comma separated ports. **tcp {all | <ports>}**: Disables capturing TCP packets on all or up to 10 comma separated ports. **udp {all | <ports>}**: Disables capturing UDP packets on all or up to 10 comma separated ports.	–	–

Parameter	Description	Range	Default
`datapath {ipsec {all-v4 | all-v6 | <peer-ip> | <peer-ipv6>} | wifi-client <mac-address> {all | decrypted | encrypted}}`	Disables capturing following packets on datapath: **ipsec {all-v4 | all-v6 | <peer-ip> | <peer-ipv6>}**: Disables capturing all IPsec packets from given peer (inner IPv4), all IPsec packets from given peer (inner IPv6), given peer (IPv4), or given peer (IPv6) address. **wifi-client <mac-address> {all | decrypted | encrypted}**: Disables capturing all IPsec packets, decrypted IPsec packets, or encrypted packets from given MAC address.	–	–
`destination {interface <slot/port> | ip-address <ipaddr> | local-filesystem}`	Disables capturing following packets on destination: **interface <slot/port>**: Stops sending captured packets to the slot/port of an interface. **ip-address <ipaddr>**: Stops sending captured packets to the given IP address of a remote destination. **local-filesystem**: Stops sending captured packets in pcap files.	–	–

Usage Guidelines

No packet capture disables capturing packets for debugging.

Example

Access the CLI and use the following command to disable other packet-capture:

```
(host) [mynode] #no packet-capture controlpath other
```

Access the CLI and use the following command to disable all packet-capture from a wifi-client:

```
(host) [md] #no packet-capture datapath wifi-client 00:1a:1e:aa:bb:cc
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

ntp

```
ntp
   authenticate
   authentication-key <keyid> {md5|sha1} <keyvalue>
   server {<ip>|<ip6>} {[iburst|key] <keyid>}
   server-mode
   source
   standalone
   trusted-key
```

Description

This command allows you to configure NTP options.

Syntax

Parameter	Description	Range	Default
`authenticate`	This parameter enables the controller to authenticate the NTP server before synchronizing local time with server. This helps identify secure servers from fraudulent servers. This command has to be enabled for NTP authentication to work.	—	—
`authentication-key`	This command configures a key identifier and secret key and adds them into the database. NTP authentication works with a symmetric key configured by user. The key is shared by the client (Aruba managed device) and an external NTP server.	—	—
`<key-id>`	The key identifier is a string that is shared by the client (Arubamanaged device) and an external NTP server. This value is added into the database.	—	—
`md5|sha1 <keyvalue>`	The key value is a secret string, which along with the key identifier, is used for authentication. This is added into the database.	—	—
`server`	This command configures an NTP server. You can configure the Mobility Master to set its system clock using NTP by specifying one or more NTP servers.	—	—
`<ip>/<ip6>`	IPv4/IPv6 address of the Peer.	—	—

Parameter	Description	Range	Default
iburst	(Optional) This parameter causes the Mobility Master to send up to ten queries within the first minute to the NTP server. This option is considered “aggressive” by some public NTP servers.	—	disabled
key <key-id>	This is the key identifier used to authenticate the NTP server. This needs to match the key identifier configured in the **ntp authentication-key** command.	—	—
server-mode [disable]	This command disables NTP server mode.	—	—
source	This command specifies the source address for NTP client traffic.	—	—
loopback	This parameter sets loopack interface as the source for NTP client traffic.	—	—
<vlanid>	This parameter sets source VLAN for NTP client traffic.	—	—
standalone	This command configures NTP time serve.	—	—
vlan-range <word>	Configures VLAN interfaces on which NTP adheres for serving time where: <word>: Represents VLAN range.	—	—
trusted-key	This command configures an additional subset of trusted keys which can be used for NTP authentication.	—	—
<keyid>	An additional trusted string that can be used for authentication.	—	—

Usage Guidelines

Network Time Protocol (NTP) authentication enables the controller to authenticate the NTP server before synchronizing local time with server. This helps identify secure servers from fradulent servers. This command has to be enabled for NTP authentication to work.

Starting from 8.1.0.0, you can specify the source address for NTP traffic originating from the Mobility Master using the **source** parameter. Before this enhancement, the NTP traffic’s source address was dynamically decided by the **NTP** module. The source of the NTP client traffic can be either a loopback interface or a specific VLAN ID. To allow time synchronization to be independent of any physical interfaces that could be down, use the loop back interface as the NTP source address.

Example

The following command configures an NTP server:

```
(host) [mynode] (config) #ntp authenticate
```

The following command configures the loopback interface as the source for NTP client traffic:

```
(host) [mynode] (config) #ntp source loopback
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **sha1** sub-parameter was added.
ArubaOS 8.1.0.0	The **server-mode** and **source** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

openflow-controller

```
openflow-controller
   auxiliary-channel-port <port>
   host-ageout-time <value>
   mode passive
   no
   openflow-controller-enable
   port <port>
   tls-ca-cert-file <tls-ca-cert-file>
   tls-certificate-file <tls-certificate-file>
   tls-enable
   tls-key-file  <tls-key-file>
   topology-discovery-enable
```

Description

This command configures OpenFlow Controller on Mobility Master.

Syntax

Parameter	Description	Range	Default
`auxiliary-channel-port`	Configures a listening port for OpenFlow Controller in the auxiliary channel (UDP) to send and receive packets without consuming bandwidth on the main channel.	—	—
`host-ageout-time`	Configures the ageout time for the host.	—	—
`mode {passive}`	Sets the OpenFlow Controller mode. This release of ArubaOS provides support only for passive mode.	passive	passive
`no`	Negates any configuration.	—	—
`openflow-controller-enable`	Enables or disables OpenFlow Controller on Mobility Master	—	disabled
`port`	The listening port for the OpenFlow Controller.	1-65535	6633
`tls-ca-cert-file`	Configures the CA certificate file from the specified path.	—	—
`tls-certificate-file`	Configures the certificate file from the specified path.	—	—
`tls-enable`	Enables or disables TLS.	—	disabled
`tls-key-file`	Configures the key from the specified path	—	—
`topology-discovery-enable`	Enables the Openflow Controller topology.	—	disabled

Usage Guidelines

The OpenFlow Controller must be configured from the **/mm** node hierarchy of Mobility Master. OpenFlow Controller is disabled by default. For OpenFlow to be functional in a network, you must enable OpenFlow Controller on the Mobility Master and OpenFlow agent on the required Managed devices. By default, OpenFlow is disabled on Mobility Master as well as the managed devices.

Examples

The following commands enables OpenFlow Controller on Mobility Master:

```
(host) [mm] (config) #openflow-controller
(host) [mm] (openflow-controller) #openflow-controller-enable
```

Related Commands

Command	Description
show openflow-controller	Displays the OpenFlow configuration and flow information on Mobility Master.
openflow-profile	This command configures OpenFlow profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Master

openflow-profile

```
openflow-profile
   auxiliary-channel-port <port>
   bind-vlan [add|remove] <vlan>
   controller-ip <ip-addr> <port>
   mode passive
   no
   openflow-auxiliary-enable
   openflow-enable
   tls-ca-cert-file <tls-ca-cert-file>
   tls-certificate-file <tls-certificate-file>
   tls-enable
   tls-key-file  <tls-key-file>
   version {v1.0|v1.3}
```

Description

This command configures OpenFlow profile on the managed device.

Syntax

Parameter	Description	Range	Default
`auxiliary-channel-port <port>`	Configures a listening port for OpenFlow Controller in the auxiliary channel (UDP) to send and receive packets without consuming bandwidth on the main channel.	—	—
`bind-vlan [add|remove] <vlan>`	Configures a specified range of OpenFlow VLANS. You can optionally add or remove the specified VLANs or VLAN range from the configured list of VLANs.	—	—
`controller-ip <port>`	Configures the IP and listening port of the OpenFlow Controller running on Mobility Master.	1-65535	6633
`mode {passive}`	Sets the OpenFlow agent mode. This release of ArubaOS provides support only for passive mode.	passive	passive
`no`	Negates any configuration.	—	—
`openflow-auxiliary-enable`	Enables or disables OpenFlow auxiliary channel.	—	disabled

Parameter	Description	Range	Default
`openflow-enable`	Enables or disables OpenFlow agent on the managed device.	—	disabled
`tls-ca-cert-file <tls-ca-cert-file>`	Configures the CA certificate file from the specified path.	—	—
`tls-certificate-file <tls-certificate-file>`	Configures the certificate file from the specified path.	—	—
`tls-enable`	Enables or disables TLS.	—	disabled
`tls-key-file <tls-key-file>`	Configures the key from the specified path	—	—
`version {v1.0|v1.3}`	Configures the OpenFlow version.	—	v1.3

Usage Guidelines

The OpenFlow profile must be configured from the **/md** node hierarchy of Mobility Master. OpenFlow profile is disabled by default. For OpenFlow to be functional in a network, you must enable OpenFlow Controller on the Mobility Master and OpenFlow agent on the required Managed devices. By default, OpenFlow is disabled on Mobility Master as well as the managed devices.

Examples

Execute the following commands to configure and enable the OpenFlow profile:

```
(host) [md] (config) #openflow-profile
(host) [md] (Openflow-profile) #openflow-enable
(host) [md] (Openflow-profile) #controller-ip <master-ip> <port>
```

Related Commands

Command	Description
show openflow-profile	Displays the OpenFlow profile configuration information on the managed device.
show openflow	Displays the OpenFlow information on the managed device.
openflow-controller	Configures the OpenFlow Controller on Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Master

packet-capture

```
packet-capture
   controlpath [interprocess {all |  <ports>}] [other] [sysmsg {all | <opcodes>] [tcp
   {all | <ports>}] [udp {all | <ports>]]
   copy-to-flash {controlpath-pcap | datapath-pcap}
   datapath {ipsec <peer-ip>|<peer-ipv6>} [wifi-client <mac-address> {decrypted | encrypted |
   all}]
   destination [interface <slot/module/port>] [ip-address <ip-address>] [local-filesystem]
   no
   reset-pcap {controlpath-pcap | datapath-pcap}
```

Description

Use this command to enable or disable packet capturing and set packet capturing options for a single packet capture session.

Syntax

Parameter	Description	Default
`controlpath`	Enables controlpath packet capture. Captured packets are stored in /var/log/oslog/filter.pcap. **NOTE:** Only capture to local-filesystem is supported for controlpath capture.	Disabled
`interprocess`	Enables or disables interprocess packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all ports. All CLI ports, which are TCP, are always skipped.	Disabled
`other`	Enable or disable all other types of packets.	Disabled
`sysmsg`	Enable or disable internal messaging packets. Specify up to ten comma-separated opcodes to capture; use `all` to sniff all opcodes. All CLI ports, which are TCP, are always skipped.	Disabled
`tcp`	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all TCP ports. All CLI ports, which are TCP, are always skipped.	Disabled
`udp`	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all UDP ports. All CLI ports, which are TCP, are always skipped.	Disabled
`copy-to-flash`	Copies captured packets to the flash.	—
`controlpath-pcap`	Copies controlpath captures. They are saved as **controlpath-pcap.tar.gz**.	—
`datapath-pcap`	Copies datapath captures. They are saved as **datapath-pcap.tar.gz**.	—

Parameter	Description	Default
`datapath`	Enables datapath packet capture. Captured packets are stored in /var/log/oslog/datapath.pcap or mirrored out of the managed device.	Disabled
`ipsec <peer-ip>`	Enable or disable IPsec packet capturing. Enter the IPsec peer IP address to specify a given peer. NOTE: Capture to local-filesystem is not supported with this option.	Disabled
`ipsec <peer-ipv6>`	Enable or disable IPsec packet capturing. Enter the IPsec peer IPv6 address to specify a given peer. NOTE: Capture to local-filesystem is not supported with this option.	Disabled
`wifi-client <mac-address> {decrypted | encrypted | all}`	Enable or disable packet capturing from a wifi client. Specify the client device by entering the device's MAC address. Additionally, you can specify what type of traffic captured: decrypted, encrypted, or all.	Disabled
`destination`	Configures the capture destination.	—
`interface <slot/module/port>`	Interface in <slot>/<module>/<port> format.	—
`ip-address <ip-address>`	Sends packet captures to a specific IP address.	—
`local-filesystem`	Stores captured packets on the managed device in pcap files.	—
`no`	Negates any configured parameter.	
`reset-pcap`	Deletes old pcap files and restarts the active capture.	—
`controlpath-pcap`	Deletes old controlpath pcap files and restarts the active controlpath capture.	—
`datapath-pcap`	Deletes old datapath pcap files and restarts the active datapath capture.	—

Usage Guidelines

The packet-capture command can perform two types of packet capture: controlpath and datapath. Controlpath only captures packet destined for the managed device. Datapath captures packets that are being forwarded by the managed device, such as packets from a wifi client.

Packets can be retrieved through the **tar logs** command; look for the filter.pcap or datapath.pcap file. This command activates packet capture options on the current session. They are not saved and applied across all reboots.

If you do want to enable a packet capture session without setting values that can be saved and used for another session, use the command packet-capture. The related command packet-capture-defaults lets you define a set of packet capture options and save them in the configuration file. These setting will be automatically enabled when the managed device boots up. Any settings defined using the command packet-capture will override packet-capture-defaults.

Example

The following command enables packet capturing for debugging a wireless WEP station doing VPN. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
(host) [/md] (config) #packet-capture sysmsg 30,29,90
(host) [/md] (config) #packet-capture udp 500,4500,1701,1812,1645
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

packet-capture-defaults

```
packet-capture
   controlpath [interprocess {all |  <ports>}] [other] [sysmsg {all | <opcodes>] [tcp
   {all | <ports>}] [udp {all | <ports>}]
   datapath {ipsec <peer-ip>} [wifi-client <mac-address> {decrypted | encrypted | all}]
   destination [interface <slot/module/port>] [ip-address <ip-address>] [local-filesystem]
   no
```

Description

Use this command to enable or disable packet capturing and define a set of default packet capturing options on the control path for debugging purposes.

Syntax

Parameter	Description	Default
`controlpath`	Enables controlpath packet capture. Captured packets are stored in `/var/log/oslog/filter.pcap`. Only capture to local-filesystem is supported for controlpath capture.	Disabled
`interprocess`	Enables or disables interprocess packet capturing. . Specify up to ten comma-separated ports to capture; use `all` to sniff all ports. All CLI ports, which are TCP, are always skipped.	Disabled
`other`	Enable or disable all other types of packets.	Disabled
`sysmsg`	Enable or disable internal messaging packets. Specify up to ten comma-separated opcodes to capture; use `all` to sniff all opcodes. All CLI ports, which are TCP, are always skipped.	Disabled
`tcp`	Enable or disable TCP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all TCP ports. All CLI ports, which are TCP, are always skipped.	Disabled
`udp`	Enable or disable UDP packet capturing. Specify up to ten comma-separated ports to capture; use `all` to sniff all UDP ports. All CLI ports, which are TCP, are always skipped.	Disabled
`datapath`	Enables datapath packet capture. Captured packets are stored in `/var/log/oslog/datapath.pcap` or mirrored out of the controller.	Disabled
`ipsec <peer-ip>`	Enable or disable IPsec packet capturing. Enter the IPsec peer IP address to specify a given peer. **NOTE:** Capture to local-filesystem is not supported with this option.	Disabled

Parameter	Description	Default
`wifi-client <mac-address> {decrypted | encrypted | all}`	Enable or disable packet capturing from a wifi client. Specify the client device by entering the device's MAC address. Additionally, you can specify what type of traffic captured: decrypted, encrypted, or all.	Disabled
`destination`	Configures the capture destination.	—
`interface <slot/module/port>`	Interface in `<slot>/<module>/<port>` format.	—
`ip-address <ip-address>`	Sends packet captures to a specific IP address.	—
`local-filesystem`	Stores captured packets on the controller in pcap files.	—
`no`	Negates any configured parameter.	

Usage Guidelines

This command applies to control path packets; not datapath packets. Packets can be retrieved through the **tar log** command; look for the filter.pcap file. This command activates packet capture options on the current switch. They are not saved and applied across switches.

Example

The following command sets the default packet capture values to debug a wireless WEP station doing VPN. Once these default settings are defined, you can use the packet-capture command to enable packet capturing with these values. This example uses the following parameters and values:

- Station up/down: sysmsg opcode 30
- WEP key plumbing: sysmsg opcode 29
- DHCP: sysmsg opcode 90
- IKE: UDP port 500 and 4500
- Layer 2 Tunneling Protocol (L2TP): UDP port 1701

```
(host) [mynode] (config)#packet-capture-defaults sysmsg 30,29,90 udp 500,4500,1701,1812,1645
```

Use the show packet-capture command to show the current action and the default values.

```
(host) [mynode] (config)#show packet-capture

Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering TCP with 2 port(s) enabled:
  2
  1
Packet filtering UDP with 1 port(s) enabled:
  1
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.


Packet Capture Defaults(across switches and reboots if saved)
=============================================================
Packet filtering TCP with 2 port(s) enabled:
  2
  1
```

```
Packet filtering UDP with 1 port(s) enabled:
  1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

page

```
page <length>
```

Description

This command sets the number of lines of text the terminal will display when paging is enabled.

Syntax

Parameter	Description	Range
`length`	Specifies the number of lines of text displayed.	24 - 100

Usage Guidelines

Use this command in conjunction with the **paging** command to specify the number of lines of text to display. For more information on the pause mechanism that stops the command output from printing continuously to the terminal, see paging on page 774.

If you need to adjust the screen size, use your terminal application to do so.

Example

The following command sets 80 as the number of lines of text displayed:

```
(host) [mynode] (config) #page 80
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

paging

`paging`

Description

This command stops the command output from printing continuously to the terminal.

Syntax

No parameters

Usage Guidelines

By default, paging is enabled.

With paging enabled, there is a pause mechanism that stops the command output from printing continuously to the terminal. If paging is disabled, the output prints continuously to the terminal. To disable paging, use the **no paging** command. You must be in enable mode to disable paging.

The paging setting is active on a per-user session. For example, if you disable paging from the CLI, it only affects that session. For new or existing sessions, paging is enabled by default.

You can also configure the number of lines of text displayed when paging is enabled. For more information, refer to the command page on page 773.

If you need to adjust the screen size, use your terminal application to do so.

Example

The following command enables paging:

```
(host) [mynode] (config) #paging
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

pan active-profile

```
pan active-profile
   profile <profile name>
```

Description

This command makes a Palo Alto Network profile active from a set of profiles.

Syntax

Parameter	Description
`profile <profile name>`	The name of the PAN profile to be activated.

Usage Guidelines

This command makes a PAN profile active from a set of profiles, if any. Only one PAN profile can be active at a time.

```
(host) [mynode] (config) #pan active-profile
(host) [mynode] (Palo Alto Networks Active Profile) #profile default
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

pan profile

```
pan profile <profile-name>
   clone
   firewall host <host> port <port> username <username> passwd <password>
   no
```

Description

This command configures a Palo Alto Networks profile to allow a managed device to communicate with a PAN firewall.

Syntax

Parameter	Description
`clone`	Name of an existing PAN profile configuration from which parameter values are copied.
`firewall`	Configures the information for the associated PAN firewall.
`host <host>`	IP address or hostname of the PAN firewall.
`port <port>`	Port number of the PAN firewall.
`username <username>`	The username of the PAN firewall.
`passwd <password>`	The password of the PAN firewall.
`no`	Negates any configured parameter.

Usage Guidelines

This command is used to configure the PAN firewall that the managed device will be communicating with. The username and password must match the name of the admin account configured on the PAN firewall.

```
(host) [mynode] (config) #pan profile default
(host) [mynode] (Palo Alto Networks Servers Profile "default") #firewall host 192.0.2.1 port
5642 username axde passwd ZAQ!2wsx
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

panic

```
panic {clear | info {file <filename> <symbolfile>|nvram <symbolfile>} | list {file
<filename>|nvram} | save <filename>}
```

Description

This command manages information created during a system crash.

Syntax

Parameter	Description
`clear`	Removes panic information from non-volatile random access memory (NVRAM).
`info`	Displays the content of specified panic files.
`list`	Lists panic information in the specified file in flash or in NVRAM.
`save`	Saves panic information from NVRAM into the specified file in flash.

Usage Guidelines

To troubleshoot system crashes, use the **panic save** command to save information from NVRAM into the specified file, then use the **panic clear** command to clear the information from NVRAM.

Example

The following command lists panic information in NVRAM:

```
(host) [mynode] #panic list nvram
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

papi-security

```
papi-security {enhanced-security|key <key>}
no
```

Description

The papi-security command enforces advanced security options and provides an enhanced level of security. It allows to enable or disable the PAPI Enhanced Security configuration and to configure a new security key if required.

Syntax

Parameter	Description	Range	Default
`Enhanced-security`	Enables PAPI Enhanced Security	—	Disable
`Key <key>`	Secret key that is used to authenticate messages between systems	10–64 characters	—
`no`	Disables the earlier configuration	—	—

Usage Guidelines

This command allows you to use advanced options that regulate PAPI communication between Mobility Master and managed devices. When enhanced security is enabled, PAPI messages are authenticated at the receiving device and are denied if validation failed.

Mismatch in secret key will affect centralized licensing and AirWave.

One of the ways PAPI messages are authenticated is through a shared secret key. The papi-security command lets you configure a key on the Mobility Master and the managed devices. If no key is configured, then the controller uses the default key.

The Mobility Master and the managed device must be configured with the same PAPI key.

Examples

To enable the PAPI Enhanced Security mode, execute the following command:

```
(host)[mynode] (config) #papi-security
(host)[mynode] (PAPI Security Profile) #enhanced-security
```

To configure a new PAPI Enhanced Security key for controllers and AirWave, execute the following command:

```
(host)[mynode] (PAPI Security Profile) #key 1234567890
```

Related Commands

Command	Description
show papi-security	Shows the status of the PAPI Enhanced Security configuration of thecontroller.
show ipc statistics app-id show ipc statistics app-name	Show the PAPI statistics for messages transmitted, received, signed, validated, denied, and more based on application ID or the application name.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master and managed devices

perf-test server

```
perf-test server
   start
      ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] [tcp [window <window>]]
      | udp}
      controller {[tcp [window <window>]] | udp}
```

Description

This command launches Iperf throughput test.

Syntax

Parameter	Description
`start`	Starts Iperf throughput tests in server mode
`ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] [tcp [window <window>]] | udp}`	Starts Iperf throughput test on an AP using: **[ap-name <ap-name>]**: AP name **[ip-addr <ip-addr>]**: IP address of AP **[ip6-addr <ip6-addr>]**: IPv6 address of IP **[tcp [window <window>]]**: Use TCP window size with suffix k for kilo or m for mega **udp**: Use UDP
`controller {[tcp [window <window>]] | udp}`	Starts Iperf throughput test on a controller using: **[tcp [window <window>]]**: Use TCP window size with suffix K for kilo or M for mega **udp**: Use UDP

Usage Guidelines

This command launches Iperf throughput test. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to start Ipref throughput test on AP **test** using TCP window size 2k:

```
(host) [mynode] #perf-test server start ap ap-name test tcp window 28
```

Related Commands

Command	Description
show perf-test reports	Use this command to view the results of an Iperf throughput test.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

perf-test client

```
perf-test client
   start
      ap {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]} [host {<ip>|<ip6>}]
      [duration <duration>] [parallel <parallel>] [tcp [window <window>]] [udp [bandwidth <band-
      width>]]
      controller [host {<ip>|<ip6>}] [duration <duration>] [parallel <parallel>] [tcp [window
      <window>]] [udp [bandwidth <bandwidth>]]
   stop
      ap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>]}
      controller
```

Description

This command launches Iperf throughput test in client mode.

Syntax

Parameter	Description
`start`	Starts Iperf throughput tests in client mode.
`ap`	Starts Iperf throughput tests on specified AP in client mode.
`ap-name <ap-name>`	Specifies name of an AP.
`ip-addr <ip-addr>`	Specifies IP address of an AP.
`ip6-addr <ip6-addr>`	Specifies IPv6 address of an AP.
`host {<ip>|<ip6>}]`	Specifies IP or IPv6 address of perf server.
`duration <duration>`	Specifies time, in seconds, to transmit. Default is 10 and range is 10 to 120.
`parallel <parallel>`	Specifies number of parallel clients threads to run. This should be less than the number of parallel threads on the server.
`tcp [window <window>]`	Specifies TCP window size to use.
`udp [bandwidth <bandwidth>]]`	Specifies UDP bandwidth to use.
`controller`	Starts Iperf throughput tests on specified controller in client mode.
`stop`	Stops Iperf throughput tests in client mode

Usage Guidelines

This command launches/stops Iperf throughput test in client mode. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to start Ipref throughput test on an AP named **ap215** using TCP window size 2k in client mode:

```
(host) [mynode] #perf-test client start ap ap-name ap215 host 192.0.2.1 duration 10 parallel 1 tcp window 2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

perf-test port

```
perf-test port {close|open}
```

Description

This command closes/opens Iperf throughput test port 5001.

Syntax

Parameter	Description
`close`	Closes Iperf throughput test port 5001.
`open`	Opens Iperf throughput test port 5001.

Usage Guidelines

This command closes/opensIperf throughput test port 5001. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to close Ipref throughput test port 5001:

```
(host) [mynode] #perf-test port close
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

pcap (deprecated)

```
pcap {raw-start <ipaddr> <target-ipaddr> <target-port> <format> [bssid <bssid>] [channel
<number>] [maxlen <maxlen>]}|{interactive <am-ip> <filter> <target-ipaddr> <target-port>
[bssid <bssid>][channel <number>]}|{clear|pause|resume|stop <am-ip> <id> [bssid <bssid>]}
```

Description

These commands manage packet capture (PCAP) on Aruba air monitors.

Syntax

Parameter	Description
`raw-start`	Stream raw packets to an external viewer.
`<ipaddr>`	IP address of the air monitor collecting packets.
`<target-ipaddr>`	IP address of the client station running Wildpacket's AiroPeek monitoring application.
`<target-port>`	UDP port number on the client station where the captured packets are sent.
`<format>`	Specify a number to indicate one of the following formats for captured packets: ■ **0** : pcap ■ **1** : peek ■ **2** : airmagnet ■ **3** : pcap+radio header ■ **4** : ppi
`bssid`	(Optional) BSSID of the Air Monitor interface for the PCAP session.
`<bssid>`	BSSID of the Air Monitor Interface, which is usually its MAC address.
`channel`	(Optional) Number of a radio channel to tune into to capture packets
`maxlen`	(Optional) Limit the length of 802.11 frames to include in the capture to a specified maximum.
`<maxlen>`	(Optional) Maximum number of packets to be captured.
`interactive`	Start an interactive packet capture session.
`<am-ip>`	IP address of the air monitor collecting packets.
`<filter-spec>`	Packet Capture filter specification.
`<target-ipaddr>`	
`<target-port>`	
`bssid`	(Optional) Specify the BSSID of the Air Monitor interface for the PCAP session.
`<bssid>`	BSSID of the Air Monitor Interface, which is usually its MAC address.
`channel`	(Optional) Number of a radio channel to tune into to capture packets

Parameter	Description
`clear`	Clears the packet capture session.
`pause`	Pause a packet capture session.
`resume`	Resume a packet capture session.
`start`	Start a new packet capture session.
`stop`	Stop a packet capture session.
`<am-ip>`	IP address of the air monitor collecting packets.
`<id>`	ID of the PCAP session.
`bssid`	(Optional) Specify the BSSID of the Air Monitor interface for the PCAP session.
`<bssid>`	BSSID of the Air Monitor Interface, which is usually its MAC address.

Usage Guidelines

These commands direct an Aruba air monitor to send packet captures to the Wildpacket's AiroPeek monitoring application on a remote client. The AiroPeek application listens for packets sent by the air monitor.

The following pcap commands are available:

Command	Description
`clear`	Clears the packet capture session.
`pause`	Pause a packet capture session.
`resume`	Resume a packet capture session.
`start`	Start a new packet capture session.
`stop`	Stop a packet capture session.

Before using these commands, you need to start the AiroPeek application on the client and open a capture window for the air monitor. The AiroPeek application cannot be used to control the flow or type of packets sent from Aruba air monitors.

The AiroPeek application processes all packets, however, you can apply display filters on the capture window to control the number and type of packets being displayed. In the capture window, the time stamp displayed corresponds to the time that the packet is received by the client and is not synchronized with the time on the Aruba air monitor.

Example

The following command starts a raw packet capture session for the air monitor at 10.100.100.1 and sends the packets to the client at 192.168.22.44 on port 604 with pcap format:

```
(host) (config) #pcap raw-start 10.100.100.1 192.168.22.44 604 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

phonehome

```
phonehome
   auto-report
   disable
   enable
   https <from_addr>
   now
   smtp <a.b.c.d> <from_addr> [port <port_num>] {size <max_size>] [user <username> pass
   <password>]
```

Description

This command configures the PhoneHome auto reporting feature.

Syntax

Parameter	Description
`auto-report`	The managed device will periodically contact Aruba support once a week to report any errors or changes to the managed device configuration or inventory. If the managed device has not reported any errors and its configuration file has not changed, no report will be sent. **NOTE:** Before you enable auto-reporting, you must first enable the PhoneHome feature using the command **phonehome enable**.
`disable`	This parameter disables the PhoneHome feature. Phonehome automatic reporting is disabled by default.
`enable`	This parameter enables the PhoneHome feature.
`now`	Issue the **phonehome now** command in enable mode to immediately create and send a report from the managed device to Aruba support. **NOTE:** Before you use the **phonehome now** command to create and send a report, you must first access the CLI in config mode and issue the command **phonehome enable** to enable this feature.
`https <from_addr>`	Configure managed device to send PhoneHome reports to an Activate server using HTTPS. The <from-addr> email address is used to properly identify the user sending the report.
`smtp`	Configure the SMTP server that will send email messages from the managed device to Aruba support.
`<a.b.c.d>`	IP address of the SMPT server
`<from_addr>`	Local email address from which the auto reporting messages will be sent. For example, *admin@mycorp.com*.
`port <port_num>`	(Optional) Port number from which the SMTP server will send auto reporting emails. Default port number: 25.
`size <max_size>`	(Optional) If your SMTP server has a restriction on the size of the emails it can send, use this parameter to specify the maximum size limit. Any reports larger than this limit will be divided into multiple smaller emails.
`user <username>` `pass <password>`	(Optional) If your SMTP server requires user authentication before it can send an email message, enter the username and password for a valid user on your network.

Usage Guidelines

By default, managed device send PhoneHome reports to the Activate server using HTTPS.

Most deployments should retain the default behavior send PhoneHome reports via Activate. However, if the managed device is behind proxy server and does not have direct access to Internet, PhoneHome should be configured to send reports using SMTP. The following section of this document describes the benefits of each of these configurations options.

Sending Phonehome Reports using Activate

PhoneHome integration with Activate offers following benefits:

- **Simpler configuration**. Phonehome only requires you to configure the email ID of the network administrator managing the device. as Activate already has information to accurately identify your managed device. If a DNS server is not configured on the managed device, PhoneHome will query the public DNS service (8.8.8.8) to resolve the Activate server IP address.
- **Smaller bandwidth requirements**. When the PhoneHome feature sends the report to the Activate server, the PhoneHome report is zipped into a smaller package, then divided into smaller 1MB pieces before being sent to the server using secure HTTPS. Only reports sent to Activate are zipped before they are sent, so reports sent to Activate use less bandwidth than a report sent to a SMTP server.
- **Enhanced error management**. If any individual portion of the report is not successfully received by the Activate server, PhoneHome makes up to three attempts to resend just that portion of the file, rather than resending the entire report. Reports sent via SMTP must be resent in their entirety if any portion is not received by the SMTP server.
- **Automatic removal of old reports**. Once the entire report has been sent to the Activate server, Activate sends an acknowledgment to the managed device, prompting the managed device to delete its local copy of the report.

Sending Reports using SMTP

If you configure the PhoneHome feature to use SMTP, the PhoneHome status reports is sent in an email. When the managed device generates the report email with the PhoneHome data file attachment, it forwards the email to the local SMTP server configured on your local network, which then relays the message to Aruba technical support. If your email server requires the sender to be authenticated before message delivery, the managed device can connect to the SMTP server by supplying the sender's user name and password.

When PhoneHome reports are sent using SMTP, the PhoneHome report attachment is encrypted before it is transmitted to the SMTP server, and is decrypted by Aruba support the report it is received. If the PhoneHome status report email is larger than the maximum email size supported by your SMTP server, the managed device divides the PhoneHome attachment into multiple smaller attachments and sends the report to Aruba in multiple emails. If any individual portion of the report is not successfully received by the SMTP server, PhoneHome resends the entire report.

Example

The following command turns on the PhoneHome feature, enables weekly auto-reports, and identifies the SMTP server to be used by this feature:

```
(host) [mynode] (config) #phonehome enable auto-report smtp 172.21.18.170 admin@mycorp.com
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	The **phonehome now** command must be issued in enable mode. All other PhoneHome commands require config mode.

ping

```
ping
   ipv6
      <global-address> [count <count-value>] [df-flag-ipv6] [validate-reply] [packet-size
      <size-value>] [interval <interval-value>] [pattern <pattern-value>] [timeout <timeout-
      value>] [tos <tos-value>] [ttl <ttl-value>] [validate-reply] [source [[<source-address>]
      [mgmt-interface]]]
      interface [vlan <vlanid>] <linklocal-address>
   <target> [count <count-value>] [df-flag] [validate-reply] [send-amon] [packet-size <size-
   value>] [interval <interval-value>] [pattern <pattern-value>] [timeout <timeout-value>]
   [tos <tos-value>] [ttl <ttl-value>] [validate-reply] [source [[<source-address>] [mgmt-
   interface]]]
```

Description

This command sends ICMP echo packets to the specified IP or IPv6 address.

Syntax

Parameter	Description	Default	Range
`ipv6`	Ping specified IPv6 address.	—	—
`<global-address>`	Ping specified global IPv6 address	—	—
`count <count-value>`	Specifies the number of ping packets to send.	5	1-1000
`df-flag-ipv6`	Sets the do not fragment flag.	—	—
`validate-reply`	Validates the reply data.	—	—
`packet-size <size-value>`	Specifies the size in bytes of the ping datagram.	100 bytes	10-2000 bytes
`interval <interval-value>`	Sets the time interval, in seconds, between ping datagrams.	1 second	1-60 seconds
`pattern <pattern-value>`	Specifies the hexadecimal digit pattern.	—	Up to 16 digits
`timeout <timeout-value>`	Specifies the time, in seconds, to wait for response.	2 seconds	1-10 seconds
`tos <tos-value>`	Sets 8 bits of traffic class field in IPv6 header.	0	0-255

Parameter	Description	Default	Range
`ttl <ttl-value>`	Sets the TTL value, in seconds, for the ping datagram.	225 seconds	1-255 seconds
`validate-reply`	Validates the reply data.	—	—
`send-amon`	Send structured result in an AMON message.	—	—
`source [[<source-address>][mgmt-interface]`	Specifies the source interface (management interface, or VLAN ID) for the ping datagram.	—	1-4094
`interface`	Specifies interface for link-local address.	—	—
`vlan <vlanid>`	Specifies VLAN ID for local-link address.	—	—
`<linklocal-address>`	Specifies IPv6 link-local address.	—	—
`<target>`	Pings specified IP address	—	—

Usage Guidelines

You can send ICMP echo packets to a specified IP or IPv6 address.

Examples

The following example pings 192.0.2.1.

```
(host) [mynode] #ping 192.0.2.1

Press 'q' to abort.
Sending 5, 92-byte ICMP Echos to 192.0.2.1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.03/0.0312/0.036 ms
```

The following example pings the specified IPv6 global address:

```
(host) [mynode] #ping ipv6 2001:db8:0:abcd::1

Press 'q' to abort.
Sending 5, 92-byte ICMPv6 Echos to 2001:db8:0:abcd::1, timeout is 2 seconds:
.....
Success rate is 100 percent (5/5), round-trip min/avg/max = 0.03/0.0312/0.036 ms
```

Command History:

Release	Modification
ArubaOS 8.2.0.0	The **send-amon** parameter was added.
ArubaOS 8.1.0.0	The following parameters were added: ■ **interval** ■ **ttl** ■ **validate-reply**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

pkt-trace acl

```
pkt-trace acl
   <name> [enable | disable] [log] [trace-hex-mask <tmask> [log-1]] [trace [recv] [send]
   [fast] [bridge] [route] [session] [rtsp] [station] [init] [vlan] [user] [mcast] [tunnel]
   [bwm] [nat] [trunk] [cp-dp-sp] [acl-processing] [heap] [event] [cp-dp-sp-message] [port]
   [ftp] [icmp-error] [wep-encrypt] [wep-decrypt] [ipsec-encrypt] [ipsec-decrypt] [ipsec-ctrl]
   [pptp] [ip-re-assembly] [wep-icmpfr] [dhcp] [mobility] [peer] [pptp-ctrl] [tkip-encrypt]
   [tkip-decrypt] [tkip-ctrl] [tkip-alloc-err] [sip-alg] [skinny] [vocera] [gsi] [aesccm-
   encrypt] [aesccm-decrypt] [netad] [xSec-ctrl] [xSec-encrypt] [xSec-decrypt] [tcp-
   termination] [log-2] [dpi]]
```

Description

Trace packets in the datapath. Use this feature only under the supervision of Aruba technical support.

Syntax

Parameter	Description
`<name>`	Traces packets for the specified access-control list.
`enable`	Enables packet tracing for the ACL.
`disable`	Disables packet tracing for the ACL.
`log`	Writes packet trace data to log file.
`tracemask <tmask>`	Specify the trace mask. This value will be provided by Aruba technical support.
`trace-hex-mask`	Configures datapath trace mask in hexadecimal form
`<tmask>`	Specifies trace mask in hexadecimal form
`[log-1]`	Writes packet trace data to log file.
`trace`	Configures datapath trace options.
`acl-processing`	Trace mask for acl functionality
`aesccm-decrypt`	Trace mask for aesccm-decrypt functionality
`aesccm-encrypt`	Trace mask for aesccm-encrypt functionality
`bridge`	Trace mask for bridge functionality
`bwm`	Trace mask for bwm functionality
`cp-dp-sp`	Trace mask for control path, slow path and fasth path messaging functionality
`cp-dp-sp-message`	Additional trace mask for control path, slow path and fasth path messaging functionality
`dhcp`	Trace mask for dhcp functionality
`dpi`	Trace mask for datapath DPI

Parameter	Description
event	Trace mask for event functionality
fast	Trace mask for fast functionality
ftp	Trace mask for FTP functionality
gsi	Trace mask for GSI functionality
heap	Trace mask for heap functionality
icmp-error	Trace mask for ICMP error processing functionality
init	Trace mask for init functionality
ip-re-assembly	Trace mask for IP re-assembly functionality
ipsec-ctrl	Trace mask for IPsec-ctrl functionality
ipsec-decrypt	Trace mask for IPsec-decrypt functionality functionality
ipsec-encrypt	Trace mask for IPsec-encrypt functionality functionality
log-2	Enables writing packet trace data into log file
mcast	Trace mask for mcast functionality
mobility	Trace mask for mobility functionality
nat	Trace mask for NAT functionality
netad	Trace mask for netad functionality
peer	Trace mask for peer functionality
port	Trace mask for port functionality
pptp	Trace mask for PPTP functionality
pptp-ctrl	Trace mask for PPTP-ctrl functionality
recv	Trace mask for recv functionality
route	Trace mask for route functionality
rtsp	Trace mask for rtsp functionality
send	Trace mask for send functionality
session	Trace mask for session functionality
sip-alg	Trace mask for sip alg service functionality
skinny	Trace mask for skinny functionality
station	Trace mask for station functionality
tcp-termination	Trace mask for datapath TCP termination functionality

Parameter	Description
tkip-alloc-err	Trace mask for TKIP-alloc-err functionality
tkip-ctrl	Trace mask for TKIP-ctrl functionality
tkip-decrypt	Trace mask for TKIP-decrypt functionality
tkip-encrypt	Trace mask for TKIP-encrypt functionality
trunk	Trace mask for trunk functionality
tunnel	Trace mask for tunnel functionality
user	Trace mask for user functionality
vlan	Trace mask for VLAN functionality
vocera	Trace mask for Vocera functionality
wep-decrypt	Trace mask for WEP-decrypt functionality functionality
wep-encrypt	Trace mask for WEP-encrypt functionality functionality
wep-icmpfr	Trace mask for WEP-icmpfr functionality
xSec-ctrl	Trace mask for xSec-ctrl functionality
xSec-decrypt	Trace mask for xSec-decrypt functionality
xSec-encrypt	Trace mask for xSec-encrypt functionality

Example

The following example enables packet tracing for the traffic matching the acl **stateful-dot1x**.

```
(host) [mynode] #pkt-trace acl stateful-dot1x enable trace
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

pkt-trace-global

```
pkt-trace-global {enable|disable} [trace-mask <tmask>]
```

Description

Enable global packet tracing in the datapath. Use this feature only under the supervision of Aruba technical support.

Syntax

Parameter	Description
`<acl-name>`	Enable packet tracing for the specified access-control list.
`enable`	Enable global packet tracing for the ACL.
`disable`	Disable global packet tracing for the ACL.
`tracemask <tmask>`	Specify a trace mask. Use this feature only under the supervision of Aruba technical support.

Example

The following command enables the global packet tracing for all traffic.

```
(host) [mynode] (config) #pkt-trace-global enable
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

pkt-trace-rap

```
pkt-trace-rap
   enable
      [[acl <acl>]|[global]|[ingress <ingress>]] [trace-mask <trace-mask>] [[ap-name <ap-name>]
      |[ip-addr <ip-addr>]]
```

Description

This command enables packet tracing in RAP datapath.

Syntax

Parameter	Description
`enable`	Enables packet tracing in RAP datapath.
`acl <acl>`	Specifies name of the ACL.
`[global]`	Traces all packets.
`ingress <ingress>`	Traces packets from ingress.
`trace-mask <trace-mask>`	Specifies the trace mask. This value will be provided by Aruba technical support.
`ap-name <ap-name>`	Specifies name of an AP.
`ip-addr <ip-addr>`	Specifies IP address of an AP.

Example

The following example enables packet tracing in RAP datapath:

```
(host) [mynode] #pkt-trace-rap enable acl default trace-mask OA ap-name ap215
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

pptp ip local pool

```
pptp ip local pool <pool_name> <pool_start_address> [<pool_end_address>]
```

Description

This command configures an IP address pool for VPN users using PPTP.

Syntax

Parameter	Description
`<pool-name>`	User-defined name for the address pool.
`<pool_start_address>`	Starting IP address for the pool.
`<pool_end_address>`	Ending IP address for the pool.

Usage Guidelines

If VPN is used as an access method, you specify the pool from which the user's IP address is assigned when the user negotiates a PPTP session. Use the **show vpdn pptp local** command to see the used and free addresses in the pool.

PPTP is an alternative to IPsec that is supported by various hardware platforms. PPTP is considered to be less secure than IPsec but also requires less configuration. You configure PPTP with the **vpdn** command.

Example

The following command configures an IP address pool for PPTP VPN users:

```
(host) [mynode] (config) #pptp ip local pool pptp-pool1 172.16.18.1 172.16.18.24
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

present working node

```
present working node
```

Description

This command shows the full path of the current configuration node.

Syntax

No parameters.

Example

The following example shows the full path of the current configuration node:

```
(host) [mynode] #present working node
/mm/mynode
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

priority-map

```
priority-map <name>
   dot1p <priority> high
   dscp <priority> high
   no ...
```

Description

This command configures the ToS and CoS values used to map traffic into high priority queues.

Syntax

Parameter	Description	Range
`<name>`	User-defined name of the priority map.	—
`dot1p`	IEEE 802.1p priority value, or a range of values separated by a dash (-).	0-7
`dscp`	DSCP priority value, or a range of values separated by a dash (-).	0-63
`no`	Negates any configured parameter.	—

Usage Guidelines

This command allows you to prioritize inbound traffic that is already tagged with 802.1p or IP ToS in hardware queues. You apply configured priority maps to ports on the managed device (using the **interface gigbitethernet** command). This causes the managed device to inspect inbound traffic on the port; when a matching QoS tag is found, the packet or flow is mapped to the specified queue.

Example

The following commands configure a priority map and apply it to a port:

```
(host) [mynode] (config) #priority-map pri1
   dscp 4-20 high
   dscp 60 high
   dot1p 4-7 high
interface gigabitethernet 0/0/4
   priority-map pri1
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

process monitor

```
process monitor log|restart|
```

Description

The process monitor validates the integrity of processes every 120 seconds. If a process does not respond during three consecutive 120-second timeout intervals, that process is flagged as nonresponsive and the process monitor will create a log message, restart the process or reboot the managed device.

Syntax

Parameter	Description
`log`	The process monitor creates a log message when a process fails to responding properly. This is the default behavior for the process monitor
`restart`	This parameter enables strict behavior for runtime processes. When you enable this option, the process monitor will restart processes that fail to responding properly.

Usage Guidelines

The CLI command **process monitor log** enables logging for process monitoring. By default, whenever a process does not update a required file or send a heartbeat pulse within the required time limit, the process monitor records a critical log message, but does not restart any process. If you want the configure watchdog to restart a process once it fails to respond, use the CLI **command process monitor restart**.

Example

The following changes the default process monitor behavior, so the process monitor restarts nonresponsive processes.

```
(host)[mynode] #process monitor restart
```

Related Commands

The show **process monitor statistics** command displays the current status of all the processes running under the process monitor watchdog. A partial example of the output of this command is shown below:

```
(host) (config) #show process monitor statistics

  Process Monitor Statistics
  --------------------------
  Name                          State            Restarts  Timeout Value  Timeout
                                                           Chances
  ----                          -----            --------  -------------  ---------------
  /mswitch/bin/arci-cli-helper  PROCESS_RUNNING  0         120            3
  /mswitch/bin/fpcli            PROCESS_RUNNING  0         120            3
  /mswitch/bin/packet_filter    PROCESS_RUNNING  0         120            3
  /mswitch/bin/certmgr          PROCESS_RUNNING  0         120            3
  /mswitch/bin/dbstart          PROCESS_RUNNING  0         120            3
  /mswitch/bin/cryptoPOST       PROCESS_RUNNING  0         120            3
  /mswitch/bin/sbConsoled       PROCESS_RUNNING  0         120            3
  /mswitch/bin/pubsub           PROCESS_RUNNING  0         120            3
  /mswitch/bin/cfgm             PROCESS_RUNNING  0         120            3
  /mswitch/bin/syslogdwrap      PROCESS_RUNNING  0         120            3
  /mswitch/bin/aaa              PROCESS_RUNNING  0         120            3
```

```
/mswitch/bin/fpapps             PROCESS_RUNNING  0          120             3
/mswitch/bin/pim                PROCESS_RUNNING  0          120             3
/mswitch/bin/lic
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

process restart

```
process restart <name> [core]
```

Description

This command restarts a process and optionally creates a core file.

Syntax

Parameter	Description
`<name>`	Name of the process to restart.
`[core]`	Creates a core file

Example

The following example restarts the **dbsync** process and creates a core file:

```
(host) [mynode] #process restart dbsync core
WARNING: Do you really want to restart process: dbsync (y/n): y
Restarting: dbsync
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

product serial-number

```
product serial-number <sl-num>
```

Description

This command configures the product serial-number for a managed device on a Virtual Machine (VM).

Syntax

Parameter	Description
`<sl-num>`	Configure the serial number provided by Aruba.

Usage Guidelines

Before you install ArubaOS on a VM instead of a physical Arubacontroller, contact your Aruba sales representative or authorized reseller and request a VM serial number, then use this serial number as a part of your VM configuration. This serial number is a randomly generated string in the format *DC<7-digit-string>*, for example, **DC0000001**. You must configure the VM serial number and identify the passphrase for that device before you can generate a license key for that specific VM configuration.

Example

The following example configures a product serial-number:

```
(host) [mynode] #product serial-number 0123456789
```

Related Commands

Command	Description
show inventory	Display the Mobility Master serial number used to generate licenses for a Mobility Master deployment.
show license passphrase	Display the Mobility Master passphrase used to generate licenses for a Mobility Master deployment.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master or a managed device.

prompt

```
prompt <new-prompt>
```

Description

This command changes the prompt text.

Syntax

Parameter	Description	Range	Default
`new-prompt`	The prompt text displayed by the Mobility Master.	1–64	<hostname>

Usage Guidelines

You can use any alphanumeric character, punctuation, or symbol character. To use spaces, plus symbols (+), question marks (?), or asterisks (*), enclose the text in quotes.

You cannot alter the parentheses that surround the prompt text, or the greater-than (>) or hash (#) symbols that indicate user or enable CLI mode.

Example

The following example changes the prompt text to “It’s a new day!”.

```
(host) [mynode] (config) #prompt “It’s a new day!”
(It’s a new day!) (config) #
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

provision-ap

```
provision-ap
   a-ant-bearing <bearing>
   a-ant-gain <gain>
   a-ant-pol <a-ant-pol>
   a-ant-tilt-angle <angle>
   a-antenna {1|2|both}
   altitude <altitude>
   ap-group <group>
   ap-lldp-pse-detect {disabled|enabled}
   ap-name <name>
   ap-poe-power-optimization
   apdot1x-factory-cert
   apdot1x-passwd <string>
   apdot1x-tls
   apdot1x-username <name>
   cellular_nw_preference 3g-only|4g-only|advanced|auto
   cert-DN
   dns-server-ip <ipaddr>
   dns-server-ip6 <ipv6 address>
   domain-name <name>
   external-antenna
   fqln <name>
   g-ant-bearing <bearing>
   g-ant-gain <gain>
   g-ant-pol <g-ant-pol>
   g-ant-tilt-angle <angle>
   g-antenna {1|2|both}
   gateway <ipaddr>
   gateway6 <ipv6-address>
   ikepsk <key>
   installation default|indoor|outdoor
   ip6addr <ipv6-address>
   ip6prefix <ipv6-prefix>
   ipaddr <ipaddr>
   latitude <location>
   link-priority-cellular
   link-priority-ethernet
   longitude <location>
   master {<name>|<ipaddr>}
   mesh-role {mesh-point|mesh-portal|none|remote-mesh-portal}
   mesh-sae {sae-disable|sae-enable}
   netmask <netmask>
   no ...
   ocsp_default
   pap-passwd <string>
   pap-user <name>
   pkcs12-passphrase <string>
   pppoe-chap-secret<key>
   pppoe-passwd <string>
   pppoe-service-name <name>
   pppoe-user <name>
   read-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
   reprovision {all|ap-name <name>|ip-addr <ipaddr>|ip6-addr <ip6-addr>|serial-num
   <string>|wired-mac <macaddr>}
   reset-bootinfo {ap-name <name>|ip-addr <ipaddr>|wired-mac <macaddr>}
   server-ip <ipaddr>
   sch-mode-radio-0
   sch-mode-radio-1
```

```
server-ip <server-ip>
server-name <name>
set-ikepsk-by-addr <ip-addr>
syslocation <string>
uplink-vlan <uplink-vlan>
usb-dev <usb-dev>
usb-dial <usb-dial>
usb-init <usb-init>
usb-passwd <usb-passwd>
usb-power-mode {auto|enable|disable}
usb-tty <usb-tty>
usb-tty-control <usb-tty-control>
usb-type <usb-type>
usb-user <usb-user>
```

Description

This command provisions or reprovisions an AP.

Syntax

Parameter	Description	Rang-e
`a-ant-bearing`	Determines the horizontal coverage distance of the 802.11a (5 GHz) antenna from True North. From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	0-360 Deci mal Degre es
`a-ant-gain`	Antenna gain for 802.11a (5GHz) antenna.	—
`a-ant-pol`	Antenna polarization value for 5GHz radio. Use one of the following parameters: ■ 0: CO-Polarized ■ 1: Cross-Polarized	—
`a-ant-tilt-angle`	Directs the angle of the 802.11a (5GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	-90 to +90 Deci mal Degre es
`a-antenna`	Antenna use for 5 GHz (802.11a) frequency band. Use one of the following parameters: ■ 1: Use antenna 1 ■ 2: Use antenna 2 ■ both: Use both antennas (default)	1, 2, both (defa ult)

Parameter	Description	Rang-e
altitude	Altitude, in meters, of the AP. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	—
ap-group	Name of the AP group to which the AP belongs.	—
ap-lldp-pse-detect	Enabling causes the AP to detect the POE type via LLDP POE TLV. Use one of the following parameters: ■ **enabled**: The AP uses PSE TYPE in the POE TLV to detect the PSE type. ■ **disabled**: The AP detects the POE using the HW classification.	—
ap-name	Name of the AP to be provisioned.	—
ap-poe-power-optimization	Enable optimization to minimize the POE draw of the AP. Enabling optimization may disable some parts of the AP. Disabling optimization ensures all features are enabled.	—
apdot1x-factory-cert	Enable AP to use factory certificates when doing 802.1x EAP-TLS.	
apdot1x-passwd	Password of the AP to authenticate to 802.1X using PEAP.	—
apdot1x-tls	Enable AP to 802.1x using EAP-TLS.	
apdot1x-username	Username of the AP to authenticate to 802.1X using PEAP.	—

Parameter	Description	Rang-e
`cellular_nw_preference 3g-only|4g-only| advanced|auto`	This setting allows you to select how the modem should operate. ■ **auto** (default): In this mode, the modem firmware will control the cellular network service selection; so the cellular network service failover and fallback is not interrupted by the Remote AP. ■ **3g_only**: Locks the modem to operate only in 3G. ■ **4g_only**: Locks the modem to operate only in 4G. ■ **advanced**: The Remote AP controls the cellular network service selection based on the Received Signal Strength Indication (RSSI) threshold-based approach. Initially the modem is set to the default auto mode. This allows the modem firmware to select the available network. The Remote AP determines the RSSI value for the available network type (for example 4G), checks whether the RSSI is within required range, and if so, connects to that network. If the RSSI for the modem's selected network is not within the required range, the Remote AP will then check the RSSI limit of an alternate network (for example, 3G), and reconnect to that alternate network. The Remote AP will repeat the above steps each time it tries to connect using a 4G multimode modem in this mode.	—
`cert-DN`	The Server Certificate CN for Identity	—
`dns-server-ip`	IP address of the DNS server for the AP.	—
`dns-server-ip6`	IPv6 address of the DNS server for the AP.	—
`domain-name`	Domain name for the AP.	—
`external-anten na`	Use an external antenna with the AP.	—
`fqln`	FQLN for the AP, in the format <APname.floor.building.campus>.	—
`g-ant-bearing`	Determines the horizontal coverage distance of the 802.11g (2.4GHz) antenna from True North. From a planning perspective, the horizontal coverage pattern does not consider the elevation or vertical antenna pattern. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	0-360 decimal degrees

Parameter	Description	Rang-e
g-ant-gain	Antenna gain for 802.11g (2.4GHz) antenna.	—
g-ant-pol	Antenna polarization value for 2.4GHz radio. Use one of the following parameters: ■ 0: CO-Polarized ■ 1: Cross-Polarized	—
g-ant-tilt-angle	Directs the angle of the 802.11g (2.4GHz) antenna for optimum coverage. Use a - (negative) value for downtilt and a + (positive) value for uptilt. **NOTE:** This parameter is supported on outdoor APs only. If you use this parameter to configure an indoor AP, an error message is displayed.	-90 to +90 Decimal Degrees
g-antenna	Antenna use for 2.4 GHz (802.11g) frequency band. Use one of the following parameters: ■ 1: Use antenna 1 ■ 2: Use antenna 2 ■ both: Use both antennas	1, 2, both
gateway	IP address of the default gateway for the AP.	—
gateway6	IPv6 address of the default gateway for the AP.	—
ikepsk	IKE preshared key for the AP.	—
installation	Specify the type of installation (indoor or outdoor). The default parameter automatically selects an installation mode based upon the AP model type.	default indoor outdoor
ip6addr	Static IPv6 address of the AP.	—
ip6prefix	The prefix of static IPv6 address of the AP.	—
ipaddr	Static IP address for the AP.	—
latitude	Latitude coordinates of the AP. Use the format: Degrees, Minutes, Seconds (DMS). For example: 37 22 00 N	—
link-priority-cellular <link-priority-cellular>	Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary link.	—

Parameter	Description	Rang-e
`link-priority-ethernet <link-priority-ethernet>`	Set the priority of the wired uplink. Each uplink type has an associated priority; wired ports having the highest priority by default.	—
`longitude`	Longitude coordinates of the AP. Use the DMS format. For example: 122 02 00 W	—
`master`	Name or IP address of the Mobility Master.	—
`mesh-role`	Configure the AP to operate as a mesh node. You assign one of three roles: **mesh portal**, **mesh poin**t or r**emote mesh point**. If you select "none," the AP operates as a thin AP.	—
`mesh-sae`	Enable or disable Simultaneous Authentication of Equals (SAE) on a mesh network. This option offers enhanced security over the default wpa2-psk-aes mesh security setting, and provides secure, attack-resistant authentication using a PSK. SAE supports simultaneous initiation of a key exchange, allowing either party to initiate an exchange or both parties to initiate a key exchange simultaneously To use the SAE feature, you must enable this parameter on all mesh nodes (points and portals) in the network, to prevent mesh link connectivity issues. **NOTE:** This is a Beta feature only. This parameter should be kept "disabled" for this release.	—
`netmask`	Netmask for the IP address.	—
`ocsp_default`	If this parameter is set to 0 (default accept) and the certificate status is unknown, the server certificate is considered valid and the Remote AP comes up. If this parameter is set to 1 (default deny) and the certificate status is unknown, the server certificate is considered revoked and the Remote AP does not come up. By default, OCSP default is set to 0 (default accept).	—
`no`	Negates any configured parameter.	—

Parameter	Description	Rang-e
pap-passwd	PAP password for the AP. You can use special characters in the PAP password. Following are the restrictions: ■ You cannot use double-byte characters ■ You cannot use a tilde (~) ■ You cannot use a tick (') ■ If you use quotes (single or double), you must use the backslash (\) before and after the password	—
pap-user	PAP username for the AP.	—
pkcs12-passphrase	Passphrase in PKCS12 format.	—
pppoe-chap-secret	PPPoE CHAP secret key for the AP.	—
pppoe-passwd	PPPoE password for the AP.	—
pppoe-service-name	PPPoE service name for the AP.	—
pppoe-user	PPPoE username for the AP.	—
read-bootinfo	Retrieves current provisioning parameters of the specified AP. **NOTE:** This parameter can only be used on the Mobility Master.	—
reprovision	Provisions one or more APs with the values in the provisioning-params workspace. To use **reprovision**, you must use **read-bootinfo** to retrieve the current values of the APs into the provisioning-ap-list. **NOTE:** This parameter can only be used on the Mobility Master.	—
reset-bootinfo	Restores factory default provisioning parameters to the specified AP. **NOTE:** This parameter can only be used on the Mobility Master.	—
sch-mode-radio-0	If you are provisioning an 802.11n-capable AP, you can issue the sch-mode-radio-0 command to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This setting is disabled by default.	—
sch-mode-radio-1	If you are provisioning an 802.11n-capable AP, you can issue the sch-mode-radio-1 command to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This setting is disabled by default.	—

Parameter	Description	Rang-e
server-ip	IPv4 or IPv6 address of the managed device from which the AP boots.	—
server-name	DNS name of the managed device from which the AP boots.	—
set-ikepsk-by-addr	Set a IKE preshared key to correspond to a specific IP address.	—
syslocation	User-defined description of the location of the AP.	—
uplink-vlan <uplink-vlan>	If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature. **NOTE:** If an AP is provisioned with an uplink VLAN, it *must be connected to a trunk mode port* or the AP's frames will be dropped.	—
usb-dev	The USB device identifier, if the device is not already supported.	—
usb-dial	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.	—
usb-modeswitch "-v <default_vendor> -p <default_product> -V <target_vendor> -P <target_product> -M <message_content>"	USB cellular devices on Remote APs typically register as modems, but may occasionally register as a mass-storage device. If a Remote AP cannot recognize its USB cellular modem, use the **usb-modeswitch** command to specify the parameters for the hardware model of the USB cellular data-card. **NOTE:** You must enclose the entire modeswitch parameter string in quotation marks.	—

Parameter	Description	Rang-e
`usb-init`	The initialization string for the USB modem. This string configures the AP Name setting of the USB modem. For the USB modem to understand this string, the value entered should adhere to one of the following formats: ■ Use double-quotes and prefix them with a backslash character. See example below: **"AT+CGDCONT=1,\"IP\",\"APN\""** ■ Use single-quote instead of double-quotes. AP translates single-quote into double-quotes. See example below: **"AT+CGDCONT=1,'IP','APN'"** ■ Use the string begin-end pair without double quotes. See example below: **AT+CGDCONT=1,'IP','APN'** ■ In some cases, the 4G/LTE modem requires the configuration of two AP Names during USB initialization. The first AP Name initiates the connection to obtain an IP address, and the second AP Name sends and receives data. Use the **;** delimiter character to create two separate strings for the AP Names in the command. See example below: **"AT+CGDCONT=1,\"IP\",\"APN1\";1,1,\"APN2\""** **NOTE:** You must obtain the AP Name from your ISP and ensure that each AP Name entry follows the manufacturer's AT command reference.	—
`usb-passwd`	A PPP password, if provided by the cellular service provider	—
`usb-power-mode auto| enable|disable`	Set the USB power mode to control the power to the USB port.	—
`usb-tty`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.	—

Parameter	Description	Rang-e
`usb-tty-control`	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.	—
`usb-type`	Specify the USB driver type. ■ **acm**: Use ACM driver ■ **airprime**: Use Airprime driver ■ **beceem-wimax**: Use Beceem driver for 4G-WiMAX ■ **ether**: Use CDC Ether driver for direct IP 4G device ■ **hso**: Use HSO driver for newer Option ■ **none**: Disable 3G or 2G network on USB ■ **option**: Use Option driver ■ **pantech-3g**: Same as "pantech-uml290" - to support upgrade ■ **pantech-uml290**: Use Pantech USB driver for UML290 device ■ **ptumlusbnet**: Use Pantech USB driver for 4G device ■ **rndis**: Use a RNDIS driver for a 4G device ■ **sierra-evdo**: Use EVDO Sierra Wireless driver ■ **sierra-gsm**: Use GSM Sierra Wireless driver ■ **sierrausbnet**:Use SIERRA Direct IP driver for 4G device ■ **storage**: Use USB flash as storage device for storing Remote AP certificates	—
`usb-user`	The PPP username provided by the cellular service provider	—

Usage Guidelines

You do not need to provision APs before installing and using them.

The exceptions are outdoor APs, which have antenna gains that you must provision before they can be used, and APs configured for mesh. You must provision the AP before you install it as a mesh node in a mesh deployment.

Users less familiar with this process may prefer to use the **Provisioning** page in the WebUI to provision an AP.

Provisioned or reprovisioned values do not take effect until the AP is rebooted. APs reboot automatically after they are successfully reprovisioned.

In order to enable cellular uplink for a Remote AP, the Remote AP must have the device driver for the USB data card and the correct configuration parameters. ArubaOS includes device drivers for the most common hardware types, but you can use the **usb** commands in this profile to configure a Remote AP to recognize and use an unknown USB modem type.

Provisioning a Single AP

To provision a single AP:

1. Use the **read-bootinfo** option to read the current information from the deployed AP you wish to reprovision.
2. Use the **show provisioning-ap-list** command to see the AP to be provisioned.
3. Use the **copy-provisioning-params** option to copy the AP's parameter values to the provisioning-params workspace.
4. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
5. Use the **reprovision** option to provision the AP with the values in provisioning-params workspace. The AP automatically reboots.

Provisioning Multiple APs at a Time

You can change parameter values for multiple APs at a time, however, note the following:

- You cannot provision the following AP-specific options on multiple APs:
  - ap-name
  - ipaddr
  - pap-user
  - pap-passwd
  - ikepsk

  If any of these options are already provisioned on the AP, their values are retained when the AP is reprovisioned.
- The values of the server-name, a-ant-gain, or g-ant-gain options are retained if they are not reprovisioned.
- All other values in the provisioning-params workspace are copied to the APs.

To provision multiple APs at the same time:

1. Use the **read-bootinfo** to read the current information from each deployed AP that you wish to provision.

The AP parameter values are written to the provisioning-ap-list. To reprovision multiple APs, the APs must be present in the provisioning-ap-list. Use the **show provisioning-ap-list** command to see the APs that will be provisioned. Use the **clear provisioning-ap-list** command to clear the provisioning-ap-list.

2. Use the **copy-provisioning-params** option to copy an AP's parameter values to the provisioning-params workspace.
3. Use the provision-ap options to set new values. Use the **show provisioning-params** command to display parameters and values in the provisioning-params workspace. Use the **clear provisioning-params** command to reset the workspace to default values.
4. Use the **reprovisionall** option to provision the APs in the provisioning-ap-list with the values in provisioning-params workspace. All APs in the provisioning-ap-list automatically reboot.

The following are useful commands when provisioning one or more APs:

- **show|clear provisioning-ap-list** displays or clears the APs that will be provisioned.
- **show|clear provisioning-params** displays or resets values in the provisioning-params workspace.
- **show ap provisioning** shows the provisioning parameters an AP is currently using.

Example

The following commands change the IP address of the Mobility Master on the AP:

```
(host) [mynode] (config) #provision-ap
   read-bootinfo ap-name lab103
   show provisioning-ap-list
   copy-provisioning-params ap-name lab103
   master 10.100.102.210
   reprovision ap-name lab103
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: ■ **apdot1x-factory-cert** ■ **apdot1x-tls** ■ **a-ant-pol** ■ **g-ant-pol** ■ **ap-lldp-pse-detect**
ArubaOS 8.1.0.0	The **server-ip** parameter was modified to accept IPv6 address.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms, except for the parameters noted in the syntax table.	Base operating system, except for the parameters noted in the syntax table.	Config mode on Mobility Master

pwd

```
pwd
```

Description

This command displays the full path of the current configuration node.

Syntax

No parameters.

Example

The following example indicates that the current node-path is **/mm/mynode**:

```
(host) [mynode] (config) #pwd
/mm/mynode
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

read-bootinfo

```
read-bootinfo {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}|{wired-mac <wired-mac>}
```

Description

This command retrieves the current provisioning parameters of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Retrieves the current provisioning parameters of an AP for specified AP name.
`ip-addr <ip-addr>`	Retrieves the current provisioning parameters of an AP for specified IP address.
`ip6-addr <ip6-addr>`	Retrieves the current provisioning parameters of an AP for specified IPv6 address.
`wired-mac <wired-mac>`	Retrieves the current provisioning parameters of an AP for specified wired MAC address.

Usage Guidelines

This command retrieves the current provisioning parameters of an AP. For the remaining parameters, see the command syntax.

Example

The following example retrieves the current provisioning parameters of an AP named ap-205:

```
(host) [mynode] #read-bootinfo ap-name ap-205
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

reload

```
reload
   force
   device-mac
```

Description

This command reboots the managed device.

Syntax

Parameter	Description
`force`	Forces reboot without waiting for confirmation.
`device-mac`	Specifies the device MAC address for reboot.

Usage Guidelines

Use this command to reboot a managed device if required after making configuration changes or under the guidance of Aruba Networks customer support. The **reload** command powers down the managed device, making it unavailable for configuration. After the managed device reboots, you can access it over a local console connected to the serial port, or through an SSH, Telnet, or WebUI session.

Example

The following restarts the managed device without waiting for confirmation:

```
(host) [mynode] #reload force

System will now restart!
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

rename

```
rename <filename> <newfilename>
```

Description

This command renames an existing system file.

Syntax

Parameter	Description
`filename`	An alphanumeric string that specifies the current name of the file on the system.
`newfilename`	An alphanumeric string that specifies the new name of the file on the system.

Usage Guidelines

Use this command to rename an existing system file on the controller. You can use a combination of numbers, letters, and punctuation (periods, underscores, and dashes) to rename a file. The new name takes affect immediately.

Make sure the renamed file uses the same file extension as the original file. If you change the file extension, the file may be unrecognized by the system. For example, if you have an existing file named `upgrade.log`, the new file must include the `.log` file extension.

You cannot rename the active configuration currently selected to boot the controller. If you attempt to rename the active configuration file, the controller returns the following message:

```
Cannot rename active configuration file
```

To view a list of system files, and for more information about the directory contents, see dir on page 426.

Example

The following command changes the file named **test_configuration** to **deployed_configuration**:

```
(host) [mynode] (config) #rename test_configuration deployed_configuration
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

reprovision

```
reprovision {wired-mac <wired-mac> | ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr> | serial-num <serial-num> | all}
```

Description

This command sends current provisioning-profile to access points.

Syntax

Parameter	Description	Range	Default
`all`	Reprovisions all access points listed in provisioning_ap_list	–	–
`ap-name <ap-name>`	Reprovisions an AP with the specified AP name.	–	–
`ip-addr <ip-addr>`	Reprovisions an AP with the specified IP address.		
`ip6-addr <ip6-addr>`	Reprovisions an AP with the specified IPv6 address.	–	–
`serial-num <serial-num>`	Reprovisions an AP with the specified serial number.	–	–
`wired-mac <wired-mac>`	Reprovisions an AP with the specified MAC address.	–	–

Usage Guidelines

This command sends current provisioning-profile to access points. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to reprovision an AP **test**:

```
(host) [mynode] #reprovision ap-name test
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

reset-bootinfo

```
reset-bootinfo
  ap-name
  ip-addr
  wired-mac
```

Description

This command restores the factory default values for an access point.

Syntax

Parameter	Description
`ap-name <ap-name>`	Restores the factory default values for the specified name of the access point.
`ip-addr <ip-addr>`	Restores the factory default values for the specified IP address of the access point.
`wired-mac <wired-mac>`	Restores the factory default values for the specified MAC address of the AP.

Usage Guidelines

This command restores the factory default values for an access point. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to restore factory default values for an access point with MAC address **00:1a:1e:aa:bb:cc**:

```
(host) [mynode] #reset-bootinfo wired-mac 00:1a:1e:aa:bb:cc
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

restore

```
restore
   config
   factory_default
   flash
```

Description

This command restores the file or configuration.

Syntax

Parameter	Description
`config`	Restores configuration directories from a configbackup.tar.gz file.
`factory_default`	Restores factory default settings.
`flash`	Restores important directories from flashbackup.tar.gz file.

Usage Guidelines

Use the **backup flash** command to tar and compress flash directories to the flashbackup.tar.gz file.

Example

The following command restores directories from the flashbackup.tar.gz file:

```
(host) [mynode] #restore flash
Please wait while we restore the flash backup........
Flash restored successfully.
Please reload (reboot) the controller for the new files to take effect.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

rf am-scan-profile

```
<profile-name>
   clone <profile>
   dwell-time-active-channel
   dwell-time-other-reg-domain-channel
   dwell-time-rare-channel
   dwell-time-reg-domain-channel
   no
   scan-mode
```

Description

Configure an Air Monitor (AM) scanning profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile.	1-63 characters	—
`clone <profile>`	Copy data from another AM scanning profile	—	—
`dwell-time-active-channel`	Dwell time (in ms) for channels where there is wireless activity.	100-32768 ms	500 ms
`dwell-time-other-reg-domain-channel`	Dwell time (in ms) for channels not in the APs regulatory domain.	100-32768 ms	250 ms
`dwell-time-rare-channel`	Dwell time (in ms) for rare channels.	100-32768 ms	100 ms
`dwell-time-reg-domain-channel`	Dwell time (in ms) for AP's Regulatory domain channels	100-32768 ms	250 ms
`no`	Delete the command	—	—
`scan-mode`	Set the scanning mode for the radio.	—	—
`all-reg-domain`	Scan channels in all regulatory domain	—	—
`rare`	Scan *all* channels (all regulatory domains and rare channels)	—	—
`reg-domain`	Scan channels in the APs regulatory domain	—	—

Usage Guidelines

Channels are categorized into the following types:

- **Active Channel:** This qualifier indicates that wireless activity (for example, a probe request) is detected on this channel by the presence of an AP or other 802.11 activity.

- **All Regulatory Domain Channels:** A valid non-overlapping channel that is in the regulatory domain of at least one country.
- **Rare Channels:** Channels that fall into a frequency range outside of the regulatory domain; 2484 MHz and 4900MHz-4995MHz (J-channels), and 5000-5100Mhz.
- **Regulatory Domain Channels:** A channel that belongs to the regulatory domain of the country in which the AP is deployed. The set of channels that belong to this group is a subset of the channels in all-reg-domain channel group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All Platforms	RFProtect	Config mode on Mobility Master.

rft

```
rft test profile ht-link-quality ap-name <ap-name> [dest-mac <dest-mac> [radio {0|1}mcs]]

rft test profile link-quality {ap-name <ap-name> dest-mac <dest-mac> [phy {a|g}|
 radio {0|1}] | bssid <bssid> dest-mac <dest-mac> | ip-addr <ip-addr>
 dest-mac <macaddr> [phy {a|g}|radio {0|1} | ip6-addr <ip6-addr> dest-mac <macaddr> [phy {a|g}
|radio {0|1}]}

rft test profile raw {ap-name <name> dest-mac <dest-mac> [phy {a|g}|radio {0|1}] | bssid
<bssid> dest-mac <dest-mac> | ip-addr <ip-addr> dest-mac <dest-mac> [phy {a|g}|radio {0|1}]}
```

Description

This command is used for RF troubleshooting.

Syntax

Parameter	Description	Range
`ap-name`	Name of the AP that performs the test.	—
`dest-mac`	MAC address of the client to be tested.	—
`phy`	802.11 type, either a or g.	a | g
`radio`	Radio ID, either 0 or 1.	0 | 1
`bssid`	BSSID of the AP that performs the test.	—
`ip-addr`	IP address of the AP that performs the test.	
`ip6-addr`	IPv6 address of the AP that performs the test.	

Usage Guidelines

This command can run predefined test profiles for antenna connectivity, link quality, or raw testing. You should only run these commands when directed to do so by anAruba support representative.

Command History

Version	Modification
ArubaOS 8.2.0.0	The **ht-link-quality** and **ip6-addr** parameters were added.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

rf arm-rf-domain-profile

```
rf arm-rf-domain profile
   arm-rf-domain-key <arm-rf-domain-key>
```

Description

This profile holds a non-editable key defined by Mobility Master, and used to sign over-the air (OTA) ARM updates exchanged between APs.

Syntax

Parameter	Description
`<arm-rf-domain-key>`	Non-editable key value

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

rf arm-profile

```
rf arm-profile <profile>
   40MHz-allowed-bands {All|None|a-only|g-only}
   80MHz support
   acceptable-coverage-index <number>
   active-scan (not intended for use)
   aggressive-scan
   assignment {disable|maintain|multi-band|single-band}
   backoff-time <seconds>
   cellular-handoff-assist
   channel-quality-aware-arm
   channel-quality-threshold <channel-quality-threshold>
   channel-quality-wait-time <seconds>
   client-aware
   client-match
   clone <profile>
   cm-band-a-min-signal <cm-band-a-min-signal>
   cm-band-g-max-signal <cm-band-g-max-signal>
   cm-dot11v
   cm-lb-client-thresh <#-of-clients>
   cm-lb-signal-delta <cm-lb-signal-delta>
   cm-lb-snr-thresh <dB>
   cm-lb-thresh <%-of-clients>
   cm-max-steer-fails <#-of-fails>
   cm-mu-client-thresh <count>
   cm-mu-snr-thresh <value>
   cm-report-interval
   cm-stale-age <secs>
   cm-steer-timeout <secs>
   cm-sticky-check_intvl <secs>
   cm-sticky-min-signal <-dB>
   cm-sticky-snr <dB>
   cm-sticky-snr-delta
   cm-update-interval <dB>
   cm-unst-ageout-interval days <days> hours <hours>
   cm-vht-min-signal <cm-vht-min-signal>
   dynamic-bw
   dynamic-bw-beacon-failed-thresh <dynamic-bw-beacon-failed-thresh>
   dynamic-bw-cca-ibss-thresh <dynamic-bw-cca-ibss-thresh>
   dynamic-bw-cca-intf-thresh <dynamic-bw-cca-intf-thresh>
   dynamic-bw-clear-time <dynamic-bw-clear-time>
   dynamic-bw-wait-time <dynamic-bw-wait-time>
   error-rate-threshold <percent>
   error-rate-wait-time <seconds>
   free-channel-index <number>
   high-noise-backoff-time <high-noise-backoff-time>
   ideal-coverage-index <number>
   interfering-ap-weight <number>
   load-aware-scan-threshold
   max-tx-power <dBm>
   min-scan-time <# of scans>
   min-tx-power <dBm>
   mode-aware
   multi-band-scan
   no ...
   ota-updates
   ps-aware-scan
   radar-backoff-time <radar-backoff-time>
   rogue-ap-aware
```

```
scan mode {all-reg-domain|reg-domain}
scan-interval
scanning
video-aware-scan
voip-aware-scan
```

Description

This command configures the Adaptive Radio Management (ARM) profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`40MHz-allowed-bands`	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.	All/None/ a-only/g-only	a-only
`All`	Allows 40 MHz channels on both the 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.	—	—
`None`	Disallows use of 40 MHz channels.	—	—
`a-only`	Allows use of 40 MHz channels on the 5 GHZ (802.11a) frequency band only.	—	—
`g-only`	Allows use of 40 MHz channels on the 2.4 GHZ (802.11b/g) frequency band only.	—	—
`80MHz-support`	If enabled, 80 MHz channels can be used in the 5 GHz frequency band on APs that support 802.11ac.	—	enabled
`acceptable-coverage-index`	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. This setting applies to multi-band implementations only.	1-6	4
`active-scan`	When active-scan is enabled, an AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. This feature is disabled by default, and should *not be enabled* except under the direct supervision of Aruba Technical Support. Default: disabled	—	disabled
`aggressive-scan`	When this feature is enabled, an AP radio with no clients will scan channels every second.	—	enabled

Parameter	Description	Range	Default
`assignment`	Activates one of four ARM channel/power assignment modes.	—	single-band (new installations only)
`disable`	Disables ARM channel/power assignments.	—	—
`maintain`	Maintains existing channel assignments.	—	—
`multi-band`	Computes ARM assignments for both 5 GHZ (802.11a) and 2.4 GHZ (802.11b/g) frequency bands.	—	—
`single-band`	Computes ARM assignments for a single band.	—	—
`backoff-time`	Time, in seconds, an AP backs off after requesting a new channel or power.	120-3600	240 sec
`cellular-handoff -assist`	When both the ClientMatch and cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G or 4G-capable Wi-Fi device such as an iPhone, iPad, or Android client at the edge of Wi-Fi network coverage switch from Wi-Fi to an alternate 3G or 4G radio that provides better network access. This feature is disabled by default, and is recommended only for Wi-Fi hotspot deployments. **NOTE:** To configure this feature for an individual AP radio, use the command **wlan virtual-ap profile <profile> cellular-handoff-assist**.	—	disabled
`channel-quality -aware-arm`	If enabled, ARM changes are based upon an internally calculated channel quality metric. When this feature is disabled, ARM initiates channel changes based on thresholds defined in this profile, and chooses the channel based on the calculated interference index value.. Default: Disabled	—	disabled
`channel-quality -threshold`	Channel quality percentage below which ARM initiates a channel change.	0-100	70
`channel-quality -wait-time`	If channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.	1-3600	120
`client-aware`	If the Client Aware option is enabled, the AP does not change channels if there is active client traffic on that AP. If Client Aware is disabled, the AP may change to a more optimal channel, but this change may also disrupt current client traffic.	—	enabled

Parameter	Description	Range	Default
`client match`	ClientMatch helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless client's probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is enabled by default	—	enabled
`clone`	Name of an existing ARM profile from which parameter values are copied.	—	—
`cm-band-a-min-signal <cm-band-a-min-signal>`	Minimum signal level required for the targeted A band radio in a Client Match band steer move (-dBm).	—	75
`cm-band-g-max-signal <cm-band-g-max-signal>`	Maximum signal level of the G band radio that can trigger a Client Match band steer move (-dBm)	—	45
`cm-dot11v`	Client Match steers using 802.11v BSS Transition Management.	—	enabled
`cm-lb-client-thresh <#-of-clients>`	If an AP radio has fewer clients than the client match load balancing threshold defined by this parameter, the AP will not participate in load balancing.	0-100 clients	30
`cm-lb-signal-delta`	Client match will not move a client to a new radio if the signal strength of the target AP is this dB value lower than the radio to which the client is currently associated. This parameter works differently than the cm-lb-snr-thresh value, which imposes a definite value on the target AP's signal-to-noise radio. the cm-lb-signal-delta imposes a *relative* constraint based upon the signal strength of the radio to which the client is currently associated.	0-20 dB	5 dB
`cm-lb-snr-thresh <dB>`	Clients must detect a SNR from an underutilized AP radio at or above this threshold before ClientMatch considers load balancing a client to that radio.	0-100 dB	25

Parameter	Description	Range	Default
`cm-lb-thresh <%-of-clients>`	When ClientMatch is enabled, clients may be steered from a highly utilized channel on an AP to a channel with fewer clients. If a channel on an AP radio has this percentage fewer clients than another channel supported by the client, ClientMatch may move clients from the busier channel to the channel with fewer clients.	0-100 %	20
`cm-max-steer-fails <#-of-fails>`	The controller keeps track of the number of times ClientMatch failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If ClientMatch attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as unsteerable for that specific trigger. This parameter defines the maximum allowed number of client match steering fails with the same trigger before the client is marked as unsteerable for that trigger.	0-100 failures	5
`cm-mu-client-thresh <count>`	Total number of clients that can be associated to a radio, in which the radio can still be considered for multi-user (MU) steering.	—	15
`cm-mu-snr-thresh <value>`	Minimum SNR value of a client on the target radio, in which the radio can still be considered for multi-user (MU) steering.	> 25	30
`cm-report-interval <secs>`	This interval defines how often an AP sends an updated client probe report to the controller. Each client probe report contains a list of MAC addresses for clients that have been active in the last two minutes, and the AP radio SNR values seen by those clients.	0-255 secs	30
`cm-stale-age <secs>`	The controller can maintain client match data for the maximum number of supported clients for that controller platform, showing the detected SNR values for up to 16 candidate APs per client. This table is periodically updated as APs send client probe reports to the controller. This parameter defines the amount of time that the controller should retain client match data from each client probe report. Different controller types support varying numbers of clients. ■ 7005: 1024 client ■ 7010: 2048 clients ■ 7030: 4096 clients ■ 7240: 32000 clients ■ 7220: 24000 clients ■ 7210: 16000 clients	0- 65535 seconds	900 secs

Parameter	Description	Range	Default
`cm-steer-timeout`	When a client is steered from one AP to a more desirable AP, the steer timeout feature helps facilitate the move by defining the amount of time that any APs to which the client should NOT associate will not respond to the AP.	0-255 secs	
`cm-sticky-check -interval <secs>`	Frequency at which the AP checks for client's received SNR values. If the SNR value drops below the threshold defined by the **cm-sticky-snr** parameter for three consecutive check intervals, that client may be moved to an different AP.	0-255 secs	3 secs
`cm-sticky-min -signal <-dB>`	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the candidate AP radio is at or higher than the minimum signal level defined by this parameter*and* the candidate radio has a higher signal strength than the radio to which the client is currently associated. (The required improvement in signal strength can be defined using the **cm-sticky-snr-delta** command.)	0-255 (-dB)	65
`cm-sticky-snr <dB>`	If the client's received signal strength indicator (RSSI) is above this signal-to-noise ratio (SNR) threshold, that client will be allowed to stay associated to its current AP. If the client's received signal strength is below this threshold, it may be moved to a different AP.	0-255 dB	18
`cm-sticky-snr-delta`	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the AP radio is stronger than its current radio by the dB level defined by the cm-sticky-snr-thresh parameter, and the candidate radio also has a minimum signal level defined by the cm-sticky-min-signal parameter.	0-100 dB	10
`cm-unst-ageout-interval days <days> hours <hours>`	The client entries in an unsteerable client list remain in effect for the interval defined by this parameter before they age out.	—	2 days

Parameter	Description	Range	Default
`cm-unst-ageout`	When client match and the client match unsteerable client ageout feature are enabled, the controller periodically sends APs that are not a desired AP match for a client in a list of unsteerable clients. These lists contain a list of MAC addresses for up to 128 clients that should not be steered to that AP. The following controller types support a aggregate maximum of unsteerable clients for all APs associated to that controller. ■ 7005: 256 unsteerable clients ■ 7010: 512 unsteerable clients ■ 7030: 1024 unsteerable clients ■ 7240: 8000 unsteerable clients ■ 7220: 6000 unsteerable clients ■ 7210: 4000 unsteerable clients	—	—
`cm-vht-min-signal <cm-vht-min-signal>`	ArubaOS can match 802.11ac-capable (VHT) clients with 802.11ac radios under favorable channel conditions so that the clients can utilize the 80MHz channel and better MCS rates. This parameter defines the minimum radio signal detected by the client before the client will be steered to that 802.11ac radio.		
`dynamic-bw`	Issue the **dynamic-bw** parameter to enable the ARM dynamic bandwidth switch feature. When enabled ARM can detect 20MHz interferers that can impact an AP radio using an 80MHz channel and move the AP radio to another 80MHz channel. For more information, see 80MHz Dynamic Bandwidth Switch on page 841	–	disabled
`dynamic-bw-beacon-failed-thresh`	The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the number of failed beacons exceeds this value during the observation window.	1-500	30
`dynamic-bw-cca-ibss-thresh`	The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the clear channel asignment IBSS percentage drops below this value during the observation window.	1-100	10
`dynamic-bw-cca-intf-thresh`	The ARM dynamic bandwidth switch feature may trigger a change in the radio channel bandwidth if the clear channel asignment interference percentage exceeds this value during the observation window.	1-100	30

Parameter	Description	Range	Default
dynamic-bw-clear-time	The ARM dynamic bandwidth switch feature returns the AP radio to 80MHz channel after this clear time period if there is no high volume of traffic.	1-300 seconds	30
dynamic-bw-wait-time	Minimum time in seconds dynamic bandwidth switch indicators have to be true to trigger a 80MHz to 40MHz bandwidth change.	1-300 seconds	30
error-rate-threshold	The percentage of errors in the channel that triggers a channel change. Recommended value is 50%. A value of 0% disables this feature.	0-100	default-a: 70% default-g: 70%
error-rate-wait-time	Time, in seconds, that the error rate has to be at least the error rate threshold to trigger a channel change. Supported range is 1-2,147,483,647 Recommended Values: 1-100	_	default-a: 90 sec default-g: 90 sec
free-channel-index	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel. Recommended value is 25.	10-40	default-a: 40 default-g: 25
high-noise-backoff-time	The duration, in minutes, for blacklisting AirMatch Solver's channel after 2 consecutive high noise detections. Setting the value to 0 disables the backoff window.	0-3600	Default: 720 minutes (12 hours)
ideal-coverage-index	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be. Recommended value is 10.	2-20	default-a: 6 default-g: 6
load-aware-scan-threshold	Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high. The Load Aware Scan Threshold is the traffic throughput level an AP must reach before it stops scanning. The supported range for this setting is 0-20000000 bytes/second. (Specify 0 to disable this feature.)	—	1250000 bytes/second

Parameter	Description	Range	Default
max-tx-power	Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127	default-a: 18 dBm default-g: 9 dBm
min-scan-time	Minimum number of times a channel must be scanned before it is considered for assignment. The supported range for this setting is 0-2,147,483,647 scans. Best practices are to configure a Minimum Scan Time between 1-20 scans. Default: 8 scans	1-2,147,483,647 Recommended Values: 1-20	8 scans
min-tx-power	Minimum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory minimum. This value takes into account both radio transmit power and antenna gain. Higher power level settings may be constrained by local regulatory requirements and AP capabilities.	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 127	default-a: 12 dBm default-g: 6 dBm
mode-aware	If enabled, ARM will turn APs into Air Monitors (AMs) if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).	—	disabled
multi-band-scan	When enabled, single-radio APs try to scan across bands for rogue AP detection.	—	enabled
no	Negates any configured parameter.	—	—
ota-updates	The **ota-updates** option allows an AP to get information about its RF environment from its neighbors, even the AP cannot scan. If this feature is enabled, when an AP on the network scans a foreign (non-home) channel, it sends other APs an Over-the-Air (OTA) update in an 802.11 management frame that contains information about the scanning AP's home channel, the current transmission EIRP value of its home channel, and one-hop neighbors seen by that AP. Default: enabled	—	enabled
ps-aware-scan	When enabled, the AP will not scan if Power Save is active.	—	disabled

Parameter	Description	Range	Default
radar-backoff-time	The duration, in minutes, for blacklisting AirMatch solver's channel after 2 consecutive radar detections. Setting the value to 0 disables the backoff window.	0-3600	Default: 720 minutes (12 hours)
rogue-ap-aware	When enabled, the AP will try to contain off-channel rogue APs.	—	disabled
scan-interval	If scanning is enabled, the scan interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired. **Recommended Values**: 0-30 seconds	0-2,147,483, 647 seconds	10 seconds
scan-mode	Select the scan mode for the AP: ■ **all-reg-domain**: The AP scans channels within all regulatory domains. This is the default setting. ■ **reg-domain**:Limit the AP scans to just the regulatory domain for that AP.	—	all-reg-domain
scanning	The Scanning check box enables or disables AP scanning across multiple channels. Disabling this option also disables the following scanning features: ■ Multi Band Scan ■ Rogue AP Aware ■ Voip Aware Scan ■ Power Save Scan Do not disable Scanning unless you want to disable ARM and manually configure AP channel and transmission power.	—	enabled
video-aware-scan	As long as there is at least one video frame every 100 mSec the AP will reject an ARM scanning request. Note that for each radio interface, video frames must be defined in one of two ways: ■ Classify the frame as video traffic via a session ACL. ■ Enable WMM on the WLAN's SSID profile and define a specific DSCP value as a video stream. Next, create a session ACL to tag the video traffic with the that DSCP value.	—	enabled

Parameter	Description	Range	Default
`voip-aware-scan`	Aruba's VoIP Intelligent Call Handling (ICH) prevents any single AP from becoming congested with voice calls. When you enable ICH, you should also enable **voip-aware-scan** parameter in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that **scanning** is also enabled.	—	disabled

Usage Guidelines

Adaptive Radio Management (ARM) is a radio frequency (RF) resource allocation algorithm that allows each AP to determine the optimum channel selection and transmit power setting to minimize interference and maximize coverage and throughput. This command configures an ARM profile that you apply to a radio profile for the 5 GHz or 2.4 GHz frequency band (see rf dot11a-radio-profile on page 843 or rf dot11g-radio-profile on page 854).

Default Profiles

ArubaOS includes two default ARM profiles, **default-a** for 5 Ghz radios, and **default-g** for 2.4 GHz radios. Previous 6.4.x releases support a single **default** ARM profile applicable to both radio bands.

When you upgrade to ArubaOS 6.4.4.0 or later from a pre-6.4.4.0 release, any changes made to the **default** ARM profile will be applied to the new **default-a** and **default-g** profiles. If the **default** profile was *not* modified, that profile will be removed after the upgrade, when the **default-a** and **default-g** profiles are created. Note that any user-created profiles will not be modified during the upgrade, and will retain all their existing values.

Channel Quality

Hybrid APs and Spectrum Monitors determine channel quality by measuring channel noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of Wi-Fi retries. Regular APs using ARM derive channel quality values by measuring the noise floor for that channel.

Client Match

The ARM client match feature continually monitors a client's RF neighborhood to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients. This feature is recommended over the legacy bandsteering and spectrum load balancing features, which, unlike client match, do not trigger AP changes for clients already associated to an AP.

Legacy 802.11a/b/g devices do not support ClientMatch. When client match is enabled on 802.11n-capable devices, ClientMatch overrides any settings configured for the legacy bandsteering, station handoff assist or load balancing features. 802.11ac-capable devices do not support the legacy bandsteering, station hand off or load balancing settings, so these APs must be managed on using client match.

When this feature is enabled on an AP, that AP is responsible for measuring the RF health of its associated clients. The AP receives and collects information about clients in its neighborhood, and periodically sends this information to the controller. The controller aggregates and maintains a database of information about AP transmit power elvels, client transmit power levels and AP RSSI levels as seen by clients. The controller shares this database with the APs (for their associated clients) and the APs use the information to compute the client-based RF neighborhood and determine which APs should be considered candidate APs for each client. When the controller receives a client steer request from an AP, the controller identifies the optimal AP candidate and

manages the client's relocation to the desired radio. This is an improvement from previous releases, where ARM was managed exclusively by APs, the without the larger perspective of the client's RF neighborhood.

The following client/AP mismatch conditions are managed by ClientMatch:

- **Load Balancing**: Client match balances clients across APs on different channels, based upon the client load on the APs and the SNR levels the client detects from an underutilized AP. If an AP radio can support additional clients, the AP will participate in client match load balancing and clients can be directed to that AP radio, subject to predefined SNR thresholds.
- **Sticky Clients**: ClientMatch also helps mobile clients that tend to stay associated to an AP despite low signal levels. APs using client match continually monitor the client's RSSI as it roams between APs, and move the client to an AP when a better radio match can be found. This prevents mobile clients from remaining associated to an APs with less than ideal RSSI, which can cause poor connectivity and reduce performance for other clients associated with that AP.
- **Band Steering/Band Balancing**: APs using ClientMatch monitor the RSSI for clients that advertise a dual-band capability. If a client is currently associated to a 2.4 GHz radio and the AP detects that the client has a good RSSI from the 5 Ghz radio, the controller will attempt to steer the client to the 5 Ghz radio, as long as the 5 Ghz RSSI is not significantly worse than the 2.4 GHz RSSI, and the AP retains a suitable distribution of clients on each of its radios.

80MHz Dynamic Bandwidth Switch

If an AP radio uses an 80MHz channel, the radio only sends out frames out when the entire 80MHz channel is clear, even if the AP is sending only a 20MHz management frame or 40MHz data frame. As a result, throughput on the selected 80 MHz channel can be negatively impacted if interference occurs on both 20MHz channels of the secondary 40MHz channel.

The ARM dynamic bandwidth switch feature allows ARM to detect the 20MHz interferers in this situation, and potentially move the AP radio to another 80MHz channel, or change the AP transmissions to 40MHz, and use the primary 40MHz channel instead.

When this feature is enabled, ARM starts a dynamic bandwidth switch observation window if load-aware scan rejects increase, *and* the clear channel assignment IBSS percentage (the percentage of channel traffic sent from that AP radio) drops below the value defined by the **dynamic-bw-cca-ibss-thresh** parameter.

If an observation window opens, and the clear channel assignment interference threshold exceeds the value defined by the **dynamic-bw-cca- intf-thresh** parameter, and the number of failed beacons from the radio exceeds the threshold defined by the **dynamic-bw-beacon- failed-thresh** parameter during that observation period, ARM will move the AP to another available 80MHz channel with the minimum interference index. If no other 80MHz channel si available, ARM downgrades the radio bandwidth to 40MHz.

ARM Scanning

The default ARM scanning interval is determined by the **scan-interval** parameter in the ARM profile. If the AP does not have any associated clients (or if most of its clients are inactive) ARM will dynamically readjust this default scan interval, allowing the AP obtain better information about its RF neighborhood by scanning non-home channels more frequently. Starting with ArubaOS 6.2, if an AP attempts to scan a non-home channel but is unsuccessful, the AP will make additional attempts to rescan that channel before skipping it and continuing on to other channels.

Using Adaptive Radio Management (ARM) in a Mesh Network

When a mesh portal operates on a mesh network, the mesh portal determines the channel used by the mesh feature. When a mesh point locates an upstream mesh portal, it will scan the regulatory domain channels list to determine the channel assigned to it, for a mesh point always uses the channel selected by its mesh portal. However, if a mesh portal uses an ARM profile enabled with a single-band or multi-band channel/power

assignment and the scanning feature, the mesh portal will scan the configured channel lists and the ARM algorithm will assign the proper channel to the mesh portal.

If you are using ARM in your network, is important to note that mesh points, unlike mesh portals, do not scan channels. This means that once a mesh point has selected a mesh portal or an upstream mesh point, it will tune to this channel, form the link, and will not scan again unless the mesh link gets broken. This provides good mesh link stability, but may adversely affect system throughput in networks with mesh portals and mesh points. When ARM assigns optimal channels to mesh portals, those portals use different channels, and once the mesh network has formed and all the mesh points have selected a portal (or upstream mesh point), those mesh points will not be able to detect other portals on other channels that could offer better throughput. This type of suboptimal mesh network may form if, for example, two or three mesh points select the same mesh portal after booting, form the mesh network, and leave a nearby mesh portal without any mesh points. Again, this will not affect mesh functionality, but may affect total system throughput.

Example

The following command configures VoIP-aware scanning for the arm-profile named “voice-arm:”

```
(host) [mynode] (config) #rf arm-profile voice-arm
  voip-aware-scan
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **high-noise-backoff-time** and **radar-backoff-time** parameters were added.
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

rf dot11a-radio-profile

```
rf dot11a-radio-profile <profile>
   am-scan-profile <profile-name>
   arm-profile <profile>
   beacon-period <milliseconds>
   beacon-regulate
   cap-reg-eirp <cap-reg-eirp>
   cell-size-reduction <cell-size-reduction>
   channel <num|num+|num->
   channel-reuse {static|dynamic|disable}
   channel-reuse-threshold
   clone <profile>
   csa
   csa-count <number>
   deploy-hour <deploy-hour>
   disable-arm-wids-function
   dot11h
   eirp-max <eirp-max>
   eirp-min <eirp-min>
   eirp-offset <eirp-offset>
   energy-detect-threshold <energy-detect-threshold>
   high-throughput-enable
   ht-radio-profile <profile>
   interference-immunity
   max-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
   maximum-distance <maximum-distance>
   mgmt-frame-throttle-interval <seconds>
   mgmt-frame-throttle-limit <number>
   min-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
   mode {ap-mode|am-mode|spectrum-mode}
   no ...
   radar-test-mode
   radio-enable
   slb-mode channel|radio
   slb-threshold
   slb-update-interval <secs>
   spectrum-load-bal-domain
   spectrum-load-balancing
   spectrum-monitoring
   spectrum-profile <profile>
   spur-immunity <spur-immunity>
   transmit
   tx-power <dBm>
   very-high-throughput-enable
```

Description

This command configures AP radio settings for the 5 GHz frequency band, including the Adaptive Radio Management (ARM) profile for standalone controllers and the high-throughput (802.11n) radio profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`am-scan-profile <name>`	Configure an Air Monitor (AM) scanning profile	—	“default”
`arm-profile`	Configures Adaptive Radio Management (ARM) feature. See rf arm-profile on page 830.	—	“default”
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP’s presence, identity, and radio characteristics to wireless clients.	60 (minimum)	100 milli-seconds
`beacon-regulate`	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.	—	disabled
`cap-reg-eirp <cap-reg-eirp>`	Work around a known issue on Cisco 7921G telephones by specifying a cap for a radio’s maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.	1–31 dBm.	
`cell-size-reduction <cell-size-reduction>`	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP’s receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. This value should only be changed if the network is experiencing performance issues. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value. Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio’s transmission (Tx) power to match its new received (Rx) power level. Failure to match a device’s Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.	1-5 5dB	0 dB

Parameter	Description	Range	Default
`channel`	Channel number for the AP 802.11a/802.11n/802.11ac physical layer. This parameter is only supported on a standalone controller, and is not available in the Mobility Master command-line interface. The available channels depend on the regulatory domain (country). Channel number configuration options for 20 MHz, 40 MHz, and 80 Mhz modes: ■ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ■ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ■ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel. **NOTE:** 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.	Depends on regulatory domain	—

Parameter	Description	Range	Default
`channel-reuse`	When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.) ■ Static mode: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ Dynamic mode: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ Disable mode: This mode does not support the tuning of the CCA Detect Threshold.	enabled disabled	enabled
`channel-reuse-threshold`	RX Sensitivity Tuning Based Channel Reuse Threshold, in - dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold.	Depends on regulatory domain	—
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`csa`	Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.	—	disabled
`csa-count`	Number of CSA announcements that are sent before the AP begins transmitting on the new channel.	1-16	4

Parameter	Description	Range	Default
`deploy-hour <0-23>`	Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Master, the AirMatch solution will be deployed according to the time zone of the managed device. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller. If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence	0-23	5
`disable-arm-wids-function`	Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option. CAUTION: Use carefully, since this effectively disables ARM and WIDS	1-16	4
`dot11h`	Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities. This parameter is disabled by default.	—	disabled
`eirp-max <eirp-max>`	Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	1-127	18
`eirp-min <eirp-min>`	The minimum transmission power level (in dBm) to be assigned to the AP radio(s). **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	1-127	12
`eirp-offset`	Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	-6 to 6 dBm	0 dBm

Parameter	Description	Range	Default
energy-detect-threshold	Modify the Energy Detect Threshold (EDT) used by the radio in making transmit decisions. The EDT is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. Specify a value of 0 to use the default EDT for this radio. (This value may vary by AP model) **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	0, 1-12	0 (disabled)
high-throughput-enable	Enables high-throughput (802.11n) features on a radio using the 5 GHz frequency band.	—	enabled
ht-radio-profile	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See rf ht-radio-profile on page 875.	—	“default-a”
interference-immunity	Set a value for 802.11 interference immunity. This parameter sets the interference immunity on the 2.4 Ghz band. The default setting for this parameter is level 2. When performance drops due to interference from non- 802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: ■ Level 0: no ANI adaptation. ■ Level 1: noise immunity only. ■ Level 2: noise and spur immunity. ■ Level 3: level 2 and weak OFDM immunity. ■ Level 4: level 3 and FIR immunity. ■ Level 5: disable PHY reporting. **NOTE:** Do not raise the noise immunity feature’s default setting if the channel-reuse-threshold on page 846 feature is also enabled. A level-3 to level-5 Noise Immunity setting is not compatible with the Channel Reuse feature. **NOTE:** It is recommended not to adjust interference immunity without guidance from Aruba support.	Level-0 - Level-5	Level-2
max-channel-bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Master managed devices. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	20MHz, 40MHz, 80MHz or 160MHz	80MHz

Parameter	Description	Range	Default
`minimum-channel-band-width`	Sets the minimum channel bandwidth for APs associated to Mobility Master managed devices. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	20MHz, 40MHz, 80MHz	20MHz
`maximum-distance`	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km. The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 5 GHz frequency band radio: ■ 20MHz mode: 58km ■ 40MHz mode: 27km Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.	0-57km (40MHz mode) 0-27km (20MHz mode)	0 meters
`mgmt-frame-throttle-interval`	Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-60	1 second interval
`mgmt-frame-throttle-limit`	Maximum number of management frames allowed in each throttle interval. **NOTE:** This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-999999	20 frames per interval
`mode`	One of the operating modes for the AP.		ap-mode
`ap-mode`	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.	—	—
`am-mode`	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.	—	—
`spectrum-mode`	Device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.	—	—
`no`	Negates any configured parameter.	—	—
`radar-test-mode`	For internal use only.	—	—
`radio-enable`	Enables or disables radio configuration.	—	enabled

Parameter	Description	Range	Default
`slb-mode channel|radio`	SLB Mode allows control over how to balance clients. Select one of the following options ■ channel: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ radio: Radio-based load-balancing balances clients across APs		channel
`slb-update-interval <secs>`	Specify how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.	1-2147483647 seconds	30 seconds
`smart-antenna`	Enable or disable the smart antenna feature on AP-335 access points.	enabled disabled	enabled
`spectrum-load-bal -domain`	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment. ■ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is not defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain isalso defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.	—	—
`spectrum-load-balancing`	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.	—	disabled

Parameter	Description	Range	Default
`spectrum-monitoring`	Issue this command to turn APs in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel. For further details on using hybrid APs and spectrum monitors to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, refer to the Spectrum Analysis chapter of the ArubaOS User Guide. For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.3.0.x User Guide.	—	default
`spectrum-profile <profile>`	Specify the rf spectrum profile used by hybrid APs and spectrum monitors. This profile sets the spectrum band and device ageout times used by a spectrum monitor or hybrid AP radio. For details, see rf spectrum-profile on page 879.	—	default
`spur-immunity <spur-immunity>`	Spur Immunity for 5 GHz radio. This parameter fine-tunes the Cyclic Power Threshold (CPT) of a 5 GHz radio. The value specified here is the offset from the base value of 2 dB (for example, setting the CPT value to 1 corresponds to 2 + 1 = 3 dB. Similarly, setting the CPT value to 10 corresponds to 2+10 = 12 dB). Use this parameter when high channel utilization is observed in the 5 GHz radio of 130 Series access points in a noise-free environment causing client association or throughput issues. Adjust the CPT value to eliminate the spur impacts. Range definition is as follows: ■ 0: default CPT ■ 1-19: CPT growth from default (3 dB to 21 dB) ■ 20: Setting this parameter to 20 sets the cell-size-reduction value to 1. Cell-size-reduction is the receive coverage area of the AP. **NOTE:** Configure this parameter under the supervision of Aruba Technical Support. **NOTE:** Setting the spur immunity to a higher value may decrease the AP RF coverage. **NOTE:** This parameter is applicable for 130 Series access points only. The controller ignores this parameter if configured for non-130 Series access points.	0-20 CPT	0 CPT
`transmit`	Enable or dzisable transmission of frames on the radio. **NOTE:** This parameter should only be used for radio test purposes.	enabled disabled	disabled

Parameter	Description	Range	Default
`tx-power`	Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through calibration. This parameter is only supported on a standalone controller, and is not available in the Mobility Master command-line interface. This parameter can be set from -51 to 51 in 0.1 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities. **NOTE:** Use this parameter to set transmit power levels for APs associated to a stand-alone controller not using ARM.	-51 dBm to 51 dBm	14 dBm
`very-high-throughput-enable`	Enable or disable support for Very High Throughput (802.11ac) on the radio.	—	Enabled

Usage Guidelines

This command configures radios that operate in the 5 GHz frequency band, which includes radios utilizing the IEEE 802.11a or IEEE 802.11n standard. Channels must be valid for the country configured in the AP regulatory domain profile (see ap regulatory-domain-profile on page 239).To view the supported channels, use the **show ap allowed-channels** command.

APs initially start up with default **ack-timeout**, **cts-timeout** and **slot-time** values. When you modify the **maximum-distance** parameter in an rf dot11a radio profile or rf dot11g radio profile, new **ack-timeout**, **cts-timeout** and **slot-time** values may be derived, but those values are never less then the default values for an indoor AP.

Mesh radios on outdoor APs have additional constraints, as mesh links may need to span long distances. For mesh radios on outdoor APs, the effect of the default **maximum-distance** parameter on the **ack-timeout**, **cts-timeout** and **slot-time** values depends on whether the APs are configured as mesh portals or mesh points. This is because mesh portals use a default **maximum-distance** value of 16,050 meters, and mesh points use, by default, the maximum possible **maximum-distance** value.

The **maximum-distance** value should be set correctly to span the largest link distance in the mesh network so that when a mesh point gets the configuration from the network it will apply the correct **ack-timeout**, **cts-timeout** and **slot-time** values.The values derived from the **maximum-distance** setting depend on the band and whether 20Mhz/40MHz mode of operation is in use.

The following table indicates values for a range of distances:

Timeouts[usec]	--- 5GHz radio ---			--- 2.4GHz radio ---		
Distance[m]	Ack	CTS	Slot	Ack	CTS	Slot
0 (outdoor:16050m)	128	128	63	128	128	63
0 (indoor:600a,6450g)	25	25	9	64	48	9
200 (==default)	25	25	9	64	48	9
500	25	25	9	64	48	9
600	25	25	9	64	48	9
1050	28	28	13	64	48	31
5100	55	55	26	64	55	31
10050	88	88	43	88	88	43
15000	121	121	59	121	121	59
16050	128	128	63	128	128	63
58200(5G limit 20M)	409	409	203	-	-	-

```
52650(2.4G limit 20M) -          -         -        372        372       185
27450(5G limit 40M)   204        204       101      -          -         -
24750(2.4G limit 40M) -          -         -        186        186       92
```

Examples

The following command configures APs to operate in AM mode for the selected dot11a-radio-profile named "sample-a:"

```
(host)[node](config) #rf dot11a-radio-profile sample-a mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 5 Ghz frequency band for the selected dot11a-radio profile named "samplea-" and assigns a high-throughout radio profile named "default-a:"

```
            (host)[node](config) #rf dot11a-radio-profile sample-a
  high-throughput-enable
  ht-radio-profile default-a
```

The following command configures a primary channel number of 157 and a secondary channel number of 161 for 40 MHz mode of operation with a dot11a-radio profile named "sample-a:"

```
(host)[node](config) #rf dot11a-radio-profile sample-a channel <157+>
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Modified the range of the **eirp-max** and **eirp-min** parameters.
ArubaOS 8.1.0.0	The **deploy-hour**, **eirp-offset**, **energy-detect-threshold,** and **minimum-channel-bandwidth** parameters were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms.	Base operating system	Config mode on Mobility Master.

rf dot11g-radio-profile

```
rf dot11g-radio-profile <profile>
   am-scan-profile <profile-name>
   arm-profile <profile>
   beacon-period <milliseconds>
   beacon-regulate
   cap-reg-eirp <cap-reg-eirp>
   cell-size-reduction <cell-size-reduction>
   channel <num|num+|num->
   channel-reuse {static|dynamic|disable}
   channel-reuse-threshold
   clone <profile>
   csa
   csa-count <number>
   deploy-hour <deploy-hour>
   disable-arm-wids-function
   dot11b-protection
   dot11h
   eirp-max 3|6|9|12|15|18|21|24|27|30|33|127
   eirp-min 3|6|9|12|15|18|21|24|27|30|33|127
   eirp-offset <eirp-offset>
   energy-detect-threshold <energy-detect-threshold>
   high-throughput-enable
   ht-radio-profile <profile>
   interference-immunity
   max-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
   maximum-distance <maximum-distance>
   mgmt-frame-throttle-interval <seconds>
   mgmt-frame-throttle-limit <number>
   min-channel-bandwidth 20MHz|40MHz|80MHz|160MHz
   mode {ap-mode|am-mode|spectrum-mode}
   no ...
   radio-enable
   slb-mode channel|radio
   slb-threshold
   slb-update-interval <secs>
   smart-antenna
   spectrum-load-bal-domain
   spectrum-load-balancing
   spectrum-monitoring
   spectrum-profile
   transmit
   tx-power <dBm>
   very-high-throughput-enable
```

Description

This command configures AP radio settings for the 2.4 GHz frequency band, including the Adaptive Radio Management (ARM) profile and the high-throughput (802.11n) radio profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`am-scan-profile <profile-name>`	Configure an Air Monitor (AM) scanning profile.	—	—
`arm-profile`	Configures Adaptive Radio Management (ARM) feature. See rf arm-profile on page 830.	—	“default”
`beacon-period`	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP’s presence, identity, and radio characteristics to wireless clients.	60 (minimum)	100 milliseconds
`beacon-regulate`	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.	—	disabled
`cap-reg-eirp <cap-reg-eirp>`	Work around a known issue on Cisco 7921G telephones by specifying a cap for a radio’s maximum equivalent isotropic radiated power (EIRP). When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.	1–31 dBm.	

Parameter	Description	Range	Default
`cell-size-reduction <cell-size-reduction>`	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. This value should only be changed if the network is experiencing performance issues. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value. Values from 1 dB - 55 dB reduce the power level that the radio can hear by that amount. If you configure this feature to use a non-default value, you must also reduce the radio's transmission (Tx) power to match its new received (Rx) power level. Failure to match a device's Tx power level to its Rx power level can result in a configuration that allows the radio to send messages to a device that it cannot hear.	1-5 5dB	0 dB

Parameter	Description	Range	Default
`channel`	Channel number for the AP 802.11g/802.11n.802.11ac physical layer. The available channels depend on the regulatory domain (country). This parameter is only supported on a standalone controller, and is not available in the Mobility Master command-line interface. Channel number configuration options for 20 MHz, 40 MHz, and 80 Mhz modes: ■ num: Entering a channel number disables 40 MHz mode and activates 20 MHz mode for the entered channel. ■ num+: Entering a channel number with a plus (+) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by increasing the primary channel number by 4. Example: 157+ represents 157 as the primary channel and 161 as the secondary channel. ■ num-: Entering a channel number with a minus (-) sign selects a primary and secondary channel for 40 MHz and 80 Mhz modes. The number entered becomes the primary channel and the secondary channel is determined by decreasing the primary channel number by 4. Example: 157- represents 157 as the primary channel and 153 as the secondary channel.	Depends on regulatory domain	—

Parameter	Description	Range	Default
	NOTE: 20 MHz clients are allowed to associate when a primary and secondary channel are configured; however, the client will only use the primary channel.		
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`csa`	Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption.	—	disabled
`csa-count`	Number of CSA announcements that are sent before the AP begins transmitting on the new channel.	1-16	4

Parameter	Description	Range	Default
`channel-reuse`	When you enable the channel reuse feature, it can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.) ■ **Static mode**: This mode of operation is a coverage-based adaptation of the Clear Channel Assessment (CCA) thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ **Dynamic mode**: In this mode, the Clear Channel Assessment (CCA) thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ **Disable mode**: This mode does not support the tuning of the CCA Detect Threshold.	enabled disabled	enabled

Parameter	Description	Range	Default
`channel-reuse-threshold`	RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold.	depends on regulatory domain	—
`deploy-hour <0-23>`	Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Master, the AirMatch solution will be deployed according to the time zone of the managed device. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller. If this parameter is set in both the AirMatch profile and the 802.11g radio profile, the setting in the 802.11g radio profile will take precedence.	0-23	5
`disable-arm-wids-function`	Disables Adaptive Radio Management (ARM) and Wireless IDS functions. These can be disabled if a small increase in packet processing performance is desired. If a radio is configured to operate in Air Monitor mode, then these functions are always enabled irrespective of this option. CAUTION: Use carefully, since this effectively disables ARM and WIDS	1-16	4

Parameter	Description	Range	Default
`dot11b-protection`	Enable or disable protection for 802.11b clients. This parameter is enabled by default. Disabling this feature may improve performance if there are no 802.11b clients on the WLAN. WARNING: Disabling protection violates the 802.11 standard and may cause interoperability issues. If this feature is disabled on a WLAN with 802.11b clients, the 802.11b clients will not detect an 802.11g client talking and can potentially transmit at the same time, thus garbling both frames.	—	enabled
`dot11h`	Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities This parameter is disabled by default.	—	disabled
`eirp-max`	Maximum effective isotropic radiated power (EIRP) from 3 to 33 dBm in 3 dBm increments. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33 or 127	9
`eirp-min`	The minimum transmission power level (in dBm) to be assigned to the AP radio(s). **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33 or 127	6

Parameter	Description	Range	Default
`eirp-offset`	Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	-6 to 6 dBm	0 dBm
`energy-detect-threshold`	Modify the Energy Detect Threshold (EDT) used by the radio in making transmit decisions. The EDT is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. Specify a value of 0 to use the default EDT for this radio. (This value may vary by AP model)	0, 1-12	0 (disabled)
`high-throughput-enable`	Enables high-throughput (802.11n) features on a radio using the 2.4 GHz frequency band.	—	enabled
`ht-radio-profile`	Name of high-throughput radio profile to use for configuring high-throughput support on the 5 GHz frequency band. See rf ht-radio-profile on page 875.	—	“default-a”

Parameter	Description	Range	Default
`interference-immunity`	Set a value for 802.11 interference immunity. This parameter sets the interference immunity on the 2.4 Ghz band. The default setting for this parameter is level 2. When performance drops due to interference from non- 802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: ■ Level 0: no ANI adaptation. ■ Level 1: noise immunity only. ■ Level 2: noise and spur immunity. ■ Level 3: level 2 and weak OFDM immunity. ■ Level 4: level 3 and FIR immunity. ■ Level 5: disable PHY reporting. **NOTE:** Do not raise the noise immunity feature's default setting if the channel-reuse-threshold on page 846 feature is also enabled. A level-3 to level-5 Noise Immunity setting is not compatible with the Channel Reuse feature. **NOTE:** It is recommended not to adjust interference immunity without guidance from Aruba support.	Level-0 - Level-5	Level-2

Parameter	Description	Range	Default
`max-channel-bandwidth`	Sets the maximum channel bandwidth for APs associated to Mobility Master managed devices. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	20MHz, 40MHz, 80MHz or 160MHz	80MHz
`min-channel-bandwidth`	Sets the minimum channel bandwidth for APs associated to Mobility Master managed devices. **NOTE:** This parameter is only supported on Mobility Master, and is not available in on a standalone controller.	20MHz, 40MHz, 80MHz	20MHz
`maximum-distance`	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km. The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 2.4GHz frequency band radio: ■ 20MHz mode: 54km ■ 40MHz mode: 24km Note that if you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600m will use default settings.	0-24km (40MHz mode) 0-54km (20MHz mode)	0 meters

Parameter	Description	Range	Default
`mgmt-frame-throttle-interval`	Averaging interval for rate limiting management frames in seconds. Zero disables rate limiting. Note: This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-60	1 second interval
`mgmt-frame-throttle-limit`	Maximum number of management frames allowed in each throttle interval. **NOTE:** This parameter only applies to AUTH and ASSOC/RE-ASSOC management frames.	0-999999	20 frames per interval
`mode`	One of the operating modes for the AP.		ap-mode
`ap-mode`	Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN.		
`am-mode`	Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.		
`spectrum-mode`	Device operates as an spectrum monitor, and can send spectrum analysis data to a desktop or laptop client. For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.3.0.x User Guide.		
`no`	Negates any configured parameter.	—	—
`radio-enable`	Enables or disables radio configuration.	—	enabled

Parameter	Description	Range	Default
`slb-mode channel|radio`	SLB Mode allows control over how to balance clients. Select one of the following options: ■ **channel**: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ **radio**: Radio-based load-balancing balances clients across APs		channel
`slb-threshold`	If the spectrum load balancing feature is enabled, this parameter controls the percentage difference between number of clients on a channel that triggers load balancing. The default value is 20%, meaning that spectrum load balancing is activated when there are 20% more clients on one channel than on another channel used by the AP radio.	1-100%	20%
`slb-update-interval <secs>`	Specify how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.	1-2147483647 seconds	30 seconds
`smart-antenna`	Enable or disable the smart antenna feature on AP-335 access points.	enabled disabled	enabled

Parameter	Description	Range	Default
`spectrum-load-bal-domain`	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled Adaptive Radio Management (ARM) scanning and channel assignment. ■ If spectrum load balancing is enabled in a 802.11g radio profile but the spectrum load balancing domain is *not* defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11g radio profile and a spectrum load balancing domain *isalso* defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.	—	—

Parameter	Description	Range	Default
`spectrum-load-balancing`	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.	—	disabled
`spectrum-monitoring`	Issue this command to turn APs in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel. For further details on using hybrid APs and spectrum monitors to examine the radio frequency (RF) environment in which the Wi-Fi network is operating, refer to the Spectrum Analysis chapter of the ArubaOS User Guide. For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.3.0.x User Guide.	—	default

Parameter	Description	Range	Default
`spectrum-profile <profile>`	Specify the rf spectrum profile used by hybrid APs and spectrum monitors. This profile sets the spectrum band and device ageout times used by a spectrum monitor or hybrid AP radio. For details, see rf spectrum-profile on page 879.	—	default
`transmit`	Enable or disable transmission of frames on the radio. **NOTE:** This parameter should only be used for radio test purposes.	enabled disabled	disabled
`tx-power`	Sets the initial transmit power (dBm) on which the AP operates, unless a better choice is available through calibration. This parameter can be set from -51 to 51 in 0.1 dBm increments, or set to the regulatory maximum value of 127 dBm. Transmission power may be further limited by regulatory domain constraints and AP capabilities. **NOTE:** This parameter is only supported on a standalone controller, and is not available in the Mobility Master command-line interface.	-51 dBm to 51 dBm	14 dBm

Parameter	Description	Range	Default
`very-high-throughput-rates-enable`	This feature enables Very High Throughput (VHT) rates on the 2.4 GHz band, providing 256-QAM modulation and encoding that allows for 600 Mbit/sec performance over 802.11n networks. Maximum data rates are increased on the 2.4 GHz band through the addition of VHT Modulation and Coding Scheme (MCS) values 8 and 9, which support the highly efficient modulation rates in 256-QAM. Starting with ArubaOS 6.4.2.0, VHT is supported on 220 Series access points on both 20 and 40 MHz channels. Using the controller's CLI or WebUI, VHT MCS values 0-9 are enabled, overriding the existing high-throughput (HT) MCS values 0-7, which have a lower maximum data rate. However, this feature should be disabled if individual rate selection is required.	—	disabled

Usage Guidelines

This command configures radios that operate in the 2.4 GHz frequency band, which includes radios utilizing the IEEE 802.11b/g or IEEE 802.11n standard. Channels must be valid for the country configured in the AP regulatory domain profile (see ap regulatory-domain-profile on page 239).To view the supported channels, use the **show ap allowed-channels** command.

APs initially start up with default **ack-timeout**, **cts-timeout** and **slot-time** values. When you modify the **maximum-distance** parameter in an rf dot11a radio profile or rf dot11g radio profile, new **ack-timeout**, **cts-timeout** and **slot-time** values may be derived, but those values are never less then the default values for an indoor AP.

Mesh radios on outdoor APs have additional constraints, as mesh links may need to span long distances. For mesh radios on outdoor APs, the effect of the default **maximum-distance** parameter on the **ack-timeout**, **cts-timeout** and **slot-time** values depends on whether the APs are configured as mesh portals or mesh points. This is because mesh portals use a default **maximum-distance** value of 16,050 meters, and mesh points use, by default, the maximum possible **maximum-distance** value.

The **maximum-distance** value should be set correctly to span the largest link distance in the mesh network so that when a mesh point gets the configuration from the network it will apply the correct **ack-timeout**, **cts-timeout** and **slot-time** values. The values derived from the **maximum-distance** setting depend on the band and whether 20Mhz/40MHz mode of operation is in use.

The following table indicates values for a range of distances:

```
Timeouts[usec] --- 5GHz radio ---        --- 2.4GHz radio ---
```

```
Distance[m]           Ack       CTS     Slot      Ack       CTS     Slot
-------------------------------------------------------------------------
0 (outdoor:16050m)    128       128       63      128       128       63
0 (indoor:600a,6450g)  25        25        9       64        48        9
200 (==default)        25        25        9       64        48        9
500                    25        25        9       64        48        9
600                    25        25        9       64        48        9
1050                   28        28       13       64        48       31
5100                   55        55       26       64        55       31
10050                  88        88       43       88        88       43
15000                 121       121       59      121       121       59
16050                 128       128       63      128       128       63
58200(5G limit 20M)   409       409      203        -         -        -
52650(2.4G limit 20M) -          -        -       372       372      185
27450(5G limit 40M)   204       204      101        -         -        -
24750(2.4G limit 40M) -          -        -       186       186       92
```

Examples

The following command configures APs to operate in AM mode for the selected dot11g-radio-profile named “sample-g:”

```
(host)[mynode](config)#rf dot11g-radio-profile sample-g
  mode am-mode
```

The following command configures APs to operate in high-throughput (802.11n) mode on the 2.4 Ghz frequency band for the selected dot11g-radio profile named “sample-g” and assigns a high-throughout radio profile named “default-g:”

```
(host)[mynode](config)#rf dot11g-radio-profile sample-g
  high-throughput-enable
  ht-radio-profile default-g
```

The following command configures a primary channel number of 1 and a secondary channel number of 5 for 40 MHz mode of operation with the dot11g-radio profile named “sample-g:”

```
(host)[mynode](config)# rf dot11g-radio-profile sample-g channel <1+>
```

Command History

Release	Modification
ArubaOS 8.1.0.0	The **deploy-hour**, **eirp-offset**, **energy-detect-threshold,** and **minimum-channel-bandwidth** parameters were introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

rf event-thresholds-profile

```
rf event-thresholds-profile <profile>
   bwr-high-wm <percent>
   bwr-low-wm <percent>
   clone <profile>
   detect-frame-rate-anomalies
   fer-high-wm <percent>
   fer-low-wm <percent>
   ffr-high-wm <percent>
   ffr-low-wm <percent>
   flsr-high-wm <percent>
   flsr-low-wm <percent>
   fnur-high-wm <percent>
   fnur-low-wm <percent>
   frer-high-wm <percent>
   frer-low-wm <percent>
   frr-high-wm <percent>
   frr-low-wm <percent>
   no ...
```

Description

This command configures the event thresholds profile.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`bwr-high-wm`	If bandwidth in an AP exceeds this value, a bandwidth exceeded condition exists. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.	0-100	0%
`bwr-low-wm`	After a bandwidth exceeded condition exists, the condition persists until bandwidth drops below this value. The recommended value is 70%.	0-100	0%
`clone`	Name of an existing radio profile from which parameter values are copied.	—	—
`detect-frame-rate-anomalies`	Enable or disables detection of frame rate anomalies.	—	disabled
`fer-high-wm`	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, a frame error rate exceeded condition exists. The recommended value is 16%.	0-100	0%

Parameter	Description	Range	Default
`fer-low-wm`	After a frame error rate exceeded condition exists, the condition persists until the frame error rate drops below this value. The recommended value is 8%.	0-100	0%
`ffr-high-wm`	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, a frame fragmentation rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`ffr-low-wm`	After a frame fragmentation rate exceeded condition exists, the condition persists until the frame fragmentation rate drops below this value. The recommended value is 8%.	0-100	8%
`flsr-high-wm`	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, a low-speed rate exceeded condition exists. This could indicate a coverage hole. The recommended value is 16%.	0-100	16%
`flsr-low-wm`	After a low-speed rate exceeded condition exists, the condition persists until the percentage of low-speed frames drops below this value. The recommended value is 8%.	0-100	8%
`fnur-high-wm`	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, a non-unicast rate exceeded condition exists. This value depends upon the applications used on the network.	0-100	0%
`fnur-low-wm`	After a non-unicast rate exceeded condition exists, the condition persists until the non-unicast rate drops below this value.	0-100	0%
`frer-high-wm`	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, a frame receive error rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`frer-low-wm`	After a frame receive error rate exceeded condition exists, the condition persists until the frame receive error rate drops below this value. The recommended value is 8%.	0-100	8%
`frr-high-wm`	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, a frame retry rate exceeded condition exists. The recommended value is 16%.	0-100	16%
`frr-low-wm`	After a frame retry rate exceeded condition exists, the condition persists until the frame retry rate drops below this value. The recommended value is 8%.	0-100	8%
`no`	Negates any configured parameter.	—	—

Usage Guidelines

The event threshold profile configures Received Signal Strength Indication (RSSI) metrics. When certain RF parameters are exceeded, these events can signal excessive load on the network, excessive interference, or faulty equipment. This profile and many of the detection parameters are disabled (value is 0) by default.

Example

The following command configures an event threshold profile:

```
(host)[node](config) #rf event-thresholds-profile et1
   detect-frame-rate-anomalies
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

rf ht-radio-profile

```
rf ht-radio-profile <profile>
   40MHz-intolerance
   clone <profile>
   diversity-spreading-workaround
   honor-40MHz-intolerance
   no
```

Description

This command configures high-throughput AP radio settings. High-throughput features use the IEEE 802.11n standard.

Syntax

Parameter	Description	Range	Default
`<profile>`	Name of this instance of the profile. The name must be 1-63 characters. **Default Options:** ■ "Default-a" is generally used in association with high-throughput devices running on the 5 GHz frequency band, see rf dot11a-radio-profile on page 843. ■ "Default-g" is generally used in association with high-throughput devices running on the 2.4 GHz frequency band, see rf dot11g-radio-profile on page 854. ■ "Default" is generally used when the same ht-radio-profile is desired for use with both frequency bands.	—	default-a default-g default
`40MHz-intolerance`	Controls whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed.	—	disabled
`clone`	Name of an existing high-throughput radio profile from which parameter values are copied.	—	—
`honor-40MHz-intolerance`	When enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.	—	enabled
`no`	Negates any configured parameter.	—	—
`diversity-spreading-workaround`	When this feature is enabled, all legacy transmissions will be sent using a single antenna. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n cyclic shift diversity (CSD) data. This feature is disabled by default and should be kept disabled unless necessary.		disabled

Usage Guidelines

The ht-radio-profile configures high-throughput settings for networks utilizing the IEEE 802.11n standard, which supports 40 MHZ channels and operates in both the 2.4 GHZ and 5 GHZ frequency bands.

Most transmissions to high throughput (HT) stations are sent through multiple antennas using cyclic shift diversity (CSD). When you enable the disable-diversity-spreading parameter, CSD is disabled and only one antenna transmits data, even if they are being sent to high-throughput stations. Use this feature to turn off antenna diversity when the AP must support legacy clients such as Cisco 7921g VoIP phones, or older 802.11g clients (e.g. Intel Centrino clients). Note, however, that enabling this feature can reduce overall throughput rates.

The ht-radio-profile you wish to use must be assigned to a dot11a and/or dot11g-radio-profile. You can assign the same profile or different profiles to the 2.4 GHZ and 5 GHZ frequency bands. See rf dot11a-radio-profile on page 843 and rf dot11g-radio-profile on page 854.

Example

The following command configures an ht-radio-profile named “default-g” and enables 40MHz-intolerance:

```
(host)[node](config) #rf ht-radio-profile default-g
   40MHz-intolerance
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms, but operates with IEEE 802.11n compliant devices only	Base operating system	Config mode on Mobility Master.

rf optimization-profile

```
rf optimization-profile <profile-name>
   clone <profile>
   handoff-assist
   low-rssi-threshold <number>
   no ...
   rssi-check-frequency <number>
   rssi-falloff-wait-time <number>
```

Description

This command configures the RF optimization profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`clone`	Name of an existing optimization profile from which parameter values are copied.	—	—
`handoff-assist`	Allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold.	—	disabled
`low-rssi-threshold`	Minimum RSSI, above which deauth should never be sent.	1-255	10
`no`	Negates any configured parameter.	—	—
`rssi-check-frequency`	Interval, in seconds, to sample RSSI.	9-255	3 seconds
`rssi-falloff-wait-time <number>`	Number of times the detected client RSSI level must fall below the minimum RSSI threshold the before the AP sends a deauthorization message to the client. The maximum value is 8 times.	0-8	4

Example

The following command configures an RF optimization profile:

```
(host)[node](config) #rf optimization-profile Angela1
(host)[node](RF Optimization Profile "Angela1") #rssi-falloff-wait-time 3
(host)[node](RF Optimization Profile "Angela1") #rssi-check-frequency 2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

rf spectrum-profile

```
rf spectrum-profile <profile-name>
   age-out audio|bluetooth|cordless-ff-phone|cordless-fh-base|cordless-fh-network|generic-
   ff|generic-fh|microwave|microwave-inverter|unknown|video|wifi|xbox
   clone <source>
   no ...
```

Description

Define the device ageout times used by a spectrum monitor, or hybrid AP radio.

Syntax

Parameter	Description	Range	Default
`age-out`	Use the **age-ou t** parameter to define the number of seconds for which a specific device type must stop sending a signal before the spectrum monitor considers that device no longer active on the network.		
`audio`	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as Fixed Frequency (Audio).	5-65535 seconds	10 sec
`bluetooth`	Bluetooth devices. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	25 sec
`cordless-ff-phone`	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as Fixed Frequency (Cordless Phones).	5-65535 seconds	10 sec
`cordless-fh-base`	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as Frequency Hopper (Cordless Base).	5-65535 seconds	240 sec
`cordless-fh-network`	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as Frequency Hopper (Cordless Network). Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.	5-65535 seconds	60 sec

Parameter	Description	Range	Default
`generic-ff`	All fixed frequency devices that do not fall into one of the other categories are classified as Fixed Frequency (Other). Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).	5-65535 seconds	10 sec
`generic-fh`	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as Frequency Hopper (Other). Some examples include IEEE 802.11 FHSS devices, game consoles and cordless/hands-free devices that do not use one of the known cordless phone protocols.	5-65535 seconds	25 sec
`generic-interferer`	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a Generic Interferer. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.	5-65535 seconds	30 sec
`microwave`	Common residential microwave ovens with a single magnetron are classified as a Microwave. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device. Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	15 sec
`microwave-inverter`	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as Microwave (Inverter). Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).	5-65535 seconds	15 sec

Parameter	Description	Range	Default
`video`	Video transmitters that continuously transmit video on a single frequency are classified as Fixed Frequency (Video). These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.	5-65535 seconds	60 sec
`wifi`	Wi-Fi devices.	5-65535 seconds	600 sec
`xbox`	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as Frequency Hopper (Xbox). Note that this setting is applicable to 2.4GHz spectrum monitor radios only.	5-65535 seconds	25 sec
`clone <source>`	Make a copy of an existing spectrum profile.		600 sec
`no`	Remove a spectrum profile or negate a configured parameter.		

Usage Guidelines

The Spectrum Analysis software module provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify the 802.11 devices on the network. APs that gather spectrum data are called Spectrum Monitors, or *SMs*, and reference a spectrum profile that determines the band monitored by that SM radio. Use this profile to modify default device ageout times for spectrum monitors and hybrid APs using this profile.

For a list of APs that can be converted into a spectrum monitor or hybrid AP, refer to the Spectrum Analysis chapter of the ArubaOS 8.3.0.x User Guide.

Example

The following command creates the spectrum profile **spectrum2**.

```
(host)[node](config) #rf spectrum-profile spectrum2
```

Related Commands

show rf spectrum-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	RF Protect license	Config mode on Mobility Master.

router mobile

```
router mobile
```

Description

This command enables Layer-3 (IP) mobility.

Syntax

No parameters.

Usage Guidelines

Use this command to enable IP mobility on a controller. IP mobility is disabled by default on the controller. This command must be executed on all controllers(master and local) that need to provide support for layer-3 roaming in a mobility domain. You can enable or disable IP mobility on a virtual AP profile with the **wlan virtual-ap** command (IP mobility is enabled by default in a virtual AP profile).

It is recommended to reboot the controller every time you enable or disable IP mobility.

Example

This command enables IP mobility:

```
(host) [mynode] (config) #router mobile
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

router ospf

```
router ospf
   aggregate-route rapng-vpn <addr> <mask>
   area <area-id>
           default-cost <cost>
           no [default-cost | nssa | stub]
           nssa [default-information-originate | no-redistribution | no-summary]
           stub [no-summary]
   default-information originate always
   redistribute
           loopback
           rapng-vpn
           static
           vlan [add <vlan-ids> | remove <vlan-ids> | <vlan-ids>]
   router-id <rtr-id>
   subnet exclude <addr> <mask>
```

Description

This command configures OSPF configuration for the upstream router. This command is only available in the Config mode.

Syntax

Parameter	Description	Range	Default
`aggregate-route rapng-vpn <addr> <mask>`	Configures the aggregate route information for specified IP address and subnet mask and redistributes RAPNG VPN address	–	–
`area <area-id>`	Configures OSPF area for specified area ID (IP address)	–	–
`default-cost <cost>`	Configures summary default-cost of a NSSA/stub area	0 to 16777215	–
`no [default-cost | nssa | stub]`	Removes configured default-cost of NSSA/stub, NSSA, or stub	–	–
`nssa [default-information-originate | no-redistribution | no-summary]`	Configures origination of type 7 default into NSSA area, sets NSSA area for no distribution into this NSSA area, or stops sending of summary LSA into this NSSA area	–	–
`stub [no-summary]`	Configures an area as stub area and stops sending summary LSA into this area	–	–

Parameter	Description	Range	Default
`default-information originate always`	Configures distribution of default information by distributing a default route	–	–
`redistribute`	Redistributes the route	–	–
`loopback`	Redistributes loopback addresses	–	–
`rapng-vpn`	Redistributes RAPNG VPN addresses	–	–
`static`	Redistributes static IP routes.	–	–
`vlan [add <vlan-ids> | remove <vlan-ids> | <vlan-ids>]`	Redistributes VLAN user subnet, adds user VLANs to list, or removes user VLANs from list.	–	–
`router-id <rtr-id>`	Configures router ID for specified IP address	–	–
`subnet exclude <addr> <mask>`	Configures IP address and subnet mask that OSPF will not advertise	–	–

Usage Guidelines

OSPFv2 is a dynamic Interior Gateway routing Protocol (IGP) based on IETF RFC 2328. The OSPF implementation allows managed devices to deploy effectively in a Layer 3 topology.

Example

The following example configures an IP address 192.0.2.1 and subnet mask 255.0.255.255 that OSPF will not advertise:

```
(host) [mynode] (config) #router ospf subnet exclude 192.0.2.1 255.0.255.255
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced
ArubaOS 8.1.0.0	The **static** sub-parameter was added under the **redistribute** parameter.

Command Information

Platforms	License	Command Mode
All Platforms	Base operating system	Configuration mode on managed devices

routing-policy-map

```
routing-policy-map
   branch <XX:XX:XX:XX:XX:XX> access-list <STRING>
   role <STRING> access-list <STRING>
```

Description

This command associates a routing ACL with a specific user role on a managed device.

Syntax

Parameter	Description
`branch <XX:XX:XX:XX:XX:XX>`	By default, when a branch office deployment uses IPsec maps to define the connections between each branch office managed device and its Mobility Master, the global ACL **master-boc-traffic** is applied to those IPsec maps. Use this command to apply a local ACL to the GRE tunnel between a specific branch office managed device and its Mobility Master, overriding the default **master-boc-traffic** ACL.
`role <STRING>`	Name of the user role to be associated with the specified routing ACL.
`access-list <STRING>`	Name of the route ACL to be associated to the specified user role.

Usage Guidelines

The commands to associate an access list to a user role vary, depending upon the type of access list being associated to that role. Ethertype, MAC, and session ACLs are applied globally across all managed devices, but routing access lists may vary between locations, so they are mapped to a user role in a local configuration setting.

In an environment where an IPsec map defines the connections between the managed device and Mobility Master, the global ACL **master-boc-traffic** is applied to all IPsec maps between the managed device and Mobility Master. If any managed device requires a different ACL, issue the command **routing-policy-map branch <mac-addr> access-list <acl>** on that managed device to associate a different ACL to the L3 GRE tunnel between that one managed device and Mobility Master. This local setting will override the global settings defined in the master-boc-traffic ACL.

Example

The following example maps a user role to a routing ACL.

```
(host)[node](config) #routing-policy-map
   role employee access-list branch1
```

To associate the user role with an ethertype, MAC or session ACL, use the command **user-role <role> access-list eth|mac|session <acl>**.

Related Commands

Command	Description
ip access-list route	Configures an ACL for policy-based routing (PBR).
ip nexthop-list	Defines a next-hop list for a routing policy.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

sc-migration

```
sc-migration
   export sc-ca-cert {self-signed-cert|<custom-cert>}
   import <ip>
```

Description

This command is used by the migration tool to export and import migration data from controllers in ArubaOS 6.x deployments to ArubaOS 8.x deployment.

Syntax

Parameter	Description
`export`	Exports the setup data into */tmp/dbsync/migration/setupInfo.xml*
`sc-ca-cert [self-signed-cert|<custom-cert>]`	(Optional) Specify the CA certificate to be sent to the managed device. You can specify one of the following certificates: ■ **self-signed-cert**—Self-signed CA certificate is exported into */tmp/dbsync/migration/sc_ssc.pem* ■ **<custom-cert>**—The specified custom certificate (*/flash/certmgr/TrustedCA/<custom-cert>*) is exported into */tmp/dbsync/migration/<custom-cert>*
`import <ip>`	Runs the upgrade scripts on the configuration (*default.cfg*) stored in the specified IP address. The upgraded configuration is applied on Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config or Enable mode on managed device.

scheduler-profile

```
scheduler-profile <profile>
   clone
   priority-map q0|q1|q2|q3 <que-prio-list>
   queue-weights q0|q1|q2|q3 <que-weight>
```

Description

Define a schedule profile that associates priorities to four uplink queues.

Syntax

Parameter	Description
`clone <profile>`	Make a copy of an existing scheduler profile
`priority map q0|q1|q2|q3 <que-prio-list>`	Specify one or more priority levels (0-7) for each queue type (q0 through q3). Each of the seven priority levels must be supported by one of the four queues.
`queue-weights q0|q1|q2|q3 <que-weight>`	(Optional) Enter the percentage of available bandwidth that should be made available to traffic in each of the four queues. **NOTE:** If you do not specify a weight for each queue, the queue service is based exclusively on the priority of the queue, where the lower priority queues are not serviced until the higher priority queue is clear. With this option, the highest level priority is guaranteed as much bandwidth as possible, but there can be phases where the 2nd, 3rd and 4th priority queues may receive little or no bandwidth.

Example

ArubaOS supports minimum bandwidth guarantees per traffic class, and allows critical delay-sensitive applications like voice and video to use more bandwidth and/or be scheduled with higher priority. Each interface can be associated with a scheduler profile, that supports four queues with different priority levels. If you use session ACLs to define traffic policies on the managed device, you can use the scheduler profile to automatically associate these different priority levels assigned by these policies to a scheduler profile queue. The scheduler profile must be associated with an interface using the command **interface cellular|gigabitethernet <slot/module/port> transmit max-rate rate mbits <mbps> scheduler-profile <profile>.**

```
(host) #support
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

scs-local-custom-cert

```
scs-local-custom-cert [scs-local-mac <mac>] [ca-cert <ca>] [server-cert <sc>] [suite-b
[gcm128]|[gcm256]]
```

Description

This command configures security for all master-local control traffic using custom certificate.

Syntax

Parameter	Description
`scs-local-mac <mac>`	Specifies MAC address of managed device.
`ca-cert <ca>`	Specifies CA certificate to use.
`server-cert <sc>`	Specifies server certificate to use.
`suite-b`	Specifies GCM-128 or GCM-256 suite B algorithm to use.

Example

The following example configures CA certificate **default_ca** and server certificate **default_server** for master-local control traffic:

```
(host) [mynode] #scs-local-custom-cert scs-local-mac 00:1a:1e:aa:bb:cc ca-cert
default_ca server-cert default_serverr
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

secondary master-ip

```
secondary masterip <secmasterip_val> [ipsec | ipsec-custom-cert | ipsec-factory-cert | vpn-ip]
```

Description

Use this command to add a secondary master-ip.

Syntax

Parameter	Description	Default
`secmasterip_val`	Configure the master ip address or FQDN.	—
`ipsec`	IPSec key of length 64 bytes.	—
`fqdn`	The Local's FQDN (max 64 bytes) used in IKE. This is optional for a Dynamically addressed Local	—
`interface`	Vlan interface to initiate IKE. The switch IP will be used if the vlan is not specified.	—
`peer-mac-1`	Specify peer MAC string.	—
`ipsec-custom-cert`	Custom Cert-based IPSec secure communication between master and local.	—
`master-mac-1-c`	Specify Master's MAC address.	—
`ipsec-factory-cert`	Factory Cert-based IPSec secure communication between master and local.	—
`master-mac-1-c`	Specify Master's MAC address.	—
`ca-cert`	Specify the CA certificate to use.	—
`master-mac-2-c`	Specify the redundant master's MAC address.	—
`vpn-ip`	VPN concentrator's IP address or FQDN.	—

Usage Guidelines

This command allows the user to add a secondary Mobility Master from the primary Mobility Master CLI. This command is allowed in the **/md** tree, both in device nodes and group nodesset.

Example

The following command enables you to add a secondary Mobility Master.

```
(host) [md] (config) #secondary masterip
```

Related Commands

Command	Description
master-l3redundancy	Configures Layer-3 redundancy for a Mobility Master.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master.

serial console redirect

```
serial console redirect {enable | disable}
```

Description

This command configures redirect to serial console.

Syntax

Parameter	Description	Range	Default
`enable`	Enables redirect to serial console.	–	–
`disable`	Disables redirect to serial console.	–	–

Usage Guidelines

This command configures redirect to serial console. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to enable the redirect to serial console:

```
(host) [mynode] #serial console redirect enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

service

```
service
   dhcp
   dhcpv6
   network-storage
   print-server
   scp
   no...
```

Description

This command enables the DHCP server on the controller.

Syntax

Parameter	Description	Default
`dhcp`	Enables the DHCP server	Disabled
`dhcpv6`	Enables the DHCPv6 server	Disabled
`network-storage`	Enables the NAS service	Disabled
`print-server`	Enables the printer service	Disabled
`scp`	Enables the scp server functionality on the controller or managed device	Disabled
`no...`	Removes the specific configuration	—

Usage Guidelines

You can enable and configure DHCP, DHCPv6, network-storage, print server, or scp in the controller to provide the following to clients:

- DHCP: IP addresses to wireless clients if an external DHCP server is not available.
- DHCPv6: IPv6 addresses to wireless clients if an external DHCPv6 server is not available.
- Network-storage: To provide access to the storage devices attached to the controller or managed device.
- Printer-server: To provide access to printers attached to the controller .
- scp: To provide SCP functionality on the controller itself rather than on an external server.

Example

The following command enables the DHCP server in the controller or managed device:

```
(host) [mynode] (config) #service dhcp
```

The following command enables the DHCPv6 server in the controller or managed device:

```
(host) [mynode] (config) #service dhcpv6
```

The following command enables the NAS services in the controller or managed device:

```
(host) [mynode] (config) #service network-storage
```

The following command enables the printer services in the controller or managed device:

```
(host) [mynode] (config) #service print-server
```

The following command enables the scp server functionality in the controller or managed device::

```
(host) [mynode] (config) #service scp
```

To disable the SCP server functionality on the controller, execute the following command:

```
(host) [mynode] (config) #no service scp
```

Related Commands

Command	Description
show scp	Shows if the SCP server functionality is enabled or not.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **scp** parameter was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on the controller or managed device

session delete

```
session delete <ip>
```

Description

This command deletes a session.

Syntax

Parameter	Description	Range	Default
`<ip>`	Deletes session of specified IP address.	–	–

Usage Guidelines

This command deletes a session. For the remaining parameters, see the command syntax.

Example

The following example deletes a session with IP address 192.0.2.1:

```
(host) [mynode] #session delete 192.0.2.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

set-ikepsk-by-addr

```
set-ikepsk-by-addr <ip-addr>
```

Description

This command configures IKE PSK corresponding to an IP address.

Syntax

Parameter	Description	Range	Default
`<ip-addr>`	Configures specified IP address to use to select IKE PSK.	–	–

Usage Guidelines

This command configures IKE PSK corresponding to an IP addres. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to configure IKE PSK corresponding to IP address **192.0.2.1**:

```
(host) [mynode] #set-ikepsk-by-addr 192.0.2.1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

set-trust-anchor

```
set-trust-anchor {self-signed | <ca-name>}
```

Description

This command configures a trust anchor for an access point.

Syntax

Parameter	Description	Range	Default
`self-signed`	Configures self signed certificate as the trust anchor.	–	–
`<ca-name>`	Configures the specified trusted CA certificate as the trust anchor.		

Usage Guidelines

This command configures a trust anchor for an access point. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to configure self-signed certificate for an access point:

```
(host) [mynode] #set-trust-anchor self-signed
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show aaa auth-survivability

```
show aaa auth-survivability
```

Description

This command shows the authentication survivability configuration on a stand-alone controller.

Syntax

No parameters.

Usage Guidelines

This command shows the authentication survivability configuration on a stand-alone controller.

Example

The following example shows the authentication survivability configuration:

```
(host) [mynode] #show aaa auth-survivability

Auth-Survivability: Disabled (Not Running)
Survival-Server Server-Cert: N/A
Survival-Server Cache lifetime: 24 hours
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on stand-alone controller

show aaa auth-survivability-cache

```
show aaa auth-survivability-cache
```

Description

This command shows the authentication survivability cached data on a stand-alone controller.

Syntax

No parameters.

Usage Guidelines

This command shows the authentication survivability cached data on a stand-alone controller.

Example

The following example shows the authentication survivability cached data:

```
(host) [mynode] #show aaa auth-survivability-cache

Auth-Survivability Cached Data
------------------------------
Station  User Name  Authenticated Using  Authenticated By  Authenticated On
-------  ---------  -------------------  ----------------  ----------------

Total Entries: 0
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on stand-alone controller

show aaa accounting tacacs

```
show aaa accounting tacacs
```

Description

Show configuration information for TACACS+ accounting servers.

Usage Guidelines

This command displays TACACS+ data for your controller if you have previously configured a TACACS+ server and server group. The output includes the current TACACS+ accounting mode (enabled or disabled), and the name of the TACACS+ server group.

Example

The output of the **show aaa accounting tacacs** command displays configuration information for a TACACS+ accounting server. The output of this command includes the following parameters:

```
(host) #show aaa accounting tacacs
TACACS Accounting Configuration
-------------------------------
Parameter       Value
---------       -----
Mode            Enabled
Commands        configuration
Server-Group    tacacs1
```

Parameter	Description
`Mode`	Shows whether this server group is **Enabled** or **Disabled**.
`Commands`	Displays the types of commands that are reported to the TACACS server group. ■ **action** reports action commands only. ■ **all** reports all commands. ■ **configuration** reports configuration commands only ■ **show** reports show commands only
`Server-Group`	Shows whether this server is **Enabled** or **Disabled**.

Related Commands

Command	Description	Mode
aaa authentication-server tacacs	Configure the TACACS+ accounting feature.	Config mode
aaa server-group	Add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication	Config mode

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show aaa alias-group

```
show aaa alias-group [<ag_name>]
```

Description

This command shows an alias-group settings.

Syntax

Parameter	Description	Range	Default
<ag_name>	Shows settings of specified alias-group.	–	–

Usage Guidelines

This command shows an alias-group settings. For the remaining parameters, see the command syntax.

Example

The following example shows the list of alias-groups:

```
(host) [mynode] #show aaa alias-group

Alias Group List
----------------
Name  References  Profile Status
----  ----------  --------------
default  2

Total:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show aaa authentication all

```
show aaa authentication all
```

Description

Show authentication statistics for your managed device, including authentication methods, successes and failures.

Usage Guidelines

This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive-portal, MAC or 801.X authentication profile, issue the commands specific to those features.

Example

The output of this command displays an authentication overview for your managed device, including the authentication methods used, and the numbers of successes or failures for each method. This example shows the numbers of authentication successes and failures for a managed device using TACACS+ and RADIUS authentication methods.

```
(host) #show aaa authentication all

Auth Method Statistics
----------------------
Method  Success  Failures
------  -------  --------
tacacs                 12                                          2Radius                 9
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show aaa authentication captive-portal

```
show aaa authentication captive-portal [<profile-name>]
```

Description

This command shows configuration information for captive portal authentication profiles.

Syntax

Parameter	Description
<profile-name>	The name of an existing captive portal authentication profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire Captive Portal Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any captive portal authentication profiles defined, use the command **aaa authentication captive-portal** to configure your captive portal profiles.

Examples

This first example shows that there are three configured captive portal profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a captive portal authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
Name            References  Profile Status
----            ----------  --------------
c-portal        2
remoteuser                                                    1
portal1                                                       1

Total: 4
```

Include a captive portal profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal profile portal1.

```
Captive Portal Authentication Profile "portal1"
-----------------------------------------------
Parameter                                       Value
---------                                       -----
Default Role                                    guest
Default Guest Role                              guest
Server Group                                    default
Redirect Pause                                  10 sec
User Login                                      Enabled
Guest Login                                     Disabled
Logout popup window                             Enabled
Use HTTP for authentication                     Disabled
```

```
Logon wait minimum wait                              5 sec
Logon wait maximum wait                              10 sec
logon wait CPU utilization threshold                 60 %
Max Authentication failures                          0
Show FQDN                                            Disabled
Authentication Protocol                              PAP
Login page                                           /auth/index.
Welcome page                                         /auth/welcom
Show Welcome Page                                    Yes
Add switch IP address in the redirection URL         Disabled
Adding user vlan in redirection URL                  Disabled
Add a controller interface in the redirection URL    N/A
Allow only one active user session                   Disabled
White List                                           N/A
Black List                                           N/A
Show the acceptable use policy page                  Disabled
User idle timeout                                    N/A
Redirect URL                                         N/A
Bypass Apple Captive Network Assistant               Disabled
URL Hash Key                                         ********
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	Role assigned to the captive portal user upon login.
`Default Guest Role`	Guest role assigned to the captive portal user upon login.
`Server Group`	Name of the group of servers used to authenticate captive portal users.
`Redirect Pause`	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link.
`User Login`	Shows whether the profile has enabled or disabled captive portal with authentication of user credentials.
`Guest Login`	Shows whether the profile has enabled or disabled captive portal guest login without authentication.
`Logout popup window`	Shows whether the profile has enabled or disabled a pop-up window that allows a user to log out. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station resets.
`Use HTTP for authentication`	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.

Parameter	Description
Logon wait minimum wait	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
Logon wait maximum wait	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high.
logon wait CPU utilization threshold	CPU utilization percentage above which the logon wait interval is applied when directing a captive portal user with the logon page.
Max Authentication failures	Maximum number of authentication failures before the user is blacklisted.
Show FQDN	If enabled, the user can see and select the fully-qualified domain name (FQDN) on the captive portal login page.
Authentication Protocol	This parameter specifies the type of authentication required by this profile, PAP is the default authentication type
Login page	URL of the page that appears for the user logon.
Welcome page	URL of the page that appears after logon and before the user is redirected to the web URL.
Add controller IP address in the redirection URL	If enabled, this option sends he controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL.
Adding user vlan in redirection URL	Shows the user's VLAN ID sent in the redirection URL, if enabled
Add a controller interface in the redirection URL	**Shows the IP address of a controller interface added to the redirection URL, if enabled.**
Allow only one active user session	If enabled, only one active user session is allowed at any time. This feature is disabled by default.
White List	Shows the configured white list on an IPv4 or IPv6 network destination. The white list contains authenticated websites that a guest can access.
Black List	Shows the configured black list on an IPv4 or IPv6 network destination. The black list contains websites (unauthenticated) that a guest cannot access.

Parameter	Description
`Show the acceptable use policy page`	If enabled, the captive portal page will show the acceptable use policy page before the user logon page. This feature is disabled by default.
`User Idle Timeout`	The user idle timeout for this profile. The valid range is 30-15300 in multiples of 30 seconds. Enabling this option overrides the global settings configured in the AAA timers. If this is disabled, the global settings are used.
`redirect-url <url>`	URL to which an authenticated user will be directed.
`URL hash key`	If this value is set, the redirection URL is hashed using the defined hash key. The characters in the hash key are hidden in the output of this command

Related Commands

Command	Description	Mode
aaa authentication captive-portal	Use aaa authentication captive-portal to configure the parameters displayed in the output of this show command.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show aaa authentication captive-portal customization

```
show aaa authentication captive-portal customization <profile-name>
```

Description

Display customization settings for a captive portal profile

Syntax

Parameter	Description
`<profile-name>`	The name of an existing captive portal authentication profile.

Usage Guidelines

The this command shows how a captive portal profile has been customized with non-default configuration settings. If you do not yet have any captive portal authentication profiles defined, use the command aaa authentication captive-portal to configure your captive portal profiles

Example

The output of the following command shows how the captive portal profile *c-portal* has been customized. If an individual parameter has not been changed from its default settings, its value entry will be blank.

```
(host) #show aaa authentication captive-portal customization c-portal
Captive-Portal Customization
----------------------------
Parameter                       Value
---------                       -----
Login page design theme         3
Login page logo image
Login page text URL             /flash/upload/custom/ssu-guest-cp/logintext.html
Login policy text URL           /upload/custom/ssu-guest-cp/acceptableusepolicy.html
Custom page background color
Custom page background image    /upload/custom/default/auth-slider-1.gif
```

The output of this command includes the following parameters:

Parameters	Description
`Login page design theme`	Indicates whether the controller is using one of the two predefined login page designs (**1** or **2**) or has a custom background (**3**).
`Login page logo image`	Path and filename for a custom captive portal logo. This option is only available if the controller has a predefined login design.
`Login page text`	Path and filename of the page that appears for the user logon.
`Login policy text`	Path and filename of the page that displays user policy text.
`Custom page background color`	Hexadecimal value for a custom background color. This option is only available if the controller has a custom login page design theme.
`Custom page background image`	Path and filename for a custom JPEG captive portal background image. This option is only available if the controller has a custom login page design theme.

Related Commands

Command	Description	Mode
aaa authentication captive-portal	If you do not yet have any captive portal profiles defined, use the command aaa authentication captive-portal to configure your captive portal profiles.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show aaa authentication dot1x

```
show aaa authentication dot1x [<profile-name>|countermeasures]
```

Description

This command shows information for 802.1X authentication profiles.

Syntax

Parameter	Description
`<profile-name>`	The name of an existing 802.1X authentication profile.
`countermeasures`	Reports if WPA/WPA2 Countermeasures have been enabled for 802.1X profiles. If enabled, the AP scans for message integrity code (MIC) failures in traffic received from clients.

Usage Guidelines

Issue this command without the **<profile-name**> or **countermeasures** options to display the entire 802.1X Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed dot1x authentication configuration information for that profile. The **countermeasures** option indicates whether the 802.1X profiles have been configured for WPA/WPS2 countermeasures. If countermeasures have not been configured, the output for this command will be blank.

Examples

The following example lists all dot1x authentication profiles. The **References** column lists the number of other profiles with references to a 802.1X authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined 802.1X profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication dot1x

802.1X Authentication Profile List
----------------------------------
Name         References  Profile Status
----         ----------  --------------
default      2
default-psk  1           Predefined (editable)
dot1x        5
dot1xtest                     0

Total:4
```

To display a complete list of parameters for an individual profile, include the <profile> parameter. The example below displays some of the profile details for the authentication profile pDotix.

```
(host) #show aaa authentication dot1x pDot1x

802.1X Authentication Profile "pDot1x"
--------------------------------------
Parameter                                          Value
---------                                          -----
Max authentication failures                        0
Enforce Machine Authentication                     Disabled
```

```
Machine Authentication: Default Machine Role              guest
Machine Authentication Cache Timeout                      24 hrs
Blacklist on Machine Authentication Failure               Disabled
Machine Authentication: Default User Role                 guest
Interval between Identity Requests                        30 sec
Quiet Period after Failed Authentication                  30 sec
Reauthentication Interval                                 86400 sec
Use Server provided Reauthentication Interval             Disabled
Multicast Key Rotation Time Interval                      1800 sec
Unicast Key Rotation Time Interval                        900 sec
...
```

The output of the **show aaa authentication dot1x**command includes the following parameters:

Parameter	Value
`Max authentication failures`	Number of times a user can try to login with wrong credentials after which the user is blacklisted as a security threat. Blacklisting is disabled if this parameter is set to 0.
`Enforce Machine Authentication`	Shows if machine authentication is enabled or disabled for Windows environments. If enabled, If enabled, either the machine-default-role or the user-default-role is assigned to the user, depending on which authentication is successful.
`Machine Authentication: Default Machine Role`	Default role assigned to the user after completing only machine authentication.
`Machine Authentication Cache Timeout`	The timeout period, in hours, for machine authentication. After this period passes, the use will have to re-authenticate.
`Blacklist on Machine Authentication Failure`	If enabled, the client is blacklisted if machine authentication fails.
`Machine Authentication: Default User Role`	Default role assigned to the user after 802.1X authentication.
`Interval between Identity Requests`	Interval, in seconds, between identity request retries
`Quiet Period after Failed Authentication`	Interval, in seconds, following failed authentication.

Parameter	Value
Reauthentication Interval	Interval, in seconds, between reauthentication attempts.
Use Server provided Reauthentication Interval	If enabled, 802.1X authentication will use the server-provided reauthentication period.
Multicast Key Rotation Time Interval	Interval, in seconds, between multicast key rotations.
Unicast Key Rotation Time Interval	Interval, in seconds, between unicast key rotations.
Authentication Server Retry Interval	Server group retry interval, in seconds.
Authentication Server Retry Count	The number of server group retries.
Framed MTU	Shows the framed MTU attribute sent to the authentication server.
Number of times ID-Requests are retried	Maximum number of times ID requests are sent to the client.
Maximum Number of Reauthentication Attempts	Maximum number of reauthentication attempts.
Maximum number of times Held State can be bypassed	Number of consecutive authentication failures which, when reached, causes the controller to not respond to authentication requests from a client while the controller is in a held state after the authentication failure.
Dynamic WEP Key Message Retry Count	Number of times unicast/multicast EAPOL key messages are sent to the client.
Dynamic WEP Key Size	Dynamic WEP key size, either 40 or 128 bits.
Interval between WPA/WPA2 Key Messages	Interval, in milliseconds, between each WPA key exchange. The allowed range of values is 1000-5000 msecs, and the default value is 1000 msecs.

Parameter	Value
Delay between EAP-Success and WPA2 Unicast Key Exchange	Show the delay interval between EAP-Success and unicast key exchanges, in msec. Range: 0-2000msec. Default: 0 (no delay).
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	Interval, in milliseconds, between unicast and multicast key exchanges.
Time interval after which the PMKSA will be deleted	Show the PMKSA cache interval. Time interval in Hours. Range: 1-2000. Default: 8 hrs.
Delete Keycache upon user deletion Enabled	If enabled, the controller deletes the key cache entry when the user entry is deleted.
WPA/WPA2 Key Message Retry Count	Number of times WPA/WPA2 key messages are retried.
Multicast Key Rotation	Shows if multicast key rotation is enabled or disabled.
Unicast Key Rotation	Shows if unicast key rotation is enabled or disabled.
Reauthentication	If enabled, this option forces the client to do a 802.1X reauthentication after the expiration of the default timer for reauthentication. (The default value of the timer is 24 hours.)
Opportunistic Key Caching	If enabled, a cached pairwise master key (PMK) is derived with a client and an associated AP and used when the client roams to a new AP.

Parameter	Value
Validate PMKID	Shows if the **Validate PMKID** feature is enabled or disabled. When this option is enabled, the client must send a PMKID in the associate or reassociate frame to indicate that it supports OKC; otherwise, full 802.1X authentication takes place. (This feature is optional, since most clients that support OKC do not send the PMKID in their association request.)
Use Session Key	If enabled, the controller will use a RADIUS session key as the unicast WEP key.
Use Static Key	If enabled, the controller will use a static key as the unicast/multicast WEP key.
xSec MTU	Shows the size of the MTU for xSec.
Termination	Shows if 802.1X termination is enabled or disabled on the controller.
Termination EAP-Type	Shows the current Extensible Authentication Protocol (EAP) method, either EAP-PEAP or EAP-TLS.
Termination Inner EAP-Type	When EAP-PEAP is the EAP method, this parameter displays the inner EAP type.
Enforce Suite-B 128 bit or more security level Authentication	Shows if Suite-B 128 bit or more security level authentication enforcement is enabled or disabled.
Enforce Suite-B 192 bit security level Authentication	Shows if Suite-B 192 bit or more security level authentication enforcement is enabled or disabled.
Token Caching	If this feature enabled (and EAP-GTC is configured as the inner EAP method), token caching allows the controller to cache the username and password of each authenticated user.
Token Caching Period	Timeout period, in hours, for the cached information.

Parameter	Value
CA-Certificate	Name of the CA certificate for client authentication loaded in the controller.
Server-Certificate	Name of the Server certificate used by the controller to authenticate itself to the client.
TLS Guest Access	Shows if guest access for valid EAP-TLS users is enabled or disabled.
TLS Guest Role	User role assigned to EAP-TLS guest.
Ignore EAPOL-START after authentication	If enabled, the controller ignores EAPOL-START messages after authentication.
Handle EAPOL-Logoff	Shows if handling of EAPOL-LOGOFF messages is enabled or disabled.
Ignore EAP ID during negotiation	If enabled, the controller will Ignore EAP IDs during negotiation.
WPA-Fast-Handover	Shows if WPA-fast-handover is enabled or disabled. This feature is only applicable for phones that support WPA.
Disable rekey and reauthentication for clients on call	Shows if the rekey and reauthentication features for voice-over-WLAN clients has been enabled or disabled.
Check certificate common name against AAA server	If enabled, this parameter verifies that the certificate's common name exists in the server. This parameter is disabled by default dot1x profiles.

Related Commands

Command	Description	Mode
aaa authentication dot1x	If you do not yet have any 802.1X authentication profiles defined, use the command aaa authentication dot1x to configure your 802.1X profiles.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication mac

```
show aaa authentication mac [<profile-name>]
```

Description

This command shows information for MAC authentication profiles.Issue this command without the **<profile-name>** option to display the entire MAC Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed MAC authentication configuration information for that profile.

Syntax

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Examples

The output of the example below shows two MAC authentication profiles, **default** and **macProfile1**, which are referenced three times by other profiles. the **Profile Status** columns are blank, indicating that these profiles are both user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication dot1x pDot1x

802.1X Authentication Profile "pDot1x"
---------------------------------------
Parameter                                                Value
---------                                                -----
Max authentication failures                              0
Enforce Machine Authentication                           Disabled
Machine Authentication: Default Machine Role             guest
Machine Authentication Cache Timeout                     24 hrs
Blacklist on Machine Authentication Failure              Disabled
Machine Authentication: Default User Role                guest
Interval between Identity Requests                       30 sec
Quiet Period after Failed Authentication                 30 sec
Reauthentication Interval                                86400 sec
Use Server provided Reauthentication Interval            Disabled
Multicast Key Rotation Time Interval                     1800 sec
Unicast Key Rotation Time Interval                       900 sec
...
```

The following example displays configuration details for the MAC authentication profile “MacProfile1,” including the delimiter and case used in the authentication request, and the maximum number of times a client can fail to authenticate before it is blacklisted.

```
(host) #show aaa authentication mac MacProfile1
MAC Authentication Profile "MacProfile1"
----------------------------------------
Parameter                    Value
---------                    -----
Delimiter                    colon
Case                         upperMax Authentication failures  3
```

Related Commands

Command	Description	Mode
aaa authentication mac	Configure MAC authentication values on your controller.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication mgmt

```
show aaa authentication mgmt
```

Description

This command displays administrative user authentication information, including management authentication roles and servers.

Usage Guidelines

Issue this command to identify the default management role assigned to authenticated administrative users, and the name of the group of servers used to authenticate these users.

Example

The output of the following example displays management authentication information for your controller.

```
(host) #show aaa authentication mgmt

Management Authentication Profile
---------------------------------
Parameter     Value
---------     -----
Default Role  root
Server Group  ServerGroup1
Enable          Enabled
```

Parameter	Description
`Default Role`	This parameter shows which of the following roles the controller uses for authentication management. ■ **root**, the super user role (default). ■ **guest-provisioning**, guest provisioning role. ■ **network-operations**, network operator role. ■ **read-only**, read only role. ■ **location-api-mgmt**, location API management role. ■ **no-access**, no commands are accessible.
`Server Group`	The name of a server group.
`Enable`	The **Enable** parameter indicates whether or not this feature is enabled or disabled.

The output of the **show aaa authentication mgmt** command includes the following parameters:

Related Commands

Command	Description	Mode
aaa authentication mgmt	Configure management authentication settings.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication stateful-ntlm

```
show aaa authentication stateful-ntlm [default|<profile-name>]
```

Description

This command shows the configuration settings of the stateful NT LAN Manager (NTLM) authentication profile.

Syntax

Parameter	Description
`default`	Shows the configuration settings of the default NTLM authentication profile.
`<profile-name>`	Shows the configuration settings of the specified NTLM authentication profile.

Usage Guidelines

This command shows the configuration settings of the stateful NTLM authentication profile. Issue this command without the **<profile-name>** parameter to display the entire stateful NTLM Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed Stateful NTLM authentication configuration information for that profile. Use this command to identify the default role assigned to users who have successfully authenticated using the NTLM authentication protocol, the name of the group of windows servers used to authenticate these users, and the NTLM authentication timeout period, in seconds.

Examples

The following example shows the configuration settings of the stateful NTLM authentication profile:

```
(host) [mynode] #show aaa authentication stateful-ntlm

Stateful NTLM Authentication Profile List
-----------------------------------------
Name                References  Profile Status
----                ----------  --------------
default             1
NTLMprofile1                                                    1

Total:2
```

Two stateful NTLM authentication profiles, **default** and **NTLMprofile1** are each referenced once by other profiles. The blank **Profile Status** column indicates that these profiles are both user-defined. If a profile is predefined, the value **Predefined** appears in the Profile Status column.

The following example displays configuration details for the stateful NTLM authentication profile “default”.

```
(host)[node] #show aaa authentication stateful-ntlm default

Stateful NTLM Authentication Profile "default"
----------------------------------------------
Parameter     Value
---------     -----
Default Role  guest
Server Group  default
Mode          Disabled
Timeout       10 sec
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	This parameter shows the role assigned to NTLM authenticated users.
`Server Group`	The name of a windows server group.
`Mode`	The **Mode** parameter indicates whether or not this authentication profile is enabled or disabled.
`Timeout`	Timeout period for an authentication request, in seconds.

Related Commands

Command	Description
aaa authentication stateful-ntlm	Use the command aaa authentication stateful-ntlm to configure the settings displayed in the output of this show command.

Command History

Version	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication stateful-dot1x

```
show aaa authentication stateful-dot1x [config-entries]
```

Description

This command shows the stateful configuration settings of 802.1X authentication for clients on non-Aruba APs.

Syntax

Parameter	Description
`config-entries`	Display details for the AP Server configuration list.

Usage Guidelines

Issue this command to identify the default role assigned to the 802.1X user group, name of the group of RADIUS servers used to authenticate the 802.1X users, and the 802.1X authentication timeout period in seconds.

Example

The following example shows the stateful configuration settings of 802.1X authentication information:

```
(host) [mynode] #show aaa authentication stateful-dot1x

Stateful 802.1X Authentication Profile
--------------------------------------
Parameter     Value
---------     -----
Default Role  guest
Server Group  newgroup2
Timeout       10 sec
Mode          Enabled
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	This parameter shows which role the controller uses for 802.1X authentication management.
`Server Group`	The name of a server group.
`Timeout`	Timeout period for an authentication request, in seconds.
`Mode`	The **Mode** parameter indicates whether or not this feature is enabled or disabled.

Include the **config-entries** parameter to this command to show the AP - Server Configuration List.

```
(host) [mynode] #show aaa authentication stateful-dot1x config-entries

AP-Server Configuration List
----------------------------
Cfg-Name        AP-IP           Server  Shared-Secret
```

```
--------        -----           ------  -------------
cfg22           10.3.14.6       RADIUS1 secret-pwd
```

The output of this command includes the following parameters:

Parameter	Description
`Cfg-Name`	is a auto-generated name
`AP-IP`	IP address of the AP.
`Server`	Name of the authentication server.
`Shared-Secret`	Shared authentication secret.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication stateful-kerberos

```
show aaa authentication stateful-kerberos [default|<profile-name>]
```

Description

This command shows the configuration settings of stateful Kerberos authentication profile.

Syntax

Parameter	Description
`default`	Shows configuration settings of default Kerberos profile.
`<profile-name>`	Shows configuration settings of specified Kerberos profile name.

Usage Guidelines

This command shows configuration settings of stateful Kerberos authentication profile. For the remaining parameters, see the command syntax.

Example

The following example shows the configuration settings of the stateful Kerberos authentication profile:

```
(host) [mynode] #show aaa authentication stateful-kerberos

Stateful Kerberos Authentication Profile List
---------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  0

Total:1
```

The following example shows the configuration settings of the stateful Kerberos authentication profile “default”.

```
(host) [mynode] #show aaa authentication stateful-kerberos default

Stateful Kerberos Authentication Profile "default"
--------------------------------------------------
Parameter     Value    Set
---------     -----    ---
Default Role  guest
Server Group  default
Timeout       10 sec
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication via auth-profile

```
show aaa authentication via auth-profile [<profile-name>]
```

Description

This command displays configuration settings for the VIA Authentication profile. Issue this command without the **<profile-name>** option to display the entire VIA Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed VIA authentication configuration information for that profile.

Syntax

Parameter	Description
<profile-name>	The name of an existing VIA authentication profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire VIA Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any VIA authentication profiles defined, use the command aaa authentication via auth-profile to configure your VIA authentication profiles.

Examples

This first example shows that there are three configured captive portal profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a VIA authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication via auth-profile

VIA Authentication Profile List
-------------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
via1     2
via2     1

Total:3
```

Include a VIA authentication profile name to display a complete list of configuration settings for that profile. The example below shows settings for the VIA authentication profile via1.

```
VIA Authentication Profile "via1"
---------------------------------
Parameter                    Value
---------                    -----
Default Role                 default-via-role
Server Group                 internal
Max Authentication failures  2
Description                  VIA config for the MV office
```

The output of this command includes the following parameters:

Parameter	Description
`Default Role`	Role assigned to the captive portal user upon login.
`Server Group`	Name of the group of servers used to authenticate captive portal users.
`Max Authentication failures`	Maximum number of authentication failures before the user is blacklisted.
`Description`	Description of the VIA authentication profile.

Related Commands

Command	Description	Mode
aaa authentication via auth-profile	Use aaa authentication via auth-profile to configure the parameters displayed in the output of this show command.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication via connection-profile

```
show aaa authentication via connection-profile [<profile-name>]
```

Description

This command displays configuration settings for the VIA connection profile. Issue this command without the **<profile-name>** option to display the entire VIA Connection profile list, including profile status and the number of references to each profile. Include a profile name to display detailed VIA connection configuration information for that profile.

Syntax

Parameter	Description
<profile-name>	The name of an existing VIA connection profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire VIA connection profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

If you do not yet have any VIA connection profiles defined, use the command **aaa authentication via connection-profile** **to configure your VIA connection profiles.**

Examples

This first example shows that there are three configured connection profiles in the Captive Profile Authentication Profile List. The **References** column lists the number of other profiles with references to a VIA connection profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #show aaa authentication via connection-profile

VIA Connection Profile List
---------------------------
Name          References  Profile Status
----          ----------  --------------
connection_1  3
connection_2  1
default       0

Total:3
```

Include a connection profile name to display a complete list of configuration settings for that profile. The example below shows settings for the captive portal profile connection_1.

```
VIA Connection Profile "default"
--------------------------------
Parameter                                                  Value
---------                                                  -----
VIA Servers                                                N/A
Client Auto-Login                                          Enabled
VIA Authentication Profiles to provision                   N/A
Allow client to auto-upgrade                               Enabled
```

```
VIA tunneled networks                                    N/A
Enable split tunneling                                   Disabled
VIA Client WLAN profiles                                 N/A
Allow client side logging                                Enabled
VIA IKE V2 Policy                                        Default
VIA IKE Policy                                           Default
Use Windows Credentials                                  Enabled
Enable IKEv2                                             Disabled
Use Suite B Cryptography                                 Disabled
IKEv2 Authentication method                              user-cert
VIA IPSec V2 Crypto Map                                  default-ikev2-dynamicmap/10000
VIA IPSec Crypto Map                                     default-dynamicmap/10000
Allow user to save passwords                             Enabled
Enable Supplicant                                        Disabled
Enable FIPS Module                                       Disabled
Auto-launch Supplicant                                   Disabled
Lockdown All Settings                                    Disabled
Domain Suffix in VIA Authentication                      Disabled
Enable Controllers Load Balance                          Disabled
Enable Domain Pre-connect                                Enabled
VIA Banner Message Reappearance Timeout(minutes)         60
VIA Client Network Mask                                  255.255.255.255
Validate Server Certificate                              Enabled
VIA Client DNS Suffix List                               N/A
VIA max session timeout                                  1440 min
VIA Logon Script                                         N/A
VIA Logoff Script                                        N/A
VIA Support E-Mail Address                               N/A
Maximum reconnection attempts                            3
VIA external download URL                                N/A
Allow user to disconnect VIA                             Enabled
Content Security Gateway URL                             N/A
Comma seperated list of HTTP ports to be inspected
(apart from default port 80)                             N/A
Enable Content Security Services                         Disabled
Keep VIA window minimized                                Disabled
Block traffic until VPN tunnel is up                     Disabled
Block traffic rules                                      N/A
```

The output of this command includes the following parameters:

Parameter	Description
VIA servers	Displays the following information about the VIA server: ■ *Controller Hostname/IP Address*: This is the public IP address or the DNS hostname of the VIA controller. Users will connect to remote server using this IP address or the hostname. ■ Controller Internal IP Address: This is the IP address of any of the VLAN interface IP addresses belongs to this controller. ■ Controller Description: This is a human-readable description of the controller.
Client Auto-Login	Enable or disable VIA client to auto login and establish a secure connection to the controller. Default: Enabled
VIA Authentication Profiles to provision	This is the list of VIA authentication profiles that will be displayed to users in the VIA client.

Parameter	Description
Allow client to auto-upgrade	Enable or disable VIA client to automatically upgrade when an updated version of the client is available on the controller. Default: Enabled
VIA tunneled networks	A list of network destination (IP address and netmask) that the VIA client will tunnel through the controller. All other network destinations will be reachable directly by the VIA client.
`Enable split-tunneling`	Enable or disable split tunneling. ■ If enabled, all traffic to the VIA tunneled networks will go through the controller and the rest is just bridged directly on the client. ■ If disabled, all traffic will flow through the controller. Default: off
Allow client-side logging	Enable or disable client side logging. If enabled, VIA client will collect logs that can be sent to the support email-address for troubleshooting. Default: Enabled
VIA Client WLAN profiles	A list of VIA client WLAN profiles that needs to be pushed to the client machines that use Windows Zero Config (WZC) to configure or manage their wireless networks.
VIA IKEv2 Policy	A list of IPsec crypto maps that the VIA client uses to connect to the controller. These IPsec Crypto Maps are configured in the CLI using the `crypto-local ipsec-map <ipsec-map-name>` command.
VIA IKE Policy	List of IKE policies that the VIA Client has to use to connect to the controller.
Use Windows Credentials	Enable or disable the use of the Windows credentials to login to VIA. If enabled, the SSO (Single Sign-on) feature can be utilized by remote users to connect to internal resources. Default: Enabled
Enable IKEv2	Select this option to enable or disable the use of IKEv2 policies for VIA.
Use Suite B Cryptography	Select this option to use Suite B cryptography methods. You must install the Advanced Cryptography license to use the Suite B cryptography.
IKEv2 Authentication method	List of all IKEv2 authentication methods.
VIA IPSec V2 Crypto Map	List of all IPsec V2 that the VIA client uses to connect to the controller.
VIA IPsec Crypto Map	List of IPsec Crypto Map that the VIA client uses to connect to the controller. These IPsec Crypto Maps are configured in CLI using the `crypto-local ipsec-map <ipsec-map-name>` command.
Allow user to save passwords	Enable or disable users to save passwords entered in VIA. Default: Enabled
Enable Supplicant	If enabled, VIA starts in bSec mode using L2 suite-b cryptography. This option is disabled by default.
Enable FIPS Module	Shows if the VIA (Federal Information Processing Standard) FIPS module is enabled, so VIA checks for FIPS compliance during startup. This option is disabled by default.
Auto-Launch Supplicant	Select this option to automatically connect to a configured WLAN network.

Parameter	Description
Lockdown All Settings	If enabled, all user options on the VIA client are disabled.
Domain Suffix in VIA Authentication	Enables a domain suffix on VIA Authentication, so client credentials are sent as *domainname\username* instead of just *username*.
Enable Controllers Load Balance	This option allows the VIA client to failover to the next available selected randomly from the list as configured in the VIA Servers option. If disabled, VIA will failover to the next in the sequence of ordered list of VIA Servers.
Enable Domain Pre-Connect	This option allows users with lost or expired passwords to establish a VIA connection to corporate network. This option authenticates the user's device and establishes a VIA connection that allows users to reset credentials and continue with corporate access.
VIA Banner Reappearance Timeout	The maximum time (in minutes) allowed before the VIA login banner reappears. Default: 1440 min
VIA Client Network Mask	The network mask that has to be set on the client after the VPN connection is established. Default: 255.255.255.255
Validate Server Certificate	Enable or disable VIA from validating the server certificate presented by the controller. Default: Enabled
VIA Client DNS Suffix List	The DNS suffix list (comma separated) that has be set on the client once the VPN connection is established. Default: None.
VIA max session timeout	The maximum time (minutes) allowed before the VIA session is disconnected. Default: 1440 min
VIA Logon Script	Name of the logon script that must be executed after VIA establishes a secure connection. The logon script must reside in the client computer.
VIA Logoff Script	Name of the log-off script that must be executed after the VIA connection is disconnected. The logoff script must reside in the client computer.
VIA Support E-mail Address	The support e-mail address to which VIA users will send client logs. Default: None.
Maximum reconnection attempts	The maximum number of re-connection attempts by the VIA client due to authentication failures. Default: 3
VIA external download URL	End users will use this URL to download VIA on their computers.
Allow user to disconnect VIA	Enable or disable users to disconnect their VIA sessions. Default: Enabled
Content Security Gateway URL	If split-tunnel forwarding is enabled, access to external (non-corporate) web sites will be verified by the specified content security service provider.
Comma Separated List of HTTP Ports	Traffic from the specified ports will be verified by the content security service provider.
Enable Content Security Services	Select this check box to enable content security service. You must install the Content Security Services licenses to use this option.

Parameter	Description
Keep VIA window minimized	Enable this option to minimize the VIA client to system tray during the connection phase. Applicable to VIA client installed in computers running Microsoft Windows operating system.
Block traffic until VPN tunnel is up	If enabled, this feature will block network access until the VIA VPN connection is established.
Block traffic rules	Specify a hostname or IP address and network mask to define a whitelist of users to which the **Block traffic until VPN tunnel is up** setting will not apply.

Related Commands

Command	Description	Mode
aaa authentication via connection-profile	Use aaa authentication via connection-profile to configure the parameters displayed in the output of this show command.	Config mode

Command History

Version	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication via global-config

```
show aaa authentication via global-config
```

Description

This command shows the VIA global configuration.

Syntax

No parameters.

Usage Guidelines

This command shows the VIA global configuration.

Example

The following example shows the VIA global configuration:

```
(host) [mynode] #show aaa authentication via global-config

VIA Global Configuration
------------------------
Parameter               Value     Set
---------               -----     ---
Allow VIA SSL Fallback  Disabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master or managed devices

show aaa authentication via web-auth

```
show aaa authentication via web-auth [default]
```

Description

A VIA web authentication profile contains an ordered list of VIA authentication profiles. The web authentication profile is used by end users to login to the VIA download page (https://<server-IP-address>/via) for downloading the VIA client. Only one VIA web authentication profile is available. If more than one VIA authentication profile is configured, users can view this list and select one during the client login.

Syntax

No parameters.

Usage Guidelines

Issue this command to view the authentication profiles associated with the default web authentication profile. Use it without the profile name to see the list of authentication profiles.

Examples

```
(host) #show aaa authentication via web-auth

VIA Web Authentication List
---------------------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1

(host) #show aaa authentication via web-auth default

VIA Web Authentication "default"
--------------------------------
Parameter                   Value
---------                   -----
VIA Authentication Profiles  via1
```

The output of this command includes the following parameters:

Parameter	Description
`VIA Authentication Profiles`	This is the name of the VIA authentication profile. The value column displays the order of priority in which the profiles are displayed in the VIA client login.

Related Commands

Command	Description	Mode
aaa authentication via web-auth	Use aaa authentication via web-auth to configure the parameters displayed in the output of this show command.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication vpn

```
show aaa authentication vpn [default|default-cap|default-rap]
```

Description

This command displays VPN authentication settings, including authentication roles and servers.

Usage Guidelines

Issue this command to identify the default role assigned to VPN users, the name of the group of servers used to authenticate the VPN users, and the maximum number of authentication failures allowed before the user is blacklisted.

Example

The following example displays configuration details for the VPN authentication profile **default**, **default-cap** and **default-rap**.

```
(host) #show aaa authentication vpn default

VPN Authentication Profile "default"
------------------------------------
Parameter                    Value
---------                    -----
Default Role                 default-vpn-role
Server Group                 default
Max Authentication failures  2

(TechPubs) #show aaa authentication vpn default-cap

VPN Authentication Profile "default-cap" (Predefined)
-----------------------------------------------------
Parameter                    Value
---------                    -----
Default Role                 ap-role
Server Group                 internal
Max Authentication failures  0

(TechPubs) #show aaa authentication vpn default-rap

VPN Authentication Profile "default-rap" (Predefined (changed))
---------------------------------------------------------------
Parameter                    Value
---------                    -----
Default Role                 default-vpn-role
Server Group                 default
Max Authentication failures  0
```

Parameter	Description
Default Role	The default role to be assigned to VPN users.
Server Group	The name of the server group that performs the authentication.
Max Authentication failures	Number of times a user attempted to authenticate, but failed.

Related Commands

Command	Description	Mode
aaa authentication via auth-profile	Use the command aaa authentication via auth-profile to configure the settings displayed in the output of this show command.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication wired

```
show aaa authentication wired
```

Description

View wired authentication settings for a client device that is directly connected to a port onthe controller.

Usage Guidelines

This command displays the name of the AAA profile currently used for wired authentication.

Example

The following example shows the current wired profile for the controller is a profile named “secure_profile_3.”

```
(host) #show aaa authentication wired
Wired Authentication Profile
----------------------------
Parameter    Value
---------    -----
AAA Profile  Secure_profile_3
```

Related Commands

Command	Description	Mode
aaa authentication wired	Use the command aaa authentication wired to configure the settings displayed in the output of this show command.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication wispr

```
show aaa authentication wispr <profile-name)
```

Description

This command shows information for a WISPr authentication profiles. Issue this command without the **<profile-name>** option to display the entire WISPr Authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed WISPr authentication configuration information for that profile.

Parameter	Description
<profile-name>	The name of an existing MAC authentication profile.

Examples

The output of the example below shows two WISPr authentication profiles, **default** and **WISPR1**, which are referenced two times by other profiles. the **Profile Status** columns are blank, indicating that these profiles are both user-defined. (If a profile is predefined, the value **Predefined** appears in the Profile Status column.)

```
(host) #show aaa authentication wispr

WISPr Authentication Profile List
---------------------------------
Name          References  Profile Status
----          ----------  --------------
default       2
WISPr1  2

Total:2

(host) #show aaa authentication wispr WISPr1
WISPr Authentication Profile "WISPr1"
-------------------------------------
Parameter                           Value
---------                           -----
Default Role                        guest
Server Group                        default
Logon wait minimum wait             5 sec
Logon wait maximum wait             10 sec
logon wait CPU utilization threshold  60 %
WISPr Location-ID ISO Country Code    US
WISPr Location-ID E.164 Country Code  1
WISPr Location-ID E.164 Area Code     408
WISPr Location-ID SSID/Zone           Corp1
WISPr Operator Name                   MyCompany
WISPr Location Name                   Sunnyvale
```

The following example displays configuration details for the WISPr authentication profile “WISPr1”.

```
(host) #show aaa authentication wispr WISPr1
WISPr Authentication Profile "WISPr1"
-------------------------------------
Parameter                           Value
```

```
---------                              -----
Default Role                           guest
Server Group                           default
Logon wait minimum wait                5 sec
Logon wait maximum wait                10 sec
logon wait CPU utilization threshold   60 %
WISPr Location-ID ISO Country Code     US
WISPr Location-ID E.164 Country Code   1
WISPr Location-ID E.164 Area Code      408
WISPr Location-ID SSID/Zone            Corp1
WISPr Operator Name                    MyCompany
WISPr Location Name                    Sunnyvale
```

The output of this command includes the following parameters:

Parameter	Description
Default Role	The default role to be assigned to users that have completed WISPr authentication.
Server Group	The name of the server group that performs the authentication.
`Logon wait minimum wait`	If the controller's CPU utilization has surpassed the **Login wait CPU utilization threshold value,** the **Logon wait minimum wait** parameter defines the minimum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 5 seconds.
`Logon wait maximum wait`	If the controller's CPU utilization has surpassed the logon **wait CPU utilization threshold** value, the **Logon wait maximum wait** parameter defines the maximum number of seconds a user will have to wait to retry a login attempt. Range: 1-10 seconds. Default: 10 seconds.
`WISPr Location-ID E.164 Area Code`	The E.164 Area Code in the WISPr Location ID.
`WISPr Location-ID E.164 Country Code  1`	The 1-3 digit E.164 Country Code in the WISPr Location ID.
`WISPr Location-ID ISO Country Code`	The ISO Country Code in the WISPr Location ID.
`WISPr Location-ID SSID/Zone`	The SSID/network name in the WISPr Location ID.
`WISPr Location Name`	A name identifying the hotspot location. If no name is defined, the default ap-name is used.
`WISPr Operator Name`	A name identifying the hotspot operator.

Related Commands

Command	Description
aaa authentication wispr	Configure WISPr authentication values on your controller.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication-server all

```
show aaa authentication-server all
```

Description

View authentication server settings for both external authentication servers and the internal controller database.

Usage Guidelines

The output of this command displays statistics for the Authentication Server Table, including the name and address of each server, server type and configured authorization and accounting ports.

Examples

The following command shows information for the internal Authentication server, and another RADIUS server named RADIUS-1.

```
(host) #show aaa authentication-server all

Auth Server Table
-----------------
Name      Type    FQDN  IP addr     AuthPort  AcctPort  Status    Requests
----      ----    ----  -------     --------  --------  ------    --------
Internal  Local   n/a   10.4.62.11  n/a       n/a       Enabled   0
server    Ldap    n/a   0.0.0.0     389       n/a       Enabled   0
server    Radius  SRVR1 127.9.9.61  1812      1813      Enabled   0
default   Tacacs  n/a   127.9.10.61 49        n/a       Enabled   0
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the authentication server.
Type	The type of authentication server. ArubaOS supports LDAP, RADIUS and TACACS+ servers, in addition to its own local, internal authentication server.
FQDN	The Fully-Qualified Domain Name of the server, if configured.
IP addr	IP address of the server, in dotted-decimal format.
AuthPort	Port number used for authentication. An LDAP server uses port 636 for LDAP over SSL, and port 389 for SSL over LDAP, Start TLS operation andclear text. The default RADIUS authentication port is port 1812.
AcctPort	Accounting port on the server. The default RADIUS accounting port is port 1813.
AcctPort	Accounting port on the server.
Status	Shows whether the Authentication server is enable or disabled.
Requests	Number of authentication requests received by the server.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication-server internal

```
show aaa authentication-server internal [statistics]
```

Description

View authentication server settings for the internal controller database.

Examples

The output of the command below shows that the internal authentication server has been disabled

```
(host) #show aaa authentication-server internal

Internal Server
---------------
Host      IP addr         Retries  Timeout  Status
----      -------         -------  -------  ------
Internal  10.168.254.221  3        5        Disabled
```

The following data columns appear in the output of this command:

Parameter	Description
Host	Name of the internal authentication server.
IP addr	Address of the internal server, in dotted-decimal format.
Retries	Number of retries allowed before the server stops attempting to authenticate a request.
Timeout	Timeout period, in seconds.
Status	Shows if the server is enabled of disabled

Include the **statistics** parameter to display additional details for the internal server.

```
(host) #show aaa authentication-server internal statistics

Internal Database Server Statistics
-----------------------------------
PAP Requests            8
PAP Accepts             8
PAP Rejects             0
MSCHAPv2 Requests       0
MSCHAPv2 Accepts        0
MSCHAPv2 Rejects        0
Mismatch Response       0
Users Expired           1
Unknown Response        0
Timeouts                1
AvgRespTime (ms)        0
Uptime (d:h:m)          4:3:32
SEQ first/last/free     1,255,255
```

The following data columns appear in the output of this command:

Parameter	Description
PAP Requests	Number of PAP requests received by the internal server.
PAP Accepts	Number of PAP requests accepted by the internal server.
PAP Rejects	Number of PAP requests rejected by the internal server.
MSCHAPv2 Requests	Number of MSCHAPv2 requests received by the internal server.
MSCHAPv2 Accepts	Number of MSCHAPv2 requests accepted by the internal server.
MSCHAPv2 Rejects	Number of MSCHAPv2 requests rejected by the internal server.
Mismatch Response	Number of times the server received an authentication response to a request after another request had been sent.
Users Expired	Number of users that were deauthenticated because they stopped responding.
Unknown Response	Number of times the server did not recognize the response, possibly due to internal errors.
Timeouts	Number of times that the controller timed out an authentication request.
AvgRespTime (ms)	Time it takes the server to respond to an authentication request, in seconds.
Uptime (d:h:m)	Time elapsed since the last server reboot.
SEQ first/last/free	This internal buffer counter keeps track of the requests to the authentication server.

Related Commands

Command	Description	Mode
aaa authentication-server internal	Issue the command aaa authentication-server internal to use the internal database on a managed device for authenticating clients.	Config mode

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication-server ldap

```
show aaa authentication-server ldap [statistics|<ldap_server_name> status]
```

Description

This command shows the configuration settings of LDAP servers.

Syntax

Parameter	Description
`statistics`	Shows the statistics of all LDAP servers.
`<ldap_server_name> status`	Shows the status of the specified LDAP server.

Usage Guidelines

This command shows the configuration settings of LDAP servers. For the remaining parameters, see the command syntax.

Examples

The following example shows the LDAP server list with the names of all the LDAP servers:

```
(host) [mynode] #show aaa authentication-server ldap

LDAP Server List
----------------
Name  References  Profile Status
----  ----------  --------------
ldap1 5
ldap2 3
ldap3 1

Total:3
```

The **References** column lists the number of other profiles that reference an LDAP server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa authentication-server radius

```
show aaa authentication-server radius [statistics|<rad_server_name> radsec status]
```

Description

This command shows the configuration settings of RADIUS servers.

Syntax

Parameter	Description
`statistics`	Shows the statistics of all RADIUS servers.
`<rad_server_name> radsec status`	Shows status of RADIUS over TLS of specified RADIUS server.

Usage Guidelines

This command shows the configuration settings of RADIUS servers. For the remaining parameters, see the command syntax.

Examples

The following example shows the RADIUS server list with the names of all the RADIUS servers:

```
(host) [mynode] #show aaa authentication-server radius

RADIUS Server List
------------------
Name         References  Profile Status
----         ----------  --------------
myserver     3
radius       0
servername   0

Total:3
```

The **References** column lists the number of other profiles that reference a RADIUS server, and the **Profile Status** column indicates whether the profile is predefined. User-defined servers will not have an entry in the **Profile Status** column.

Include the optional **statistics** parameter to this command to show the following statistics for all RADIUS servers:

Parameter	Description
`Server`	Name of the RADIUS server.
`Acct Rq`	Accounting requests. This reports of the number of accounting messages (for example, start/stop/interim update) sent by the controller to a RADIUS server. This counter increments whenever the controller sends one of these messages.
`Raw Rq`	Raw requests. Number of raw authentication requests the controller sent to a RADIUS server.

Parameter	Description
PAP Rq	Pap Requests. Number of PAP authentication requests the controller sent to a RADIUS server.
CHAP Rq	CHAP requests. Number of CHAP authentication requests the controller sent to a RADIUS server.
MSCHAP Rq	MSCHAP requests. Number of MS-CHAP authentication requests the controller sent to a RADIUS server.
MSCHAPv2 Rq	MSCHAPv2 requests. Number of MS-CHAPv2 requests the controller sent to a RADIUS server.
Mismatch Rsp	Mismatch responses. Number of responses from a RADIUS server for which the controller does not have the proper request context.
Bad Auth	Bad authenticator. Number of responses from the RADIUS server with an invalid secret or bad reply digest.
Acc	Access accept. Number of responses from the RADIUS server with invalid secret or bad reply digest.
Rej	Access reject. Number of responses from the RADIUS server that indicate that client authentication failed.
Acct Rsp	Accounting response. Number of responses sent from the RADIUS server in response to accounting requests sent from the controller.
Chal	Access challenge. Number of responses from the RADIUS server containing a challenge for the client (to complete authentication).
Ukn Rsp	Unknown Response code. Number of responses from the RADIUS server that were not understood by the controller due to the purpose or type of the response
Tmout	Timeouts. Number of messages sent by the controller for which the controller did not receive a response before the message timed out. **NOTE:** Timeouts include RADIUS accounting requests. Every request controller sends to the RADIUS server is monitored for a timeout, so each retry increments this counter.
AvgRspTme	Average response time. Time taken, on an average, for the RADIUS server to respond to a message from the controller.
Tot Rq	Total errors. This counter reflects the total number of requests sent to the RADIUS server (auth and accounting requests).
Tot Rsp	This counter reflects the total number of responses received by the RADIUS server (auth and accounting responses).
Rd Err	Read errors. This counter reflects the total number of errors encountered while reading off socket corresponding to that RADIUS server.
Uptime	Amount of for which the RADIUS server has been active/up. The RADIUS server is considered to have an UP status if the server is active and serving requests. The RADIUS server is considered to be DOWN if the server is not responding. For example, if the RADIUS server does not respond for (<no of retries> *< timeout>) seconds, the controller takes the RADIUS server down. It brings the radius server back into service after the dead timeout.

Parameter	Description
SEQ	Information corresponding to the sequence number of requests. **SEQ total** corresponds to the total number of sequence numbers that can be used to communicate with the RADIUS server. **SEQ free** corresponds to the free/available/not in use sequence numbers for a particular RADIUS server.

The following example shows additional details for a RADIUS server named alpha:

```
(host) [mynode] #show  aaa authentication-server radius alpha

RADIUS Server "alpha"
---------------------
Parameter                              Value
---------                              -----
Host                                   10.15.28.101
Key                                    ********
CPPM credentials                       ade/********
Auth Port                              1812
Acct Port                              1813
Radsec Port                            2083
Retransmits                            3
Timeout                                5 sec
NAS ID                                 N/A
NAS IP                                 N/A
Enable IPv6                            Disabled
NAS IPv6                               N/A
Source Interface                       N/A
Use MD5                                Disabled
Use IP address for calling station ID  Disabled
Mode                                   Enabled
Lowercase MAC addresses                Disabled
MAC address delimiter                  none
Service-type of FRAMED-USER            Disabled
Radsec                                 Enabled
Radsec Trusted CA Name                 can-new
Radsec Server Cert Name                N/A
Radsec Client Cert                     client-new
called-station-id                      macaddr colon disable
```

The output of this command includes the following information:

Parameter	Description
Host	IP address of the RADIUS server
Key	Shared secret between the controller and the authentication server.
CPPM credentials	Setting this parameter allows the controller to use configurable username and password instead of a support password.
Auth port	Authentication port on the server.
Acct Port	Accounting port on the server.
Radsec Port	Displays the Radsec port for RADIUS data transport.

Parameter	Description
Retransmits	Maximum number of retries sent to the server by the controller before the server is marked as down.
Timeout	Maximum time, in seconds, that the controller waits before timing out the request and resending it.
NAS ID	Network Access Server (NAS) identifier to use in RADIUS packets.
NAS IP	NAS IP address to send in RADIUS packets. If you do not configure a server-specific NAS IP, the global NAS IP is used.
Enable IPv6	Shows if the RADIUS server is enabled in IPv6 mode.
NAS IPv6	IPv6 address for the global NAS IP which the controller uses to communicate with all the RADIUS servers.
Source Interface	The source interface VLAN ID number.
Use MD5	If enabled, the RADIUS server will use a MD5 hash of cleartext password.
Use IP address for calling station ID	If enabled, the RADIUS server will use an IP address instead of a MAC address for calling station IDs.
Mode	Shows whether this server is **Enabled** or **Disabled**.
Lowercase MAC addresses	If this feature is enabled, the server will send MAC addresses in lowercase letters.
MAC address delimiter	The character used as a MAC address delimiter. If no character is specified, the RADIUS server will use a colon (:) by default.
Service-type of FRAMED-USER	If this option is enabled, the server sends the service-type as FRAMED-USER instead of LOGIN-USER. This option is disabled by default
Radsec	Displays the status of the Radsec server.
Radsec Trusted CA	Displays the Certificate Authority to sign Radsec certificates.
Radsec Server Cert Name	Displays the trusted Radsec server certificate.
Radsec Client Cert	Displays the Radsec client certificate on the RADIUS server that identifies and authenticates clients.
called-station-id	Configure this parameter to be sent with the RADIUS attribute Called Station ID for authentication and accounting requests. The **called-station-id** parameter can be configured to include AP group, AP MAC address, AP name, controller IP, controller MAC address, or user vlan. The default value is controller MAC address.

The following example shows details of RADIUS over TLS for a RADIUS server named beta:

```
(host) [mynode] #show aaa authentication-server radius <servername> radsec status
```

```
Radius Server "beta" Radsec Status
----------------------------------
Radsec Server Attribute  Value
-----------------------  -----
In Service               Yes
Connected Sockets        1
```

The output of this command includes the following information:

Parameter	Description
`In Service`	Shows the status of the Radsec RADIUS server.
`Connected Sockets`	Shows the number of TLS connections with the RADIUS server.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication-server tacacs

```
show aaa authentication-server tacacs [<tacacs_server_name>]|statistics
```

Description

Display configuration settings for your TACACS+ servers.

Syntax

Parameter	Description
`<tacacs_server_name>`	Name that identifies an TACACS+ server.
`statistics`	Displays accounting, authorization, and authentication request and response statistics for the TACACS server.

Examples

The output of the example below displays the TACACS+ server list with the names of all the TACACS+ servers. The **References** column lists the number of other profiles that reference a TACACS+ server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server tacacs

TACACS Server List
----------------
Name                    References  Profile Status
----                    ----------  --------------
LabAuth                  5
TACACS1                  3

Total:2
```

Include the <tacacs_server_name> parameter to display additional details for an individual server

```
(host) #show aaa authentication-server tacacs tacacs1

TACACS Server "tacacs1"
---------------------
Parameter    Value
---------    -----
Host         10.1.1.16
Key          ********
TCP Port     49
Retransmits  3
Timeout      20 sec
Mode         Enabled
```

Parameter	Description
`host`	IP address of the TACACS+ server
`Key`	Shared secret between the controller and the authentication server.

Parameter	Description
`TCP Port`	TCP port used by the server.
`Retransmits`	Maximum number of retries sent to the server by the controller before the server is marked as down.
`Timeout`	Maximum time, in seconds, that the controller waits before timing out the request and resending it.
`Mode`	Shows whether this server is **Enabled** or **Disabled**.

The output of this command includes the following parameters:

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa authentication-server windows

```
show aaa authentication-server windows [<windows_server_name>]
```

Description

Display configuration settings for your Windows servers.

Syntax

Parameter	Description
<windows_server_name>	Name that identifies a Windows server.

Examples

The output of the example below displays the Windows server list with the names of all the Windows servers used for NTLM authentication. The **References** column lists the number of other profiles that reference a Windows server, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) #aaa authentication-server tacacs

Windows Server List
-------------------
Name              References  Profile Status
----              ----------  --------------
NTLM               1
Windows2           1

Total:2
```

Include the <windows_server_name> parameter to display additional details for an individual server.

```
(host) #show aaa authentication-server windows Windows2

Windows Server "windows"
------------------------
Parameter         Value
---------         -----
Host              172.21.18.170
Mode              Enabled
Windows Domain    MyCompanyDomain
```

The output of this command includes the following parameters:

Parameter	Description
host	IP address of the Windows server
Mode	Shows whether this server is **Enabled** or **Disabled**.
Windows Domain	Name of the Windows domain to which this server is assigned.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show aaa bandwidth-contracts

```
show aaa bandwidth-contracts [dynamic | name]
```

Description

This command shows the contract names, ID numbers, Rate limits, and Note for your bandwidth contracts.

Syntax

Parameter	Description
dynamic	Displays dynamic bandwidth contracts.
name	Displays the bandwidth contract for the name specified.

Example

Specify a bandwidth contract name to view information for a specific bandwidth contract, or omit that parameter to view information for all bandwidth contracts configured . The output of the following command shows that the bandwidth contract **VLAN** has a configured rate of 6 Mbps, and the contract **User** has a rate of 2048 Kbps.

```
(host) #show aaa bandwidth-contracts VLAN

Bandwidth ContractInstances
-------------------
Contract      Id  Rate (bits/second)
--------      --  ------------------
VLAN          1   6000000
User          2   2048000

Total contracts = 2
Per-user contract total = 4096
Per-user contract usage = 0
```

Execute the following command to view the dynamic bandwidth contracts:

```
(host) #show aaa bandwidth-contracts dynamic
Dynamic Bandwidth Contracts
---------------------------
Contract                    Id    Rate          Note
--------                    --    ----          ----
"$#-DBW-0000000004-UP"          3     2000000 bps   Group(1)
"$#-DBW-0000000004-DN"          4     1000000 bps   Group(1)
"$#-DBW-44:00:00:00:00:02-UP"   5     5000000 bps   Individual
"$#-DBW-44:00:00:00:00:02-DN"   6     6000000 bps   Individual
"$#-DBW-44:00:00:00:00:03-UP"   7     5000000 bps   Individual
"$#-DBW-44:00:00:00:00:03-DN"   8     6000000 bps   Individual
Total Instances: 6
```

Related Commands

Command	Description	Mode
aaa bandwidth-contract	Use this command to define contracts to limit traffic for a user or VLAN.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **dynamic** parameter was added.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show aaa cluster essid

```
show aaa cluster essid <essid_val>

   bucketmap              all buckets in cluster essid table
   counters               display bucket counters
   keycache               keycache
   mac                    Match macaddr
   users                  all users
```

Description

This command displays information on essid counters, bucketmap, dormant keycache, mac address, and dormant user entries for a particular ESSID.

Syntax

Parameter	Description
`bucketmap`	Displays the bucketmap details for a specified bucket.
`counters`	Displays all the bucket counters.
`keycache [standby]`	Displays the dormant keycache entries.
`users [standby]`	Displays all user entries in dormant hash table.
`mac`	Displays the match mac address

Example

The output of the example below displays the bucketmap details and the counters for the essid, Zone1TestEssid:

show aaa cluster essid Zone1TestEssid bucketmap bucket 2

```
(host) (config) #show aaa cluster essid Zone1TestEssid bucketmap bucket 2

Active Bucket Values
--------------------
Essid                Bucket  ActiveUAC     StandbyUAC    L2Conn  IS_Active  IS_Standby
-----                ------  ---------     ----------    ------  ---------  ----------
Zone1TestEssid  2       10.15.146.5  10.15.146.4  1       0          0
```

show aaa cluster essid Zone1TestEssid counters

```
(host) (config) #show aaa cluster essid Zone1TestEssid counters

Counters for ESSID: Zone1TestEssid
Bucketmap essid create.....................1
Total Bucketmap updates................1
Last update reason ....................0
Last update time ...... Fri Jun 17 12:24:18 2016
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on managed devices

show aaa cluster essid-all

```
show aaa cluster essid-all
  bucketmap
  counters
  keycache
  users
```

Description

Displays all active essid entries in essid hash table. That is, it displays information on essid counters, bucketmap, dormant keycache, and dormant user entries.

Syntax

Parameter	Description
`bucketmap`	Displays the bucketmap details for a specified bucket.
`counters`	Displays all the bucket counters.
`keycache [standby]`	Displays the dormant keycache entries.
`users [standby]`	Displays all user entries in dormant hash table.

Example

The output of the example below displays the bucketmap details and the counters for a particular ESSID:

show aaa cluster essid-all bucketmap bucket 2

```
(host) (config) #show aaa cluster essid-all bucketmap bucket 2
Active Bucket Values
--------------------
Essid                Bucket  ActiveUAC    StandbyUAC   L2Conn  IS_Active  IS_Sta

       ndby
-----                ------  ---------    ----------   ------  ---------  ------

       ----
Zone1TestEssid  2       10.15.146.5  10.15.146.4  1       0          0
```

show aaa cluster essid-all counters

```
(host) (config) #show aaa cluster essid-all counters
Global Cluster Counters:
Cluster Enabled.................2
Cluster Disabled................2
BucketMap Add...................11
BucketMap Del...................6
Macuser Dormant Evts............2
Macuser Dormant Add.............1
Macuser Dormant Delete..........1
IPuser Dormant Evts.............2
IPuser Dormant Add..............1
IPuser Dormant Delete...........1
STA dormant del to SOS..........1
STA dormant create to SOS.......1
STA dormant IP create to SOS....1
STA dormant send keys to SOS....1
Total Bucketmap updates for the system  : 11
Counters for ESSID: SriniZone1TestEssid
```

```
Bucketmap essid create.....................1
Total Bucketmap updates................1
Last update reason ...................0
Last update time ...... Fri Jun 17 12:24:18 2016
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices

show aaa cluster gsm macuser-section mac

```
show aaa cluster gsm macuser-section mac <macaddr>
```

Description

This command displays gsm mac user section for a particular MAC address.

Syntax

Parameter	Description
`macaddr`	Displays the gsm mac user section for the specified MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices

show aaa cluster gsm ipuser-section

```
show aaa cluster gsm ipuser-section {ip <ipaddr> | ipv6 <ipv6-addr>}
```

Description

This command displays gsm ip user section for a particular IP address.

Syntax

Parameter	Description
`ipaddr`	Displays the gsm ip user section for the specified IP address.
`ipv6-addr`	Displays the gsm ip user section for the specified IPv6 address.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ipv6-addr** sub-parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices

show aaa cluster gsm user-section

```
show aaa cluster gsm user-section <uuid>
```

Description

This command displays gsm user section.

Syntax

Parameter	Description
`uuid`	Enter user uuid in hex.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices

show aaa cluster member

```
show aaa cluster member
```

Description

Displays all the cluster members with their IP address and the current cluster state.

Syntax

No syntax.

Example

The output of the example below displays the cluster members.

```
(host) (config) #show aaa cluster members

Current Cluster State: ENABLED, Count: Enabled(2), Disabled(2)
---------------------------------------------------------------
Cluster  IP           NASip
-------  --           -----
Self     10.15.146.3  0.0.0.0
Peer     10.15.146.4  0.0.0.0
Peer     10.15.146.5  0.0.0.0
Peer     10.15.146.6  0.0.0.0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices.

show aaa debug

```
show aaa debug
   age {dev-id-cache [mac <A:B:C:D:E:F>]|key-cache [mac <A:B:C:D:E:F>]|pmk-cache [mac
   <A:B:C:D:E:F>]}
   pmk bss-table [<A:B:C:D:E:F>]
   role user {ip <A.B.C.D>|ipv6 <ipv6addr>|mac <A:B:C:D:E:F>}
   vlan user {ip <A.B.C.D>|ipv6 <ipv6addr>|mac <A:B:C:D:E:F>}
```

Description

This command shows AAA related debug information.

Syntax

Parameter	Description

`age`
`dev-id-cache`
`key-cache`
`pmk-cache`
	Displays the age of the GSM entry since the previous refresh (in seconds) based on:
	■ **dev-id-cache**—Device ID information in memory.
	■ **key-cache**—Key cache information in memory.
	■ **pmk-cache**—Pairwise Master Key (PMK) cache information in memory.

`pmk bss-table`	Displays PMK related debug information based on the BSSID address.

`role user`
`ip`
`ipv6`
`mac`
	Displays role derivation related debug information based on:
	■ **ip**—IPv4 address of the client.
	■ **ipv6**—IPv6 address of the client.
	■ **mac**—MAC address of the client.

`vlan user`
`ip`
`ipv6`
`mac`
	Displays VLAN derivation related debug information based on:
	■ **ip**—IPv4 address of the client.
	■ **ipv6**—IPv6 address of the client.
	■ **mac**—MAC address of the client.

Usage Guidelines

This command shows AAA related debug information.

Example

The following example shows the VLAN derivation debug information of an user with IPv4 address.

```
(host) [mynode] #show aaa debug vlan user ip 192.0.2.1

VLAN types present for this User
================================
Default VLAN                    : 3
Initial Role Contained          : 1
User Dot1x Role Contained       : 5
Dot1x Server Rule               : 5

VLAN Derivation History
=======================
VLAN Derivation History Index  :  8
1. VLAN 1    for Default VLAN
2. VLAN 1    for Current VLAN updated
3. VLAN 0    for Reset VLANs for Station up
4. VLAN 3    for Default VLAN
5. VLAN 1    for Initial Role Contained
6. VLAN 5    for Dot1x Server Rule
```

```
7. VLAN 5     for User Dot1x Role Contained
8. VLAN 5     for Current VLAN updated

Current VLAN : 5 (Dot1x Server Rule)
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa debug dev-id-cache section

```
show aaa debug dev-id-cache section {mac <macaddr>}
```

Description

This command shows section data from ClearPass Policy Manager NetWatch.

Syntax

Parameter	Description	Range	Default
`mac <macaddr>`	Shows section data from specified MAC address.	–	–

Usage Guidelines

This command shows section data from ClearPass Policy Manager NetWatch. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to show section data from MAC address **00:1a:1e:aa:bb:cc**:

```
(host) [mynode] #show aaa debug dev-id-cache section mac 00:1a:1e:aa:bb:cc

Device ID Cache Section: cppm Info
----------------------------------
Mac Address  Device Type  OS Version  Device Name  Updated At
-----------  -----------  ----------  -----------  ----------
```

Related Commands

Command	Description
show airgroup	This command displays AirGroup settings.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show aaa debug pmk bss-table

```
show aaa debug pmk bss-table [bssid <bssid>]
```

Description

This command shows information linking the PMK to the BSS.

Syntax

Parameter	Description	Range	Default
`bssis <bssid>`	Shows information linking the PMK to the specified BSSID.	–	–

Usage Guidelines

This command shows information linking the PMK to the BSS.

Example

The following example shows the authentication survivability cached data:

```
(host) [mynode] #show aaa debug pmk bss-table

PMK BSS-Table
-------------
BSSID  Mac Address
-----  -----------

Total entries = 0
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show aaa debug stm message stats

```
show aaa debug stm message stats
```

Description

This command shows the number of messages sent/received from STM.

Syntax

This command does not have any parameters.

Usage Guidelines

This command shows the number of messages sent/received from STM.

Example

Access the CLI and use the following command to show the number of messages sent/received from STM:

```
(host) [mynode] #show aaa debug stm message stats

AUTH<-->STM Messages
--------------------
Msg Type                                Total Msgs
-----------                               ----------
STM sta down                              0
STM ap location                           0
STM sta create H323                       0
STM ap state resp                         0
STM sta state resp                        0
STM tunnel resp                           0
STM monitor time                          0
STM rap user mesg                         0
STM rap user rad acct                     0
STM rap sos user ageout                   0
STM rap user rem                          0
STM rap sta state resp                    0
STM rap bridge sta info                   0
STM ap global state total                 514
STM ap global state add                   0
STM ap global state del                   514
STM ap global state modify                0
STM ap global state del sent to ike       505
STM ap global state del not sent to ike   9
STM ap provision state                    0
STM ap authen status                      0
STM FT auth req                           0
STM FT reassoc req                        0
STM FT ask R1data                         0
STM FT push R0data                        0
STM FT push neighbor                      0
STM restart mesg                          1
STM rap user agent update                 0
STM hotspot mesg                          0
STM unknown mesg                          0
                                          0
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show aaa debug vlan user

```
show aaa debug vlan user [ip <ip addr>|ipv6 <ipv6addr>|mac <macaddr>]
```

Description

Display user VLAN derivation related debug information.

Syntax

Parameter	Description
`ip <ip addr>`	User identification based on IPv4 address.
`ipv6 <ipv6addr>`	User identification based on IPv6 address.
`mac <macaddr>`	User identification based on MAC address.

Example

The output of the example below displays the VLAN derivation debug information of an user with IPv4 address.

```
(host) #show aaa debug vlan user ip 192.0.2.1

VLAN types present for this User
================================
Default VLAN                    : 3
Initial Role Contained          : 1
User Dot1x Role Contained       : 5
Dot1x Server Rule               : 5

VLAN Derivation History
=======================
VLAN Derivation History Index  :  8
1. VLAN 1    for Default VLAN
2. VLAN 1    for Current VLAN updated
3. VLAN 0    for Reset VLANs for Station up
4. VLAN 3    for Default VLAN
5. VLAN 1    for Initial Role Contained
6. VLAN 5    for Dot1x Server Rule
7. VLAN 5    for User Dot1x Role Contained
8. VLAN 5    for Current VLAN updated

Current VLAN : 5 (Dot1x Server Rule)
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa derivation-rules

```
show aaa derivation-rules [server-group <group-name>|user <name>]
```

Syntax

Parameter	Description
`<group-name>`	Name of a server group
`<name>`	Name of a user rule group

Description

Show derivation rules based on user information or configured for server groups.

Example

The output of the following command shows that the server group group1 has the internal database configured as its authentication server, and that there is a single rule assigned to that group. You can omit the **<group-name>** parameter to show a table of all your server groups.

```
(host) #show aaa derivation-rules server-group group1

Server Group

Name      Inservice  trim-FQDN  match-FQDN
----      ---------  ---------  ----------
Internal         Yes        No

Server Rule Table
-----------------
Priority  Attribute  Operation  Operand   Action    Value  Total Hits  New Hits
--------  ---------  ---------  -------   ------    -----  ----------  --------
1         Filter-Id  equals     nsFilter  set vlan  111    24
Rule Entries: 1
```

The following data columns appear in the output of this command:

Parameter	Description
`Name`	Name of the authentication server assigned to this server group
`Inservice`	Specifies if the server is in service or out-of-service.
`trim-FDQN`	If enabled, user information in an authentication request is edited before the request is sent to the server.
`match-FDQN`	If enabled, the authentication server is associated with a specified domain.
`Priority`	The priority in which the rules are applied. Rules at the top of the list are applied before rules at the bottom.
`Attribute`	This is the attribute returned by the authentication server that is examined for **Operation** and **Operand** match

Parameter	Description
`Operation`	This is the match method by which the string in **Operand** is matched with the attribute value returned by the authentication server. ■ **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. ■ **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. ■ **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. ■ **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. ■ **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. ■ **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
`Operand`	This is the string to which the value of the returned attribute is matched.
`Action`	This parameter identifies whether the rule sets a server group role (**set role**) or a VLAN (**set vlan**).
`Value`	Sets the user role or VLAN ID to be assigned to the client if the condition is met.
`Total Hits`	Number of times the rule has been applied since the last server reboot.
`New Hits`	Number of times the rule has been applied since the **show aaa derivation-rules** command was last issued.

To display derivation rules for a user group, include the **user <name>** parameter. You can also display a table of all user rules by including the **user** parameter, but omitting the **<name>** parameter

```
(host) #show aaa derivation-rules user user44
User Rule Table
---------------
Priority  Attribute  Operation  Operand  Action    Value  Total Hits  New Hits
Description
--------  ---------  ---------  -------  ------    -----  ----------  --------                  ------
-
1         location   equals     ap23                                    set role  guest  56
                                                                  guestrole1
```

The following data columns appear in the output of this command:

Parameter	Description
Priority	The priority in which the rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	This is the attribute returned by the authentication server that is examined for **Operation** and **Operand** match.
Operation	This is the match method by which the string in **Operand** is matched with the attribute value returned by the authentication server. ■ **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. ■ **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. ■ **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. ■ **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. ■ **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. ■ **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	This is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the rule sets a server group role (**set role**) or a VLAN (**set vlan**).
Value	Sets the user role or VLAN ID to be assigned to the client if the condition is met.
Total Hits	Number of times the rule has been applied since the last server reboot.
New Hits	Number of times the rule has been applied since the **show aaa derivation-rules** command was last issued.
Description	This optional parameter describes the rule. If no description was configured then it does not appear when you view the User Table.

Related Commands

Command	Description	Mode
aaa derivation-rules	Use aaa derivation-rules to define the parameters displayed in the output of this show command.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa device-id-cache

```
show aaa device-id-cache [mac <A:B:C:D:E:F>] [rows number number]
```

Description

This command shows the device ID cache information.

Syntax

Parameter	Description
`mac <A:B:C:D:E:F>`	Shows device ID cache information for specified MAC address.
`rows number number`	Shows device ID cache information for specified rows starting at specified row number.

Usage Guidelines

This command shows the device ID cache information. For the remaining parameters, see the command syntax.

Example

The following example shows the device ID cache information:

```
(host) [mynode]#show aaa device-id-cache

Device ID Cache
---------------
MAC  Device ID  Last Update
---  ---------  -----------

Device ID Cache Entries : 0
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa dns-query-interval

```
show aaa dns-query-interval <minutes>
```

Description

View the configured interval between DNS requests sent from the controller to the DNS server.

Syntax

No parameters

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. By default, DNS requests are sent every 15 minute, but the interval can be changed using the aaa dns-query-period command. Issue the **show aaa dns-query-period** command to view the current DNS query interval.

Example

This command shows that the controller will send a DNS query every 30 minutes

```
(host) # show aaa dns-query-period
DNS Query Interval = 30 minutes
```

Related Commands

To configure the DNS query interval, issue the command aaa dns-query-interval.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master and managed devices

show aaa fqdn-server-names

```
show aaa fqdn-server-names
```

Description

Show a table of IP addresses that have been mapped to fully qualified domain names (FQDNs).

Syntax

No parameters.

Usage Guidelines

If you define a RADIUS server using the FQDN of the server rather than its IP address, the controller will periodically generate a DNS request and cache the IP address returned in the DNS response. Issue this command to view the IP addreses that currently correlate to each RADIUS server FQDN.

Example

The output of this command shows the IP addresses for two RADIUS servers.

```
(host) #show aaa fqdn-server-names

Auth Server FQDN names
----------------------
FQDN                    IP Address      IPv6 Address    Refcount
----                    ----------      --------        --------
myhost1.example.com     192.0.2.3
2myhost2.example.com    192.0.2.5                       3
```

Related Commands

To configure a RADIUS authentication server using that server's fully qualified domain name, use the command aaa authentication-server radius.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master and managed devices

show aaa load-balance statistics

```
show aaa load-balance statistics server-group <sg_name>
```

Description

Display the load balancing statistics for RADIUS servers.

Syntax

Parameter	Description
`<sg_name>`	Name of the server group.

Example

```
(host) #show aaa load-balance statistics server-group dot1x-test-apsim
Statistics for Radius Servers in Server Group
---------------------------------------------
Server          Acct Rq  Raw Rq  PAP Rq  CHAP Rq  MSCHAP Rq  MSCHAPv2 Rq  Mismatch Rsp  Bad
Auth  Acc  Rej  Acct Rsp  Chal  Ukn Rsp  Tmout  Tot Rq  Tot Rsp  Rd Err  Outstanding Auths
------          -------  ------  ------  -------  ---------  -----------  ------------  -------
-  ---  ---  --------  ----  -------  -----  ------  -------  ------  -----------------
abc _RADIUS    0         0       0       0         0          26            0             0
 26   0    0         0     0        0      26      26       0       0
AUTOMATIONRAD  0         0       0       0         0          207           0             0
  207  0    0         0     0        0      207     207      0       0
```

Parameter	Description
`Server`	Name of the RADIUS server.
`Acct Rq`	Accounting requests. This reports the number of accounting messages (for example, start/stop/interim update) sent by the controller to a RADIUS server. This counter increments whenever the controller sends one of these messages.
`Raw Rq`	Raw requests. Number of raw authentication requests the controller sent to a RADIUS server.
`PAP Rq`	PAP Requests. Number of PAP authentication requests the controller sent to a RADIUS server.
`CHAP Rq`	CHAP requests. Number of CHAP authentication requests the controller sent to a RADIUS server.
`MSCHAP Rq`	MSCHAP requests. Number of MS-CHAP authentication requests the controller sent to a RADIUS server.
`MSCHAPv2 Rq`	MSCHAPv2 requests. Number of MS-CHAPv2 requests the controller sent to a RADIUS server.
`Mismatch Rsp`	Mismatch responses. Number of responses from a RADIUS server for which the controller does not have the proper request context.

Parameter	Description
Bad Auth	Bad authenticator. Number of responses from the RADIUS server with an invalid secret or bad reply digest.
Acc	Access accept. Number of responses from the RADIUS server with invalid secret or bad reply digest.
Rej	Access reject. Number of responses from the RADIUS server that indicate that client authentication failed.
Acct Rsp	Accounting response. Number of responses sent from the RADIUS server in response to accounting requests sent from the controller.
Chal	Access challenge. Number of responses from the RADIUS server containing a challenge for the client (to complete authentication).
Ukn Rsp	Unknown Response code. Number of responses from the RADIUS server that were not understood by the controller due to the purpose or type of the response
Tmout	Timeouts. Number of messages sent by the controller for which the controller did not receive a response before the message timed out. **NOTE:** Timeouts include RADIUS accounting requests. Every request controller sends to the RADIUS server is monitored for a timeout, so each retry increments this counter.
AvgRspTme	Average response time. Time taken, on an average, for the RADIUS server to respond to a message from the controller.
Tot Rq	Total errors. This counter reflects the total number of requests sent to the RADIUS server (auth and accounting requests).
Tot Rsp	This counter reflects the total number of responses received by the RADIUS server (auth and accounting responses).
Rd Err	Read errors. This counter reflects the total number of errors encountered while reading off socket corresponding to that RADIUS server.
Uptime	Amount of for which the RADIUS server has been active/up. The RADIUS server is considered to have an UP status if the server is active and serving requests. The RADIUS server is considered to be DOWN if the server is not responding. For example, if the RADIUS server does not respond for (<no of retries> *< timeout>) seconds, the controller takes the RADIUS server down. It brings the radius server back into service after the dead timeout.
SEQ	Information corresponding to the sequence number of requests. **SEQ total** corresponds to the total number of sequence numbers that can be used to communicate with the RADIUS server. **SEQ free** corresponds to the free/available/not in use sequence numbers for a particular RADIUS server.
Outstanding Auths	This value keeps track of the number of clients that are currently getting authenticated against this authentication server, i.e. clients for which the controller has sent Access-Request but has not yet received Access-Accept or Access-Reject and also the Access-Request has not timed out completely.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa main-profile

```
show aaa main-profile summary
```

Description

Show a summary of all AAA profiles.

Example

The output of the **show aaa main-profile summary** command shows roles, server group settings, and wire-to-wireless-roaming statistics for each AAA profile.

```
(host) #show aaa main-profile summary

AAA Profile summary
-------------------
                            dot1x-  rad-                                UDR-   ww-    enforce
Name       role   mac-auth  auth    acct   XML-api   RFC3576   group roam    devtype -dhcp
----       ----   --------  ------  ----   -------   -------   ----- ----    ------- -------
aaa_dot1x  logon  macprof2  dot1x   RADIUS 10.3.1.15 10.3.15.2 Usr1  Disable enabled disabled
default    logon  macprof2  dot1x   RADIUS 10.3.1.15 10.3.15.2 Usr1  Disable enabled disabled
default    guest  macprof1  default RADIUS 10.3.1.15 10.3.15.2 Usr2  Disable enabled disabled
guest
```

The following data columns appear in the output of this command:

Parameter	Description
Name	Name of the AAA profile.
role	Role for unauthenticated users.
mac-auth	Name of the server group used for MAC authentication.
dot1x-auth	Name of the server group used for dot1x authentication.
rad-act	Name of the server group used for RADIUS authentication.
XML-api	IP address of a configured XML API server.
RFC3576	IP address of a RADIUS server that can send user disconnect, session timeout and change-of-authorization messages, as described in RFC 3576.
UDR-group	Name of the user derivation rule profile.
ww-roam	Shows if wired-to-wireless roaming is enabled or disabled.
devtype	Shows if the device identification feature is enabled or disabled. When devtype-classification parameter is enabled, the output of the show user and show user-table commands shows each client's device type, if that client device can be identified.
enforce-dhcp	When this option is enabled, clients must complete a DHCP exchange to obtain an IP address. Best practices are to enable this option when you use the **aaa derivation-rules** command to create a rule with the **DHCP-Option** rule type. This parameter is disabled by default.

Related Commands

Command	Description	Mode
aaa profile	Use aaa profile define the parameters displayed in the output of this show command.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa multiple-server-accounting statistics server-group

```
show aaa multiple-server-accounting statistics server-group <sg_name>
```

Description

This command shows the multiple server accounting statistics for a server-group.

Syntax

Parameter	Description	Range	Default
<sg_name>	Shows the multiple server accounting statistics for the specified server-group.	—	—

Usage Guidelines

This command shows the multiple server accounting statistics for a server-group. For the remaining parameters, see the command syntax.

Example

The following example shows the multiple server accounting statistics for a server-group corp1:

```
(host) [mynode] #show aaa multiple-server-accounting statistics server-group corp1

Multiple Server Accounting Statistics for Radius Servers in Server Group
------------------------------------------------------------------------
Server  Acct Start Req  Acct Interim Req  Acct Stop Req
------  --------------  ----------------  -------------

Acct Start Resp  Acct Interim Resp  Acct Stop Resp  Unknown Resp
---------------  -----------------  --------------  ------------
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show aaa password-policy mgmt

```
show aaa password-policy mgmt [statistics]
```

Description

Show the current password policy for management users.

Syntax

Parameter	Description
`statistics`	Include this optional parameter to show the numbers of failed login attempts and any lockout periods for management user accounts.

Examples

The output of the **show aaa password-policy mgmt** command below shows that the current password policy requires a management user to have a password with a minimum of 9 characters, including one numeric character and one special character

```
(host) #show aaa password-policy mgmt

Mgmt Password Policy
--------------------
Parameter Value
--------- -----
Enable password policy                  Yes
Minimum password length required                        9
Minimum number of Upper Case characters                         0
Minimum number of Lower Case characters                         0
Minimum number of Digits                        1
Minimum number of Special characters (!, @, #, $, %, ^, &, *, <, >, {, }, [, ], :, ., comma,
|, +, ~, `)                     1
Username or Reverse of username NOT in Password                         No
Maximum Number of failed attempts in 3 minute window to lockout user                    0
Time duration to lockout the user upon crossing the "lock-out" threshold                        3
Maximum consecutive character repeats                   0
```

The following data columns appear in the output of this command:

Parameter	Description
Enable password policy	Shows if the defined policy has been enabled
Minimum password length required	Minimum number of characters required for a management user password. The default setting is 6 characters.
Minimum number of Upper Case characters	The maximum number of uppercase letters required for a management user password. By default, there is no requirement for uppercase letters in a password, and the parameter has a default value of 0.

Parameter	Description
Minimum number of Lower Case characters	The maximum number of lowercase letters required for a management user password. By default, there is no requirement for lowercase letters in a password, and the parameter has a default value of 0.
Minimum number of Digits	Minimum number of numeric digits required in a management user password. By default, there is no requirement for digits in a password, and the parameter has a default value of 0.
Minimum number of Special characters	Minimum number of special characters required in a management user password. By default, there is no requirement for special characters in a password, and the parameter has a default value of 0.
Username or Reverse of username NOT in Password	If **Yes**, a management user's password cannot be the user's username or the username spelled backwards. If **No**, the password can be the username or username spelled backwards.
Maximum Number of failed attempts in 3 minute window to lockout user	Number of times a user can unsuccessfully attempt to log in to the controller before that user gets locked out for the time period specified by the **lock-out threshold** below. By default, the password lockout feature is disabled, and the default value of this parameter is 0 attempts.
Time duration to lockout the user upon crossing the "lock-out" threshold	Amount of time a management user will be "locked out" and prevented from logging into the controller after exceeding the maximum number of failed attempts setting show above. The default lockout time is 3 minutes.
Maximum consecutive character repeats	The maximum number of consecutive repeating characters allowed in a management user password. By default, there is no limitation on the numbers of character that can repeat within a password, and the parameter has a default value of 0 characters.

```
(host) #show aaa password-policy mgmt statistics

Management User Table
---------------------
USER    ROLE   FAILED_ATTEMPTS  STATUS
----    ----   ---------------  ------
admin14 root   1                Locked until 12/1/2009 22:28
```

Include the optional **statistics** parameter to show failed login statistics in the Management User table. The example below shows that a single failed login attempt locked out the root user **admin14**, and displays the time when that user can attempt to login to the controller again.

Related Commands

Command	Description	Mode
aaa profile	Use aaa profile define the parameters displayed in the output of this show command.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa profile

```
show aaa profile <profile-name>
```

Description

Show configuration details for an individual AAA profile.

Example

The output of the following command shows roles, servers and server group settings, and wire-to-wireless-roaming statistics for each AAA profile.

```
(host) #show aaa profile default

AAA Profile "default"
---------------------
Parameter                          Value
---------                          -----
Initial role                       guest
MAC Authentication Profile         N/A
MAC Authentication Default Role    guest
MAC Authentication Server Group    default
802.1X Authentication Profile      default
802.1X Authentication Default Role guest
802.1X Authentication Server Group N/A
Download Role from CPPM            Disabled
L2 Authentication Fail Through     Disabled
Multiple Server Accounting         Disabled
User idle timeout                  N/A
RADIUS Accounting Server Group     N/A
RADIUS Roaming Accounting          Enabled
RADIUS Interim Accounting          Disabled
XML API server                     N/A
RFC 3576 server                    N/A
User derivation rules              N/A
Wired to Wireless Roaming          Enabled
SIP authentication role            N/A
Device Type Classification         Enabled
Enforce DHCP                       Disabled
PAN Firewall Integration           Disabled
Open SSID radius accounting        Disabled
```

The following data columns appear in the output of this command:

Parameter	Description
Name	The name of the AAA profile.
Initial Role	Role for unauthenticated users.
MAC Authentication Profile	Name of the MAC authentication profile.
MAC Authentication Default Role	Configured role assigned to the user after MAC authentication.
MAC Authentication Server Group	Name of the server group used for MAC authentication.

Parameter	Description
8021.X Authentication Profile	Name of the 802.1X authentication profile.
8021.X Authentication Default Role	Configured role assigned to the user after 802.1X authentication.
8021.X Authentication Server Group	Name of the server group used for 802.1X authentication.
Download Role from CPPM	Status of role download from ClearPass Policy Manager. If enabled, the controller downloads the role from ClearPass Policy Manager if not defined.
L2 Authentication Fail Through	To select the other authentication method if one fails.
Multiple Server Accounting	Status of multiple server accounting. If enabled, the controller sends RADIUS accounting to all servers in RADIUS accounting server group.
User idle timeout	The user idle timeout for this profile. Specify the idle timeout value for the client in seconds. A value of 0, deletes the user immediately after disassociation from the wireless network. Valid range is 30-15300 in multiples of 30 seconds.
RADIUS Accounting Server Group	Name of the server group used for RADIUS authentication.
RADIUS Roaming Accounting	Displays if Roaming RADIUS accounting service is enabled / disabled, assists in tracking a client who roams to a different AP.
RADIUS Interim Accounting	By default, the RADIUS accounting feature sends only start and stop messages to the RADIUS accounting server. If RADIUS Interim Accounting is enabled, the controller to can also end Interim-Update messages with current user statistics to the server at regular intervals.
XML API server	IP address of a configured XML API server.
RFC 3576 server	IP address of a RADIUS server hat can send user disconnect, session timeout and change-of-authorization messages, as described in RFC 3576.
User derivation rules	User attribute profile from which the user role or VLAN is derived.
Wired to Wireless Roaming	Shows whether Wired to Wireless Roaming is **Enabled** or **Disabled**.
SIP authentication role	For controllers with an installed PEFNG license, this parameter displays the configured role assigned to a session initiation protocol (SIP) client upon registration.
Device Type Classification	Shows if the device identification feature is enabled or disabled. When devtype-classification parameter is enabled, the output of the show user and show user-table commands shows each client's device type, if that client device can be identified.

Parameter	Description
Enforce DHCP	When this option is enabled, clients must complete a DHCP exchange to obtain an IP address. Best practices are to enable this option when you use the **aaa derivation-rules** command to create a rule with the **DHCP-Option** rule type. This parameter is disabled by default.
PAN firewall Integration	Displays the status of the PAN firewall integration.
Open SSID Radius Accounting	Displays the Open system SSID RADIUS accounting status.

Related Commands

Command	Description	Mode
aaa profile	Use the command aaa profile to define AAA profiles.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.
ArubaOS 8.1	The **RADIUS Roaming Accounting** parameter was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa pubcookie-authentication

```
show aaa pubcookie-authentication
```

Description

This command shows pubcookie authentication configuration.

Syntax

No parameters.

Usage Guidelines

This command shows pubcookie authentication configuration.

Example

The following example shows the pubcookie authentication configuration:

```
(host) [mynode] #show aaa pubcookie-authentication
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show aaa radius-attributes

```
show aaa radius-attributes
```

Description

Show RADIUS attributes recognized by the controller.

Example

The output of the following command shows the name, currently configured value, type, vendor and RADIUS ID for each attribute.

```
(host) #show aaa radius-attributes

Dictionary
----------
Attribute                       Value  Type     Vendor     Id
---------                       -----  ----     ------     --
MS-CHAP-NT-Enc-PW               6      String   Microsoft  311
Suffix                          1004   String
Menu                            1001   String
Acct-Session-Time               46     Integer
Framed-AppleTalk-Zone           39     String
Connect-Info                    77     String
Acct-Ouput-Packets              48     Integer
Aruba-Location-Id               6      String   Aruba      14823
Service-Type                    6      Integer
Rad-Length                      310    Integer
CHAP-Password                   3      String
Aruba-Template-User             8      String   Aruba      14823
Event-Timestamp                 55     Date
Login-Service                   15     Integer
Exec-Program-Wait               1039   String
Tunnel-Password                 69     String
Framed-IP-Netmask               9      IP Addr
Acct-Output-Gigawords           53     Integer
MS-CHAP-CPW-2                   4      String   Microsoft  311
Acct-Tunnel-Packets-Lost        86     Integer
...
```

Related Commands

Command	Description	Mode
aaa profile	Use the command aaa profile to define AAA profiles.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa radius modifier

```
show aaa radius modifier <rad_modifier_name>
```

Description

This command displays all the RADIUS modifier profiles.

Example

```
(host) [md] #show aaa radius modifier
Radius Modifier Profile List
----------------------------
Name    References  Profile Status
----    ----------  --------------
test    0
test1   0
Total:2
```

Related Commands

Command	Description	Mode
`aaa radius modifier`	Use the command aaa radius modifier to customize the RADIUS attributes.	Config mode

Command History

Version	Modification
ArubaOS 8.2.0.0	The **rad_modifier_name** parameter was added.
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master and managed devices.

show aaa rfc-3576-server

```
show aaa rfc-3576-server
<server-ip>
statistics
udp-port
```

Description

Show configuration details for an RFC-3576 server, which is a RADIUS server that can send user disconnect, session timeout and change-of-authorization (CoA) messages, as described in RFC 3576.

Syntax

Parameter	Description
`<server-ip>`	IP address of an RFC-3576 server
`statistics`	View detailed connection and authentication information for all RFC 3575 servers.
`udp-port`	Show the configured RFC3576 server port. The default value is port 3799.

Example

This first example shows that there are two configured servers in the RFC 3567 Server List. The **References** column lists the number of other profiles with references to the RFC 3567 server, and the **Profile Status** column indicates whether the server is predefined. User-defined servers will not have an entry in the **Profile Status** column.

```
(host) #show aaa rfc-3567-server

RFC 3576 Server List
--------------------
Name       References  Profile Status
----       ----------  --------------
10.2.14.6  2
```

To view details for a specific server, include the IP address of that server in the command.

```
(host)  #show aaa rfc-3576-server 192.0.2.31
RFC 3576 Server "192.0.2.31"
---------------------------
Parameter  Value
---------  -----
Key        ********
```

To view information for all RFC 3576 servers, include the **statistics** parameter.

```
(host) #show aaa rfc-3576-server statistics

RADIUS RFC 3576 Statistics
--------------------------
Statistics           10.1.2.3  10.1.2.34
----------           --------  ---------
Disconnect Requests  13         3
Disconnect Accepts   12         3
```

```
Disconnect Rejects    1           0
No Secret             0           0
No Session ID         0           0
Bad Authenticator     0           0
Invalid Request       0           0
Packets Dropped       0           2
Unknown service       0           0
CoA Requests          1           0
CoA Accepts           1           0
CoA Rejects           0           0
No permission         0           0

Packets received from unknown clients: 0
Packets received with unknown request: 0
Total RFC3576 packets Received       : 0
```

The output of the **show aaa rfc-3576-server statistics** command includes the following parameters:

Parameter	Description
Disconnect Requests	Number of disconnect requests sent by the server.
Disconnect Accepts	Number of disconnect requests sent by the server that were accepted by the user.
Disconnect Rejects	Number of disconnect requests sent by the server that were rejected by the user.
No Secret	Number of authentication requests that did not contain a RADIUS secret.
No Session ID	Number of authentication requests that did not contain a session ID.
Bad Authenticator	Number of authentication requests that contained a missing or invalid authenticator field in the packet.
Invalid Request	Number of invalid requests.
Packets Dropped	Number of packets dropped.
Unknown service	Number of requests for an unknown service type.
CoA Requests	Number of requests for a Change of Authorization (CoA).
CoA Accepts	Number of times a CoA request was accepted.
CoA Rejects	Number of times a CoA request was rejected.
No permission	Number of requests for a service that has been defined, but has not been administratively enabled.

Related Commands

Command	Description	Mode
aaa rfc-3576-server	Define RFC 3576 server profiles.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa server-group

```
show aaa server-group [<group-name>|summary]
```

Description

Show configuration details for your AAA server groups.

Syntax

Parameter	Description
<group-name>	The name of an existing AAA server group.

Usage Guidelines

Issue this command without the ><**group-name** or**summary** options to display the entire server group list, including profile status and the number of references to each profile. The **References** column lists the number of other profiles that reference a server group, and the **Profile Status** column indicates whether the server group is predefined. User-defined server groups will not have an entry in the Profile Status column. Examples

This first example shows that there are five configured server groups

```
(host) #show aaa server-group summary

Server Group List
-----------------
Name                      References  Profile Status
----                      ----------  --------------
auth-profile-2            1
coltrane-server-group     1
default                   25
group1                    0
internal                  0           Predefined

Total:5
```

To view additional statistics for all server groups, include the **statistics** parameter.

```
(host) #show aaa server-group summary
Server Groups
-------------
Name                      Servers  Rules  hits  Out-of-service
----                      -------  -----  ----  --------------
auth-profile-2            1        0      0
coltrane-server-group     1        0      0
default                   1        0      0
group1                    1        1      0
internal                  1        1      0
```

The output of the show aaa server-group summary command includes the following parameters:

Parameter	Description
name	Name of an existing AAA server group.
Servers	Number of servers in the group.
Rules	Number of rules configured for the server group.
hits	Number of hits for the server's rules.
Out-of-Service	Indicates whether the server is active, or out of service. Active servers may not have an entry in the Out-of-Service column.

To display detailed authorization, role and vlan statistics for an individual server group, include the name of the group for which you want more information.

```
(host) #show aaa server-group summary group1

Fail Through:No

Auth Servers
------------
Name      Server-Type  trim-FQDN  Match-Type  Match-Op  Match-Str
----      -----------  ---------  ----------  --------  ---------
rad1      Radius       No
rad3      Radius       No

Role/VLAN derivation rules
--------------------------
Priority  Attribute  Operation  Operand  Action    Value
--------  ---------  ---------  -------  ------    -----
1                      class      contains   admin    set role          root
```

The output of the show aaa server-group <group-name> command includes the following parameters:

Parameter	Description
Name	Specifies if the server is in service or out-of-service.
Server-Type	If enabled, user information in an authentication request is edited before the request is sent to the server.
trim-FDQN	If enabled, user information in an authentication request is edited before the request is sent to the server.
Match-Type	If the match type is **authstring** he authentication server associates with a match rule that the controller can compare with the user/client information in the authentication request. A **fdqn** match type associates the authentication server with a specified domain. An authentication request is sent to the server only if there is an exact match between the specified domain and the <domain> portion of the user information sent in the authentication request.

Parameter	Description
Match-Op	This is the match method by which the string in **Match-Str** is matched with the attribute value returned by the authentication server. ■ **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. ■ **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. ■ **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. ■ **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. ■ **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. ■ **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied
Match-Str	This is the string to which the value of the returned attribute is matched.
Priority	The priority in which role or VLAN derivation rules are applied. Rules at the top of the list are applied before rules at the bottom.
Attribute	For role or VLAN derivation rules, this is the attribute returned by the authentication server that is examined for **Operation** and **Operand** match.
Operation	For role or VLAN derivation rules, this is the match method by which the string in **Operand** is matched with the attribute value returned by the authentication server. ■ **contains** – The rule is applied if and only if the attribute value contains the string in parameter **Operand**. ■ **starts-with** – The rule is applied if and only if the attribute value returned starts with the string in parameter **Operand**. ■ **ends-with** – The rule is applied if and only if the attribute value returned ends with the string in parameter **Operand**. ■ **equals** – The rule is applied if and only if the attribute value returned equals the string in parameter **Operand**. ■ **not-equals** – The rule is applied if and only if the attribute value returned is not equal to the string in parameter **Operand**. ■ **value-of** – This is a special condition. What this implies is that the role or VLAN is set to the value of the attribute returned. For this to be successful, the role and the VLAN ID returned as the value of the attribute selected must be already configured on the controller when the rule is applied.
Operand	For role or VLAN derivation rules, this is the string to which the value of the returned attribute is matched.
Action	This parameter identifies whether the derivation rule sets a server group role (**set role**) or a VLAN (**set vlan**).
Value	Sets the user role or VLAN ID to be assigned to the client if the rule condition is met.

Related Commands

Command	Description	Mode
aaa server-group	Use aaa server-group to configure the settings displayed in the output of this show command.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state ap-group

```
show aaa state ap-group
```

Description

Show the names and ID numbers of your AP groups

Example

This first example shows that the selected controller has two defined AP groups.

```
(host) #show aaa state ap-group

AP Group Table
--------------
Name  ID
----  --
ap1             1
ap2             2
```

Related Commands

Command	Description	Mode
aaa server-group	Use aaa server-group to define the AP groups displayed in the output of this show command	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state configuration

```
show aaa state configuration
```

Description

Display authentication state configuration information, including the numbers of successful and failed authentications.

Example

This example shows authentication settings and values for a controller with no current users.

```
(host) #show aaa state configuration

Authentication State
--------------------
Name                            Value
----                            -----
Switch IP                       10.6.2.253
Switch IPv6
Master IP                       10.100.103.253
Switch Role                     local
Current/Max/Total IPv4 Users    0/6/14
Current/Max/Total IPv6 Users    0/1/1
Current/Max/Total User Entries  0/4/15
Current/Max/Total Stations      121/190/367550
Captive Portal Users            4
802.1X Users                    119
VPN Users                       0
MAC Users                        0
Stateful 802.1X Users           0
Tunneled users                   0
Configured user roles            21
Configured session ACL          41
Configured destinations         32
Configured services              77
Configured Auth servers         9
Auth server in service          9
Radius server timeouts          7062

Successful authentications
--------------------------
Web  MAC  VPN  802.1X  Krb  RadAcct  SecureID  Stateful-802.1X  Management
---  ---  ---  ------  ---  -------  --------  ---------------  ----------
138  0    0    10117   0    0        0         0                0

Failed authentications
----------------------
Web  MAC  VPN  802.1X  Krb  RadAcct  SecureID  Stateful-802.1X  Management
---  ---  ---  ------  ---  -------  --------  ---------------  ----------
48   0    0    32235   0    0        0         0                0

Idled users              = 3366
Mobility                 = Enabled
fast age                 = Disabled
per-user log             = Disabled
Bandwidth contracts       = 2/1
IP takeovers             = 21
```

```
Ping/SYN/Session attacks = 0/0/0
```

The output of the **show aaa state configuration** command includes the following parameters:

Parameter	Description
Switch IP	IP address of the managed device.
Master IP	IP address of Mobility Master.
Switch Role	Role assigned to the device.
Current/Max/Total IPv4 Users	Current number of IPv4 users on the managed device/Maximum number of IPv4 users that can be assigned to the managed device at any time/Total number of IPv4 users that have been assigned to the managed device since the last managed device reboot.
Current/Max/Total IPv6 Users	Current number of IPv6 users on the managed device/Maximum number of IPv6 users that can be assigned to the managed device at any time/Total number of IPv6 users that have been assigned to the managed device since the last managed device reboot.
Current/Max/Total Users	Current number of users on the managed device/Maximum number of users that can be assigned to the managed device at any time/Total number of users that have been assigned to the managed device since the last managed device reboot.
Current/Max/Total Stations	Current number of stations registered with the controller/Maximum number of stations that can be registered with the controller at any time/Total number of stations that have registered the controller since the last controller reboot.
Captive Portal Users	Number of current users authenticated via captive portal.
802.1X Users	Number of current users authenticated via 802.1X authentication.
VPN Users	Number of current users authenticated via VPN authentication.
MAC Users	Number of current users authenticated via MAC authentication.
Stateful 802.1X Users	Number of current users authenticated via stateful 802.1X authentication.
Tunneled users	Number of stations in tunneled forwarding mode, where 802.11 frames are tunneled to the managed device using generic routing encapsulation (GRE).
Configured user roles	Number of configured user roles.
Configured session ACL	Number of configured session ACLs.
Configured destinations	Number of destinations configured using the netdestination command.
Configured services	Number of service aliases configured using the netservice command.
Configured Auth servers	Number of configured authentication servers.
Auth server in service	Number of authentication servers currently in service.

Parameter	Description
Radius server timeouts	Number of times the RADIUS server did not respond to the authentication request.
Web	Total number of captive portal authentications or authentication failures since the last managed device reset.
MAC	Total number of MAC authentications or authentication failures since the last managed device reset.
VPN	Total number of VPN authentications or authentication failures since the last managed device reset.
802.1X	Total number of 802.1X authentications or authentication failures since the last managed device reset.
Krb	Total number of Kerberos authentications or authentication failures since the last managed device reset.
RadAcct	Total number of RADIUS accounting verifications or accounting failures since the last managed device reset.
SecureID	Number of authentication verifications or failures using methods which use one-time passwords. (For example, EAP-GTC being used as the inner EAP protocol of EAP-PEAP.)
Stateful-802.1X	Total number of Stateful 802.1X authentications or authentication failures since the last managed device reset.
Management	Total number of Management user authentications or authentication failures since the last managed device reset.
Idled users	Total number of users that are not broadcasting data to an AP.
Mobility	Shows whether the IP mobility feature has been enabled or disabled on the managed device.
Fast age	This parameter shows if fast aging of user table entries has been enabled or disabled. When this feature is enabled, if a device comes up on the network with a different IP address, the device's old IP address is immediately deleted. If the user fast-age feature is not configured, the controller retains up to two IPv4 and two IPv6 addresses per device , and these IPs are aged out only when the device becomes inactive.
Per-User Log	Shows if the managed device collects per-user log files for debugging. **NOTE:** This option is enabled using the **aaa log** command.
Bandwidth contracts	Number of configured bandwidth contracts on the managed device.
IP takeovers	Number of times a two different stations have attempted to use the same IP address (IP spoofing).
Ping/SYN/Session attacks	Number of reported ping, SYN and session attacks.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state debug-statistics

```
show aaa state debug statistics
```

Description

show debug statistics for controller authentication, authorization and accounting.

Syntax

No parameters.

Example

The following example displays debug statistics for a variety of authentication errors:

```
(host) #show aaa state debug-statistics
user miss: ARP=47, 8021Q=5216, non-IP=0, zero-IP=0, loopback=0
user miss: mac mismatch=0, spoof=269 (74), drop=390, ncfg=0
user miss: non-auth opcode=0, no-l2-user=0, l2tp=0, vrrp=0, special mac=0, iap l3 user=0
Idled users = 3376
Idled users due to MAC mismatch = 0
Idled users due to SOS: wireless tunnel=0 wireless dtunnel=0
Idled users due to SOS: wired tunnel=0 wired dtunnel=0
Idled users due to SOS: other=0
Idled users due STM deauth: tunnel=0 dtunnel=0
Idled users from STM timeout: tunnel=0 dtunnel=0
Idled users from STM: other=0
Current users with STM idle flag = 0
Idle messages: SOS=0 STM deauth=0 STM timeout=0
Logon lifetime iterations = 4501, entries deleted = 121
SIP authentication messages received 29227, dropped 29227
Missing auth user deletes: 0
Captive-portal forced user deletes: 1
Mobility Stats
         INTRA_MS 0, MAC mismatch 0, HA mismatch 0
         INTER_MS 0, MAC mismatch 0, HA mismatch 0
         MIP Update   0, Move 0, Del 0, TunAcl 0
         AAA Done 0, Del 2
         IPIP Loop forced Del: 0, Validate Visitor 0
Auth User rejects Received
L2 User:0, IPV4 :0, IPV6:0
Auth User rejects Processed
L2 User:0, IPV4 :0, IPV6:0
```

The output of this command includes the following parameters:

Parameter	Description
User Miss	
ARP	Number of ARP packets sent between the datapath and the controlpath.
8021q	Number of 802.1q (VLAN tag) packets sent between the datapath and the controlpath.

Parameter	Description
non-ip	Number of non-IP type packets sent between the datapath and the controlpath.
zero-ip	Number of packets sent without an internet protocol (IP).
loopback	If **1**, the controller has a defined loopback address. If **0**, a loopback address has not yet been configured.
mac mismatch	Number of users that were not authenticated due to MAC mismatches.
spoof	Number of users that were not authenticated due to spoofed IP addresses.
drop	Number of user authentication attempts that were dropped.
ncfg	Number of packets sent between datapath and controlpath, where the authentication module has not completed the initialization required to process the traffic.
Non-auth opcode	Number of packets whose opcode is non-auth opcode. This is a check to find if auth is responsible for processing received packet.
No-l2-user	Number of user packets dropped due to absence ofan L2 entry for the user.
l2tp	Number of l2tp users.
vrrp	Number of VRRP users.
special mac	Number of users with a special MAC address.
iap	Number of instant AP users.
idled users	Number of inactive stations that are not broadcasting data to an AP.
idled users due to MAC mismatch	For internal use only.
Idled users due to SOS	
wireless tunnel	Number of wireless users in tunnel forwarding mode that were aged out by the controller.
wireless dtunnel	Number of wireless users in decrypt tunnel forwarding mode that were aged out by the controller.
wired tunnel	Number of wired users in tunnel forwarding mode that were aged out by the controller.
wired dtunnel	Number of wired users in decrypt tunnel forwarding mode that were aged out by the controller.
Other	Number of users using modes other than tunneled or Decrypt tunneled aged out by the controller.
Idled users due STM deauth	
tunnel	Number of users in tunnel forwarding mode that aged out after STM deauthentication, and timer expiration.

Parameter	Description
dtunnel	Number of users in decrypt tunnel forwarding mode that aged out after STM deauthentication, and timer expiration.
Idled users from STM timeout	
tunnel	Number of users in tunnel forwarding mode that aged out after the STM timer expired.
dtunnel	Number of users in decrypt tunnel forwarding mode that aged out after the STM timer expired.
Idled users from STM	
other	Number of users in fowarding modes other than decrypt tunnel or tunnel mode that aged out after the STM timer expired.
Logon lifetime iteration	Number of users deleted for lack of activity.
SIP authentication message	Number of session initiation protocol (SIP) authentication messages received.
Missing auth user deletes	Number of users removed from the datapath by the auth module, even without a mapping entry in control path. This counter can help identify problems with messages sent between the controlpath and the datapath.
Mobility Stats	Number of different messages exchanged between the mobile IP and the auth module. **NOTE:** This is used for troubleshooting purposes only.
Captive-portal forced user deletes	Number of idle users deleted after captive portal authentication.
Auth User Rejects Received	
L2 User	Number of authentication rejects received for L2 users from the datapath due to a failure of the operation.
IPv4	Number of authentication rejects received for IPv4 users from the datapath due to a failure of the operation.
IPv6	Number of authentication rejects received for IPv6 users from the datapath due to a failure of the operation.
Auth User Rejects Processed	
L2 User	Number of authentication rejects for L2 users that were processed after the reject was received.
IPv4	Number of authentication rejects for IPv4 users that were processed after the reject was received.
IPv6	Number of authentication rejects for IPv6 users that were processed after the reject was received.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state log

```
show aaa state log [info]
```

Description

Display global log files for AAA events.

Syntax

Parameter	Description
`info`	This parameter displays debugging information for internal use only.

Usage Guidelines

If you have enabled per-user logging using the aaa log command, the output of this command displays global AAA log files for events that are not triggered by individual user authentication, such as AP authentication and the initial pre-authentication processes that occur before a client authenticates to the controller.

To display log files for events triggered by a specific user, use the command **show user** or **show ipv6 user-table ip <ipv6-addr> log**.

Example

The example below shows a partial list of the global log files displayed by the **show aaa state log** command..

```
(host) #show aaa state log
   1: At Thu Apr 11 10:41:27:  [L] Type cert-downloaded        * id 0 len 0, bssid
   00:00:00:00:00:00 | mac: 00:00:00:00:00:00
   2: At Thu Apr 11 10:43:17:  [L] Type ap-up                  * id 0 len 0, bssid
   6c:f3:7f:5f:2c:b0 | mac: 00:00:00:00:00:00
   3: At Thu Apr 11 10:43:17:  [L] Type ap-up                  * id 0 len 0, bssid
   6c:f3:7f:5f:2c:a0 | mac: 00:00:00:00:00:00
   4: At Thu Apr 11 10:43:50:  [L] Type station-term-start     * id 10 len 0, bssid
   6c:f3:7f:5f:2c:a0 | mac: 50:a4:c8:bd:be:41
   5: At Thu Apr 11 10:43:50:  [L] Type station-data-ready_ack * id 10 len 0, bssid
   00:00:00:00:00:00 | mac: 50:a4:c8:bd:be:41
```

Related Commands

Parameter	Description
aaa log	Issue this command to enable per-user logging.
show user show ipv6 user-table	Display log files for authentication events triggered by a specific IPv4 or IPV6 user.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state messages

Description

Display numbers of authentication messages sent and received.

Syntax

No parameters.

Usage Guidelines

This command displays a general overview of authentication statistics. To view authentication information for specific profiles such as a captive-portal, MAC or 801.x authentication profile, issue the commands specific to those features.

Example

The output of this command displays tables of statistics for PAPI, RAW socket and Sibyte messages.

```
(host) #show aaa state messages
PAPI Messages
-------------
Msg ID  Name                    Since last Read  Total
------  ----                    ---------------  -----
5004    set master ip           2                2
7005    Set switch ip           1                1
7007    Set VLAN ip             5                5
66      delete xauth vpn users  1                1

RAW socket Messages
-------------------
Msg ID  Name                        Since last Read  Total
------  ----                        ---------------  -----
1       raw PAP req                 188              188
33      captive portal config       11113            11113
59      TACACS ACCT config for cli  1                1
60      TACACS ACCT config for web  1                1

Sibyte Messages
---------------
Opcode  Name        Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----        --------------------  ----------  --------------------  ----------
2       bridge      21                    21          0                     0
4       session     4877                  4877        0                     0
11      ping        768                   768         768                   768
13      8021x       114563                114563      229126                229126
15      acl         803                   803         0                     0
16      ace         5519                  5519        0                     0
17      user        781821                781821      0                     0
27      bwm         3                     3           0                     0
29      wkey        27109                 27109       4                     4
42      nat         1                     1           0                     0
43      user tmout  4164                  4164        4160                  4160
56      forw unenc  1787103               1787103     0                     0
64      auth        5268                  5268        5267                  5267
94      aesccm key  17885                 17885       0                     0
111     dot1x term  196813                196813      151161                151161
```

```
114     rand        1614                1614        1612                1612
126     eapkey      1316231             1316231     2632462             2632462

114     rand        2                   2           0                   0
```

The output of this command contains the following parameters:

Parameter	Description
`Msg ID`	ID number for the message type.
`Name`	Message name.
`Since last Read`	Number of messages received since the buffer was last read.
`Total`	Total number of message received since the controller was last reset.
`opcode`	Code number of the message type.
`Sent Since last Read`	Number of messages sent since the buffer was last read.
`Sent Total`	Total number of message sent since the controller was last reset.
`Recv Since last Read`	Number of messages received since the buffer was last read.
`Recv Total`	Total number of message received since the controller was last reset.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state mux-tunnel

Description

Show multiplexter (MUX) tunnel IDs.

Syntax

No parameters.

Example

The example below shows statistics for one MUX tunnel

```
(host) #show aaa state mux-tunnel
Mux Tunnel Information
----------------------
      IP            Tunnel ID     Slot/Port  AP Type  AP Name
---------------  ---------------  ---------  -------  ------
10.2.1.26                                                    1
                         125                                 AP16
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of a multiplexer (MUX) server
Tunnel ID	ID number of a MUX tunnel.
Slot/Port	The slot and port used by the controller, in the format <slot>/<module>/<port>
AP Type	AP model type.
AP Name	Name of an AP.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state station

```
show aaa state station <A:B:C:D:E:F>
```

Description

Display AAA statistics for a station.

Syntax

Parameter	Description
<A:B:C:D:E:F>	MAC address of a station.

Example

The example below shows statistics for a station with four associated user IP addresses. The output of this command shows station data, the AAA profiles assigned to the station, and the station's authentication method.

```
(host) #show aaa state station 00:21:5c:85:d0:4b
Association count = 1, User count = 4
User list = 10.1.10.10 10.6.5.168 192.168.229.1 192.168.244.1
essid: ethersphere-wpa2, bssid: 00:1a:1e:8d:5b:31 AP name/group: AL40/corp1344 PHY: a,
ingress=0x10e8 (tunnel 136)
vlan default: 65, assigned: 0, current: 65 cached: 0, user derived: 0, vlan-how: 0
name: MYCOMPANY\tgonzales, role:employee (default:logon, cached:employee, dot1x:), role-how:
1, acl:51/0, age: 00:02:50
Authentication: Yes, status: successful, method: 802.1X, protocol: EAP-MD5, server: vortex
dot1xctx:1 sap:1
Flags: mba=0
AAA prof: default-corp1344, Auth dot1x prof: default, AAA mac prof:, def role: logon
ncfg flags udr 1, mac 0, dot1x 1
Born: 1233767066 (Wed Feb  4 09:04:26 2009
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa state tunneled-node

```
show aaa state tunneled-node
```

Description

This command shows tunnels originating from the tunnel nodes.

Syntax

No parameters.

Usage Guidelines

This command shows tunnels originating from the tunnel nodes.

Example

The following example shows tunnels originating from the tunnel nodes:

```
(host) [mynode] #show aaa state tunneled-node

Tunnel Information
------------------
      IP            Tunnel ID     Port  AP Type  AP Name
---------------  ---------------  ----  -------  -------
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show aaa state user

```
show aaa state user <A.B.C.D>
```

Description

Display statistics for an authenticated user.

Syntax

Parameter	Description
<A.B.C.D>	IP address of a user.

Example

The example below shows statics for a user with the IP address 10.1.10.11. The output of this command shows user data, the user's authentication method. and statistics for assigned roles, timers and flags.

```
(host) #show aaa state user 10.1.10.11
Name: MYCOMPANY\tsenter, IP: 10.1.10.11, MAC: 00:21:5c:85:d0:4a, Role:employee, ACL:51/0, Age:
00:01:46
Authentication: Yes, status: successful, method: 802.1X, protocol: EAP-MD5, server: vortex
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: Default
VLAN Derivation: Matched user rule
Idle timeouts: 0, ICMP requests sent: 0, replies received: 0, Valid ARP: 0
Mobility state: Associated, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 L3 Mob: 0
Flags: internal=0, trusted_ap=0, delete=0, l3auth=0, l2=1 mba=0
Flags: innerip=0, outerip=0, guest=0, station=0, download=1, nodatapath=0
Auth fails: 0, phy_type: a-HT, reauth: 0, BW Contract: up:0 down:0, user-how: 1
Vlan default: 65, Assigned: 0, Current: 65 vlan-how: 0
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, ProxyArp=0, Flags=0x0
Tunnel=0, SlotPort=0x1018, Port=0x10e2 (tunnel 130)
Role assigned: n/a, VPN: n/a, Dot1x:  Name: employee role-how: 0
Essid: ethersphere-wpa2, Bssid: 00:1a:1e:11:6b:91 AP name/group: AL31/corp1344 Phy-type: a-HT
RadAcct sessionID:n/a
RadAcct Traffic In 0/0 Out 0/0 (0:0/0:0:0:0,0:0/0:0:0:0)
Timers: arp_reply 0, spoof reply 0, reauth 0
Profiles AAA:default-corp1344, dot1x:default, mac: CP: def-role:'logon' sip-role:''
ncfg flags udr 0, mac 0, dot1x 0
Born: 1233772328 (Wed Feb  4 10:32:08 2009)
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa tacacs-accounting

Description

Show TACACS accounting configuration.

Syntax

No parameters.

Example

The example below shows that TACACS accounting has been enabled, and that the TACACS server is in the server group acct-server.

```
(host) #show aaa tacacs-accounting
TACACS Accounting Configuration
-------------------------------
Parameter      Value
---------      -----
Mode           Enabled
Server-Group   acct-server
```

The output of this command includes the following parameters:

Parameter	Description
Mode	Shows if the TACACS accounting feature is enabled or disable
Server-Group	The server group that contains the active TACACS server.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa timers

Description

Show AAA timer values.

Syntax

No parameters

Example

The example below shows that the controller has all default timer values:

```
(host) #show aaa timers
User idle timeout = 6 minutes
Auth Server dead time = 10 minutes
Logon user lifetime = 5 minutes
```

Related Commands

Command	Description	Mode
aaa timers	Use aaa timers to define the settings displayed in the output of this show command.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa web admin-port

```
show aaa web admin-port
```

Description

Show the port numbers of HTTP and HTTPS ports used for web administration.

Syntax

No parameters.

Example

The example below shows that the controller is configured to use HTTPS on port 4343 or 443, and HTTP on port 8888.

```
(host) #show aaa web admin-port
https port = 4343
http  port = 8888
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa xml-api server

```
show aaa xml-api server [<server_ip>]
```

Description

Show a list of XML servers used for authentication, authorization, and accounting.

Syntax

Parameter	Description
`<server_ip>`	IP address of an XML API server. Include this parameter to see if a secret key is configured for the specified server.

Example

The output of this command shows that the Mobility Master has two configured XML API servers that are each referenced by two different AAA profiles. Note that user-defined servers will not have an entry in the **Profile Status** column.

```
(host) #show aaa xml-api statistics
XML API Server List
-------------------
Name       References  Profile Status
----       ----------  --------------
10.1.2.3   2
10.4.3.2   2
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show aaa xml-api statistics

```
show aaa xml-api statistics
```

Description

Display statistics for an external XML API server.

Syntax

Parameter	Description
`<server_ip>`	IP address of XML API server.

Usage Guidelines

Issue this command to troubleshoot AAA problems and monitor usage on an XML server.

Example

The example below shows AAA statistics for an external XML server with the IP address 10.1.2.3. This command shows the number of times that a particular event has occurred per client. The first number is the number of times this event occurred. The number of new events since the last time the counters were displayed is shown in parentheses.

```
(host) #show aaa xml-api statistics
Statistics                              10.1.2.3
----------                              --------
user_authenticate                       0 (0)
user_add                                0 (0)
user_delete                             0 (0)
user_blacklist                          0 (0)
user_query                              0 (0)
unknown user                            0 (0)
unknown role                            0 (0)
unknown external agent                  0 (0)
authentication failed                   0 (0)
invalid command                         0 (0)
invalid message authentication method   0 (0)
invalid message digest                  0 (0)
missing message authentication          0 (0)
missing or invalid version number       0 (0)
internal error                          0 (0)
client not authorized                   0 (0)
Cant use VLAN IP                        0 (0)
Invalid IP                              0 (0)
Cant use Switch IP                      0 (0)
missing MAC address                     0 (0)
Packets received from unknown clients:  0 (0)
Packets received with unknown request:  0 (0)
Requests Received/Success/Failed    :    0/0/0 (0/0/0)
```

The output of this command includes the following parameters:

Parameter	Description
user_authenticate	Number of users authenticated on the XML server since the last controller reboot.
user_add	Number of users added to the controller's user table.
user_delete	Number of users removed from the controller's user table.
user_blacklist	Number of denied user association requests.
user_query	Number of user queries performed.
unknown user	Number of unknown users.
unknown role	Number of unknown user roles.
unknown external agent	Number of requests by an unknown external agent.
authentication failed	Number of failed authentication requests.
invalid command	Number of invalid XML commands
invalid message authentication method	Number of XML commands with an invalid authentication method (when a key is configured on the controller).
invalid message digest	Number of XML commands with an invalid digest type (when a key is configured on the controller).
missing message authentication	Number of XML commands with an missing authentication method (when a key is configured on the controller).
missing or invalid version number	**Number of commands with a missing or invalid version number. The version number should always be 1.0.**
internal error	Number of internal server errors
client not authorized	Number of unauthorized clients
Cant use VLAN IP	Number of time a user IP is same as the VLAN IP.
Invalid IP	Number of XML commands with an invalid IP address.
Cant use Switch IP	Redirection to a IP failed, possibly because the source IP has been NATted.
missing MAC address	Number of XML commands with a missing MAC address.
Packets received from unknown clients	Number of packets received from unknown clients.
Packets received with unknown request	Number of packets received with unknown request
Requests Received/Success/ Failed	Total number of requests received / number of successful requests / number of failed requests

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show acl ace-table

```
show acl ace-table {ace <0-7680>}|{acl <1-2699>}|{all}
```

Description

Show an access list entry (ACE) table for an ACL.

Syntax

Parameter	Description
`ace <0-7680>`	Shows a single ACE entry.
`acl <1-2699>`	Shows all ACE entries for a single ACL.
`all`	Shows all ACE entries.

Example

The following example shows that there are eighteen access control entries for ACL 1.

```
(host) #show acl ace-table acl 1
  1020: any any  1  0-65535  0-65535  f80001:permit
  1021: any any  17  0-65535  53-53  f80001:permit
  1022: any any  17  0-65535  8211-8211  f80001:permit
  1023: any any  17  0-65535  8200-8200  f80001:permit
  1024: any any  17  0-65535  69-69  f80001:permit
  1025: any any  17  0-65535  67-68  f80001:permit
  1026: any any  17  0-65535  137-137  f80001:permit
  1027: any any  17  0-65535  138-138  f80001:permit
  1028: any any  17  0-65535  123-123  f80001:permit
  1029: user 10.6.2.253 255.255.255.255  6  0-65535  443-443  f80001:permit
  1030: user any  6  0-65535  80-80  d1f90,0000 f80021:permit dnat
  1031: user any  6  0-65535  443-443  d1f91,0000 f80021:permit dnat
  1032: any any  17  0-65535  500-500  f80001:permit
  1033: any any  50  0-65535  0-65535  f80001:permit
  1034: any any  17  0-65535  1701-1701  f80001:permit
  1035: any any  6  0-65535  1723-1723  f80001:permit
  1036: any any  47  0-65535  0-65535  f80001:permit
  1037: any any  0  0-0  0-0  f180000:deny
```

Related Commands

Configure ACLs using the command ip access-list session.

Command History

Release	Modification
ArubaOS 8.2.0.0	The new range for **ace** and **acl** were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Master.

show acl acl-table

```
show acl acl-table <1-2700>
```

Description

Display information for a specified ACL.

Syntax

Parameter	Description
`acl-table <1-2700>`	Specify the number of the ACL for which you want to view information.

Example

The following example displays the ACL table for the controller.

```
(host) #show acl acl-table acl 1

AclTable
--------
ACL  Type  ACE Index  Ace Count  Name   Applied
---  ----  ---------  ---------  ----   -------
1    role  1459       18         logon  0

Total free ACE entries = 3591
Free ACE entries at the bottom = 2552
Next ACE entry to use = 1480 (table 1)
Ace entries reused 622 times
ACL count 64, tunnel acl 0

Ace entries reused 373 times
```

ACL count 64, tunnel acl 0

The output of this command displays the following parameters:

Parameter	Description
ACL	Number of the specified ACL
Type	Shows the ACL type: ■ **role**: Access list is used to define a user role. ■ **mac**: MAC ACLs allow filtering of non-IP traffic. This ACL filters on a specific source MAC address or range of MAC addresses. ■ **session**: Session ACLs define traffic and firewall policies on the controller. ■ **ether-type**: This type of ACL filters on the Ethertype field in the Ethernet frame header, and is useful when filtering non-IP traffic on a physical port. ■ **standard**: Standard ACLs are supported for compatibility with router software from other vendors. This ACL permits or denies traffic based on the source address of the packet.
ACE Index	Starting index entry for the ACL's access control entries

Parameter	Description
ACE count	Number of access control entries in the ACL
Name	Name of the ACL.
Applied	Number of times the ACL was applied to a role.
Total free ACE entries	The total number of free ACE entries. This includes available ACE entries at the bottom of the list, as well as free ACE entries in the middle of the table from previous access list entries that were later removed.
Free ACE entries at the bottom	The total number of free ACE entries at the bottom of the list.
Next ACE entry to use	Ace number of the first free entry at the bottom of the list.
ACE entries reused	For internal use only.
ACL count	Total number of defined ACLs
Tunnel ACL	Total number of defined tunnel ACLs.

The following example displays the ACL table for ACL 1.

```
(host) #show acl ace-table acl 1
Acl Table
--------
ACL  Type  ACE Index  Ace Count  Name   Applied
---  ----  ---------  ---------  ----   -------
1    role  1020       18         logon  0

Total free ACE entries = 3591
Free ACE entries at the bottom = 2991
Next ACE entry to use = 1041 (table 1)
Ace entries reused 373 times
```

ACL count 64, tunnel acl 0

Related Commands

Configure ACLs using the command ip access-list session.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show acl hits

```
show acl hits
```

Description

Show internal ACL hit counters.

Syntax

No parameters.

Usage Guidelines

Issue this command to see the number of times an ACL defined a user's role, or traffic and firewall policies for a user session.

Example

In the example below, the output of the *User Role ACL Hits* table is shown in two separate tables to allow the output to fit on a single page of this document. In the actual controller CLI, the *User Role ACL Hits* table is shown in a single, wide table.

```
(host) #show acl ace-table acl 1
User Role ACL Hits
------------------
Role            Policy               Src          Dst
----            ------               ---          ---
logon           control              any          any
logon           control              any          any
logon                                any          any
visitor         vp-control           any          any
visitor         vp-control           any          any
visitor         vp-access            any          any
visitor         vp-access            user         mswitch-master
visitor         vp-access            any          any

User Role ACL Hits------------------
Service       Action   Dest/Opcode  New Hits  Total Hits  Index
-------       ------   -----------  --------  ----------  -----
svc-icmp      permit                0         6           5052
svc-dhcp      permit                0         2           5057
0             deny                  0         53          5069
svc-dns       permit                9         46079       4885
svc-dhcp      permit                0         788         4886
svc-icmp      permit                0         536         4887
svc-http      permit                0         41          4889
6 9100-9100   permit                0         31          4892
Port Based Session ACL
----------------------
Policy     Src                    Dst  Service  Action  Dest/Opcode  New Hits  Total Hits
Index
------     ---                    ---  -------  ------  -----------  --------  ----------  --
---
validuser  10.1.1.0 255.255.255.0 any  any      deny                0         214
4655
validuser  any                    any  any      permit              6         2502
4656

Port ACL Hits
```

```
-------------
ACL  ACE  New Hits  Total Hits  Index
---  ---  --------  ----------  -----
5               22                                                  0
```

The output of this command includes the following information:

Parameter	Description
Role	Name of the role assigned by the ACL.
Policy	Name of the policy used by the ACL
Src	The traffic source, which can be one of the following: ■ <*alias*>: Name of a user-defined alias for a network host, subnetwork, or range of addresses. ■ **any**: match any traffic. ■ **host**: specify a single host IP address. ■ **network**: specify the IP address and netmask. ■ **user**: represents the IP address of the user.
Dst	The traffic destination, which can be one of the following: ■ <*alias*>: Name of a user-defined alias for a network host, subnetwork, or range of addresses. ■ **any**: match any traffic. ■ **host**: specify a single host IP address. ■ **network**: specify the IP address and netmask. ■ **user**: represents the IP address of the user.
Service	Network service, which can be one of the following: ■ IP protocol number (0-255) ■ name of a network service (use the show netservice command to see configured services) ■ **any**: match any traffic ■ **tcp**: specify the TCP port number (0-65535) ■ **udp**: specify the UDP port number (0-65535)
Action	Action if rule is applied, which can be one of the following: ■ **deny**: reject packets ■ **dst-nat**: perform destination NAT on packets ■ **dual-nat**: perform both source and destination NAT on packets ■ **permit**: forward packets ■ **redirect**: specify the location to which packets are redirected ■ **src-nat**: perform source NAT on packets
Dest/Opcode	The datapath destination ID.
New Hits	Number of ACL hits that occurred since this command was last issued.
Total Hits	Total number of ACL hits recorded since the controller last reset.
Index	Index number of the ACL.
ACL	ACL number
ACE	ACE number
New Hits	Number of times the ACL was applied since this command was last issued.

Parameter	Description
Total Hits	Number of times the ACL was applied since the controller was last reset.
Index	Index number of the ACL.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show activate

```
show activate
```

Description

This command displays the profile that allows a managed device to synchronize its remote AP whitelist with the Aruba Activate cloud-based services.

Syntax

No parameters.

Usage Guidelines

Use this command to view the credentials the managed device uses to synchronize the remote AP whitelist with an Activate server.

Example

The following example displays the Activate whitelist service settings:

```
(host)[node](config)# show activate
  activate
  --------
  Parameter                                Value                                Set
  ---------                                -----                                ---
  Activate Whitelist Service               Enabled
  Activate URL                             https://activate.arubanetworks.com
  Provision Activate URL                   https://device.arubanetworks.com
  Activate Login Username                  ztp
  Activate Login Password                  ********
  Periodic Interval for WhiteList Download 1
  Add-Only Operation                       Enabled
  Custom cert to upload to Activate        N/A
  Server cert to be used for IPSEC         N/A
```

The **Periodic Interval for WhiteList Download** parameter indicates the whitelist download period in days.

Related Commands

Parameter	Description
activate	This command synchronizes the remote AP whitelist on the managed device with the Activate whitelist database.

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or enable mode on Mobility Master.

show adp config

```
show adp config
```

Description

Show Aruba Discovery Protocol (ADP) configuration settings.

Syntax

No parameters.

Example

The following example shows that the managed device has all default settings for ADP.

```
(host)[mynode](config)#show adp config
ADP Configuration
-----------------
key         value
---         -----
discovery   enable
igmp-join   enable
igmp-vlan   0
```

The output of this command includes the following parameters:

Parameter	Description
discovery	Aruba APs send out periodic multicast and broadcast queries to locate Mobility Master. If the APs are in the same broadcast domain as Mobility Master and ADP is enabled on the managed device, the managed device automatically responds to the APs' queries with its IP address. This command shows whether ADP is enabled or disabled on the managed device.
igmp-join	Shows whether the managed device has enabled or disabled the sending of Internet Group Management Protocol (IGMP) join requests.
igmp-vlan	ID of the VLAN to which IGMP reports are sent. If this value is set to 0, the managed device will use the default route VLAN used.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show adp counters

```
show adp counters
```

Description

Show Aruba Discovery Protocol (ADP) counters.

Syntax

No parameters.

Example

The following example shows the ADP counter table for the managed device.

```
(host)[mynode](config) #show adp counters
ADP Counters
------------
key            value
---            -----
IGMP Join Tx   1
IGMP Drop Tx   0
ADP Tx         0
ADP Rx         0
```

The output of this command includes the following parameters:

Parameter	Description
`IGMP Join Tx`	Number of Internet Group Management Protocol (IGMP) join requests sent by the managed device.
`IGMP Drop Tx`	Number of Internet Group Management Protocol (IGMP) drop requests sent by the managed device.
`ADP Tx`	Number of ADP responses sent to APs.
`ADP Rx`	Number of multicast and broadcast queries received from APs trying to locate Mobility Master.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup

```
show airgroup
   active-domains
   aps
   blocked-queries [dlna|mdns]
   blocked-service-id [dlna|mdns]
   cache entries [dlna|mdns|static|verbose]
   cppm [entries|server-group]
   cppm-server {aaa|query-interval|{radius statistics}|{rfc3576 statistics}}
   domain
   effective profiles
   flow-table
   internal-state statistics {dlna|mdns|verbose}
   multi-controller-table {dlna|mdns|verbose}
   policy-entries [mac {neighborhood <macaddr>}|<macaddr>]
   servers {dlna|mdns|verbose}
   status
   switches
   tracebuf [msgs [ip <ipaddr>]|[mac <macaddr>]]|pps]
   users {dlna|mdns|verbose}
   vlan
```

Description

This command shows the global AirGroup settings.

Syntax

Parameter	Description
`active-domains`	Shows list of configured AirGroup active-domains. **NOTE:** This command is not applicable when Mobility Master is a VM.
`aps`	Shows the AP table. **NOTE:** This command is not node specific.
`blocked-queries [dlna|mdns]`	Shows dropped query IDs because the associated service is unavailable. ■ **dlna** - Shows the blocked DLNA queries. ■ **mdns** - Shows the blocked mDNS queries. **NOTE:** This command is not node specific.
`blocked-service-id [dlna|mdns]`	Shows blocked service IDs. ■ **dlna** - Shows the blocked DLNA service IDs. ■ **mdns** - Shows the blocked mDNS service IDs. **NOTE:** This command is not node specific.

`cache entries`
`dlna`
`mdns`
`static`
`verbose`
	Shows DLNA and mDNS cache entries.
	■ **dlna** - Shows the DLNA cache entries.
	■ **mdns** - Shows the mDNS cache entries.
	■ **static** - Shows the static cache entries.
	■ **verbose** - Shows additional details of airgroup cache entries
	NOTE: This command is node specific.

Parameter	Description
`cppm {entries|server-group}`	Shows ClearPass Policy Manager details. ■ **entries**: Shows information for devices registered in ClearPass Policy Manager. This command is not node specific. ■ **server-group**: Shows ClearPass Policy Manager server group information. This command is node specific.

`cppm-server`
`aaa`
`query-interval`
`radius statistics`
`rfc3576 statistics`
	Shows ClearPass Policy Manager server details.
	■ **aaa**: Shows the AAA parameters for AirGroup.
	■ **query-interval**: Shows the query interval used to refresh the ClearPass Policy Manager entries at periodic intervals.
	■ **radius statistics**: Shows the RADIUS statistics. This command is node specific.
	■ **rfc3576 statistics**: Shows the dynamic authorization extensions to RADIUS statistics. This command is node specific.

`domain`	Shows the IP address of participating managed devices.
`effective profiles`	Shows the profiles effective applied at that node. **NOTE:** This command is node specific.
`flow-table`	Shows the flows installed by AirGroup process. **NOTE:** This command is node specific.

`internal-state statistics`
`dlna`
`mdns`
`verbose`
	Shows internal state of AirGroup process.
	■ **dlna** - Shows the DLNA statistics.
	■ **mdns** - Shows the mDNS statistics.
	■ **verbose** - Shows additional details of the statistics.
	NOTE: This command is not node specific.

`multi-controller-table`
`dlna`
`mdns`
`verbose`
	Show the AirGroup cluster information.
	■ **dlna** - Shows DLNA statistics.
	■ **mdns** - Shows mDNS statistics,
	■ **verbose** - Shows additional details of the statistics.
	NOTE: This command is not applicable when Mobility Master is a VM.
	NOTE: This command is supported only on stand-alone controller domain.

`policy-entries mac`
`neighborhood <mac>`
`<mac>`
	Show the active policies.
	■ **neighborhood** - Shows the AP neighborhood to discover the server.
	■ **mac** - Shows active policies filtered by specified MAC address.
	NOTE: This command is not node specific.

`servers`
`dlna`
`mdns`
`verbose`
	Shows the server table.
	■ **dlna** - Shows the DLNA servers.
	■ **mdns** - Shows the mDNS servers.
	■ **verbose** - Shows additional information of the AirGroup servers.
	NOTE: This command is node specific.

Parameter	Description
`status`	Shows the current status of the AirGroup configuration and configured AirGroup services. **NOTE:** This command is node specific.
`switches`	Shows the switch entries. **NOTE:** This command is node specific.

`tracebuf`
`msgs [ip <ipaddr>]|[mac <macaddr>]`
`pps`
	Shows the trace buffer.
	■ **msgs** - Shows the AirGroup trace buffer.
	■ **pps** - Shows the packet arrival trace buffer.
	NOTE: This command is not node specific.

`users`
`dlna`
`mdns`
`verbose`
	Shows user table.
	■ **dlna** - Shows the DLNA users.
	■ **mdns** - Shows the mDNS users.
	■ **verbose** - Shows additional information of users.
	NOTE: This command is node specific.

`vlan`	Shows the status of all the disallowed VLANs. **NOTE:** This command is node specific.

Usage Guidelines

This command shows the global AirGroup settings. For the remaining parameters, see the command syntax.

Example

The following example shows the current status of the AirGroup configuration and configured AirGroup services:

```
(host) [mynode] #show airgroup status

AirGroup Information
--------------------
Feature               Status
-------               ------
MDNS                  Disabled
DLNA                  Enabled
Enforce Registration  Disabled
IPV6                  Enabled

AirGroup Service Information
----------------------------
Service     Status
-------     ------
remotemgmt  Disabled
DIAL        Enabled
AmazonTV    Enabled
DLNA Media  Enabled
test        Enabled
static      Enabled
combined    Enabled
DLNA Print  Disabled
allowall    Enabled
sharing     Disabled
chat        Disabled
Daniel      Enabled
itunes      Disabled
airplay     Enabled
```

```
airprint     Enabled
googlecast   Enabled
```

Related Commands

Command	Description
airgroup	This command configures AirGroup global settings, domain, and active-domain parameters.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup active-domains

```
show airgroup active-domains
```

Description

This command shows the list of configured AirGroup active-domains. This command is applicable only on stand-alone controllers.

Syntax

No parameters.

Usage Guidelines

This command shows the list of configured AirGroup active-mains. This command is applicable only on stand-alone controllers.

Example

The following example shows the list of configured AirGroup active-domains:

```
(host) [mynode] #show airgroup active-domains

AirGroup Active-Domains
-----------------------
Domain Name   Status
-----------   ------
Campus1       Included
Campus2       Included

Num active-domains:2
```

The output of this command includes the following parameters:

Column	Description
`Domain Name`	Shows the name of the domain.
`Status`	Shows the status of the domain if it is part of the active-domain list.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on stand-alone controller

show airgroup aps

```
show airgroup aps
```

Description

This command shows the AP tables.

Syntax

No parameters.

Usage Guidelines

This command shows the AP tables.

Example

The following example shows the AP tables:

```
(host) [mynode] #show airgroup aps

AirGroup APs
------------
IP  Name    Group        MAC               BSSID- A          BSSID- B/G
--  ----    -----        ---               --------          ----------
AP102   apgrp-clust  ac:a3:1e:c7:71:2e  ac:a3:1e:f7:12:f0  ac:a3:1e:f7:12:e0
7010AP  apgrp-clust  ac:a3:1e:ca:7e:04  ac:a3:1e:27:e0:50  ac:a3:1e:27:e0:40

FQLN  Neighbor count- A  Neighbor count- B/G  Neighbor base BSSID  BAND
----  -----------------  ------------------  -------------------  ----
      3                  3                     ac:a3:1e:cf:b9:90    A
                                               ac:a3:1e:27:e0:50    A
                                               40:e3:d6:bf:65:50    A
      3                  2                     ac:a3:1e:cf:b9:90    A
                                               ac:a3:1e:f7:12:f0    A
                                               40:e3:d6:bf:65:50    A

Num APs:3
```

The output of this command includes the following parameters:

Column	Description
IP	Shows the IP address of the AirGroup AP.
Name	Shows the name of the AP.
Group	Shows the group of the AirGroup user.
MAC	Shows the MAC address of the AirGroup AP.
BSSID- A	Shows the BSSID-A of the AirGroup AP
BSSID- B/G	Shows the BSSID-B/G of the AirGroup AP
FQLN	Shows the FQLN of the AirGroup AP.
Neighbor count- A	Shows the neighbor count-A of the AirGroup AP

Column	Description
Neighbor count- B/G	Shows the neighbor count-B/G of the AirGroup AP
Neighbor base BSSID	Shows the neighbor base BSSID of the AirGroup AP
BAND	Shows the band of the AirGroup AP

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup blocked-queries

```
show airgroup blocked-queries [dlna|mdns]
```

Description

This command shows the service ID that was queried but not available in the AirGroup service table.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA blocked queries.	—	—
`mdns`	Shows the mDNS blocked queries.	—	—

Usage Guidelines

This command shows the service ID that was queried but not available in the AirGroup service table. For the remaining parameters, see the command syntax.

Example

The following example displays the service ID that was queried but not available in the AirGroup service table:

```
(host) [mynode] #show airgroup blocked-queries

AirGroup dropped Query IDs
--------------------------
Service ID                                              #query-hits  Thread Num
----------                                              -----------  ----------
urn:schemas-wifialliance-org:device:WFADevice:1         9            1
urn:schemas-upnp-org:device:InternetGatewayDevice:1     485113       1
_appletv._tcp                                           60           2
_sleep-proxy._udp                                       64           2
urn:schemas-wifialliance-org:device:WFADevice:1         672          2
_airport._tcp                                           60           2
_appletv-pair._tcp                                      60           2
_touch-remote._tcp                                      60           2
urn:schemas-upnp-org:device:InternetGatewayDevice:1     90476        2
_appletv._tcp                                           60           3
_sleep-proxy._udp                                       86           3
_airport._tcp                                           146          3
_appletv-pair._tcp                                      60           3
_touch-remote._tcp                                      60           3
urn:schemas-upnp-org:device:InternetGatewayDevice:1     73056        3
urn:schemas-wifialliance-org:device:WFADevice:1         36           4
urn:schemas-upnp-org:device:InternetGatewayDevice:1     93141        4
urn:schemas-wifialliance-org:device:WFADevice:1         12           5
urn:schemas-upnp-org:device:InternetGatewayDevice:1     72176        5
Num dropped Query IDs:19
```

The output of this command includes the following parameters:

Parameter	Description
`Service ID`	Shows the service ID that was queried but not available in the AirGroup service table.
`#query-hits`	Shows the number of query hits for a service blocked by AirGroup.
`Thread Num`	Shows the thread number of the service ID.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup blocked-service-id

```
show airgroup blocked-service-id [dlna|mdns]
```

Description

This command shows the list of blocked services.

Syntax

Parameter	Description	Range	Default
`dlna`	Specifies the DLNA blocked services.	—	—
`mdns`	Specifies the mDNS blocked services.	—	—

Usage Guidelines

This command shows the list of blocked services. For the remaining parameters, see the command syntax.

Example

The following example shows the list of blocked services:

```
(host) [mynode] #show airgroup blocked-service-id

AirGroup Blocked Service IDs
----------------------------
Origin                    Service ID               #response-hits
------                    ----------               --------------
fe80::6203:8ff:fe94:74a6  _sftp-ssh._tcp           82
fe80::6203:8ff:fe94:74a6  _ssh._tcp               82
10.16.124.236             _uscan._tcp              40
10.16.126.248             _keepalive._dns-sd._udp  20
Num Blocked Service-ID:4
```

The output of this command includes the following parameters:

Parameter	Description
`Origin`	Shows the source IP address of the AirGroup server that advertises this service.
`Service ID`	Shows the blocked service ID of the server.
`#response-hits`	Shows the number of response messages received for this service ID.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup cache entries

```
show airgroup cache entries [dlna|mdns|static|verbose]
```

Description

This command shows the AirGroup mDNS and DLNA resource records in cache.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA cache entries.	—	—
`mdns`	Shows the mDNS cache entries.	—	—
`static`	Shows static cache entries.	–	–
`verbose`	Shows details cache entries.	–	–

Usage Guidelines

This command shows the AirGroup mDNS and DLNA resource records in cache. For the remaining parameters, see the command syntax.

Example

The following example shows the AirGroup mDNS resource records in the cache:

```
(host) [mynode] #show airgroup cache entries mnds

Cache Entries
-------------
Name                Type  Class  TTL   Origin   Expiry  Last Update
----                ----  -----  ---   ------   ------  -----------
world_cricket       A     IN     120   0.0.0.0  static  N/A
_icct20._tcp.local  PTR   IN     4500  0.0.0.0  static  N/A
Num Cache Entries:2
```

The output of this command includes the following parameters:

Column	Description
`Name`	Shows the name of the Service ID.
`Type`	Shows the type of mDNS or DLNA record.
`Class`	Shows the class of the record. This is usually IN.
`TTL`	Shows the time to live value of the service ID in seconds.
`Origin`	Shows the source IP of the AirGroup server.
`Expiry`	Shows the expiry period of the mDNS or DLNA record in seconds.
`Last Update`	Shows the time stamp of the last cache update.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup cppm

```
show airgroup cppm [entries|server-group]
```

Description

This command shows information for devices registered in ClearPass Policy Manager.

Syntax

Parameter	Description	Range	Default
`entries`	Shows the ClearPass Policy Manager registration information.	—	—
`server-group`	Shows the Server Group information.	—	—

Usage Guidelines

This command shows information for devices registered in ClearPass Policy Manager. For the remaining parameters, see the command syntax.

Example

The following example shows the information for devices registered in ClearPass Policy Manager:

```
(host) [mynode] #show airgroup cppm entries

ClearPass Guest Device Registration Information
-----------------------------------------------
Device             device-owner  shared location-id AP-name  shared location-id AP-FQLN
------             ------------  --------------------------  --------------------------
cc:3a:61:b1:4a:cc  lecturer
c4:85:08:a2:15:1b  N/A
00:1e:65:2d:ae:44  N/A

shared location-id AP-group  shared user-list  shared group-list  shared role-list  CPPM-Req
CPPM-Resp
---------------------------  ---------------  -----------------  ----------------  --------
---------
                             lecturer2                                             1
1
                                              DEPT1                                 1
1
                                              Physics                               1
1
                                              Chemistry
Num CPPM Entries:3
```

The output of this command includes the following parameters:

Column	Description
Device	Shows the MAC address of the AirGroup device.
device-owner	Shows the user name of the AirGroup device.
shared location-id AP-name	Shows the location ID based on AP name.
shared location-id AP-FQLN	Shows the location ID based on the FQLN value of an AP.
shared location-id AP-group	Shows the location ID based on the name of an AP group.
shared user-list	Shows one or more primary login IDs of an AirGroup user.
shared group-list	Shows one or more primary login IDs of an AirGroup user group.
shared role-list	Shows the name of the role.
CPPM-Req	Shows the number of requests sent to ClearPass Policy Manager to populate the policy details for the given client.
CPPM-Resp	Shows the number of responses received from the ClearPass Policy Manager for the policy details of the given client.

The following example shows the server group information:

```
(host) [mynode] #show airgroup cppm server-group

Airgroup AAA Server Group
-------------------------
Name  Inservice  trim-FQDN  match-FQDN
----  ---------  ---------  ----------
cppm  Yes        No
```

The output of this command includes the following parameters:

Column	Description
Name	Shows server group name.
Inservice	Shows in service status of server group.
trim-FQDN	Shows trim FQDN status of server group.
match-FQDN	Shows matching FQDN of server group.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup cppm-server

```
show airgroup cppm-server {aaa|query-interval|radius statistics|rfc3576 statistics}
```

Description

This command shows the ClearPass Policy Manager server information.

Syntax

Parameter	Description	Range	Default
`<aaa>`	Shows AirGroup aaa profile.	—	—
`query-interval`	Shows the ClearPass Policy Manager periodic query interval time.	1 - 24 hours	10 hours
`radius statistics`	Shows the RADIUS server statistics for AirGroup.	—	—
`rfc3576 statistics`	Shows the RFC3576 server statistics for AirGroup.	—	—

Usage Guidelines

This command shows the ClearPass Policy Manager server information. For the remaining parameters, see the command syntax.

Example

The following example shows the AirGroup aaa profile information:

```
(host) [mynode] #show airgroup cppm-server aaa

Airgroup AAA profile
--------------------
Parameter                                                Value        Set
---------                                                -----        ---
Server Group                                             san-dot1x
RFC 3576 server                                          10.15.16.39
Configure dead time for a down Server                    5
Configure UDP port to receive RFC 3576 server requests.  5999
```

The output of this command includes the following parameters:

Column	Description
`Parameter`	Shows the parameter name.
`Value`	Shows the value configured.
`Set`	Shows the value applied.

The following example shows the ClearPass Policy Manager query interval:

```
(host) [mynode] #show airgroup cppm-server query-interval

CPPM Server Query Interval
```

```
-------------------------
Timer Value  Unit
-----------  ----
10           hours
```

The output of this command includes the following parameters:

Column	Description
Timer Value	Shows the query interval.
Unit	Shows the unit of the query interval.

The following example shows the RADIUS server statistics:

```
(host) [mynode] #show airgroup cppm-server radius statistics

Airgroup RADIUS Server Statistics
---------------------------------
Statistics             cppm_ser01
----------             ----------
PAP Requests           30175
Mismatch Response      1070
Bad Authenticator      0
Access-Accept          29032
Access-Reject          7
Unknown Response code  0
Timeouts               6906
AvgRespTime (ms)       815
Total Requests         30175
Total Responses        30109
Uptime (d:h:m)         0:2:19
SEQ Total/Free         255/255
Orphaned requests = 0
```

The following example shows the RFC3576 server statistics:

```
(host) [mynode] #show airgroup cppm-server rfc3576 statistics

Airgroup RFC3576 Statistics
---------------------------
Statistics           10.15.16.39
----------           -----------
Disconnect Requests  0
No Secret            0
Bad Authenticator    0
Invalid Request      0
Packets Dropped      0
Unknown service      0
CoA Requests         0
CoA Accepts          0
CoA Rejects          0
No permission        0
RFC3576 port number                    : 5999
Packets received from unknown clients : 0
Packets received with unknown request : 0
Total RFC3576 packets Received        : 0
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup domain

```
show airgroup domain
```

Description

This command shows the list of configured AirGroup domains. This command is applicable only on stand-alone controllers.

Syntax

No parameters.

Usage Guidelines

This command shows the list of configured AirGroup domains. This command is applicable only on stand-alone controllers

Example

The following example shows the list of configured AirGroup domains:

```
(host) [mynode] #show airgroup domain

AirGroup Domains
----------------
Name  Description  IP-Address
----  -----------  ----------
test  test         10.15.52.2
10.15.52.16
ag                 10.15.52.2
10.15.52.16
Num domains:2
```

The output of this command includes the following parameters:

Column	Description
`Name`	Shows the name of the AirGroup domain.
`Description`	Shows a short description of the AirGroup domain.
`IP-Address`	Shows IP address or VRRP IP address the stand-alone controller.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on stand-alone controller

show airgroup flow-table

```
show airgroup flow-table
```

Description

This command shows flows configured by AirGroup.

Syntax

No parameters.

Usage Guidelines

This command shows flows configured by AirGroup.

Example

The following example shows flows configured by AirGroup process:

```
(host) [mynode] #show airgroup flow-table

AirGroup flows table
--------------------
Dpid         Flow Grp ID       Flow ID           In Port  Src Mac  Dst Mac  Ether
----         -----------       -------           -------  -------  -------  -----
c29d76de3    15dc000000000002  15dc00000000348c  *        *        *        0x800
c29d76de3    15dc00000000000a  15dc000000003494  *        *        *        0x800
1a1e01bdb0   15dc000000000005  15dc00000000348f  *        *        *        0x800
1a1e01bdb0   15dc00000000000b  15dc000000003495  *        *        *        0x800
b869a4a37    15dc000000000008  15dc000000003492  *        *        *        0x800
b869a4a37    15dc00000000000c  15dc000000003496  *        *        *        0x800

Src IP  Dst IP           Proto  Src Port  Dst Port  Actions
------  ------           -----  --------  --------  -------
*       222.173.190.239  17     60001     60001     output=controller
*       *                17     *         1900      output=controller
*       222.173.190.239  17     60001     60001     output=controller
*       *                17     *         1900      output=controller
*       222.173.190.239  17     60001     60001     output=controller
*       *                17     *         1900      output=controller
Num Switches:3
```

The output of this command includes the following parameters:

Column	Description
Dpid	Shows the Dpid information.
Flow Grp ID	Shows flow group ID information.
Flow ID	Shows the flow ID information.
In Port	Shows the in port information.
Src Mac	Shows the source MAC address.
Dst Mac	Shows the destination MAC address.

Column	Description
Ether	Shows the Ether information.
Src IP	Shows the source IP address.
Dst IP	Shows the destination IP address.
Proto	Shows the protocol information.
Src Port	Shows the source port information.
Dst Port	Shows the destination port information.
Actions	Shows the applied actions.

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show airgroup internal-state statistics

```
show airgroup internal-state statistics [dlna|mdns|verbose]
```

Description

This command shows the statistics of packets sent and received per second by AirGroup.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA statistics.	—	—
`mdns`	Shows the mDNS statistics.	—	—
`verbose`	Shows the detailed statistics.	—	—

Usage Guidelines

This command shows the statistics of packets sent and received per second by a AirGroup. For the remaining parameters, see the command syntax.

Example

The following example displays the packets sent and received per second by AirGroup:

```
(host) [mynode] #show airgroup internal-state statistics

Time: Tue Jul 12 13:18:24 2016
MDNS Messages
-------------
Opcode  Name                          Sent Since Last Read  Sent Total  Recv Since Last Read
Recv Total
------  ----                          --------------------  ----------  --------------------  -
---------
7       app                           0                     5           0                     0
-       SDN                           0                     11090       0
4152
Rx      Request                       N/A                   N/A         0
591
Rx      Response                      N/A                   N/A         0
556
Tx      Request-Refresh               0                     10104       N/A
N/A
Tx      Request-discovery             0                     1836        N/A
N/A
Tx      Request-wildcard              0                     0           N/A
N/A
Tx      Response-Solicited            0                     0           N/A
N/A
Tx      Response-Solicited-Fragment   0                     0           N/A
N/A
Tx      Response-Unsolicited          0                     0           N/A
N/A
Tx/Rx   Total                         0                     0           N/A
N/A

DLNA Messages
```

```
-------------
Opcode  Name             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----             --------------------  ----------  --------------------  ----------
-       SDN              0                     365947      0                     966861
Rx      Query            N/A                   N/A         0                     837484
Rx      Notify Announce  N/A                   N/A         0                     69450
Rx      Notify Bye       N/A                   N/A         0                     6
Tx      Response         0                     33958       N/A                   N/A

Internal MDNS Statistics
------------------------
Functionality                    Hit Count Since Last Read  Hit Count Total
-------------                    -------------------------  ---------------
Response - Cache Update          0                          3176
Response                         0                          556
Query - prepare records + Policy 0                          591
Query - Policy                   0                          12
Query - resp pkt gen & send      0                          0
Query - Response packet send     0                          331139
Query                            0                          591
Multicast Response propagate     0                          0

Internal DLNA Statistics
------------------------
Functionality                    Hit Count Since Last Read  Hit Count Total
-------------                    -------------------------  ---------------
Response - Cache Update          0                          73921
Response                         0                          0
Query - prepare records + Policy 0                          14227
Query - Policy                   0                          34360
Query - resp pkt gen & send      0                          14170
Query - Response packet send     0                          74397
Query                            0                          837484

MDNS Multi-controller Cluster Messages
--------------------------------------
Type                             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv
Total
----                             --------------------  ----------  --------------------  ----
------
Unicast Response with tag        0                     0           0                     0
Request with tag                 0                     0           0                     0
Raw Response                     0                     0           0                     0
Multicast Propagate Raw Response 0                     0           0                     0

DLNA Multi-controller Cluster Messages
--------------------------------------
Type             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----             --------------------  ----------  --------------------  ----------
Request with tag 0                     0           0                     0
Raw Response     0                     0           0                     0

Packet Arrival Statistics (per minute)
--------------------------------------
Peak Packet Arrival Rate  Peak Arrival Time  No. Servers  No. Clients
------------------------  -----------------  -----------  -----------
454                       Jul 05 10:34:42    5            16

Cache Bucket Size
-----------------
Service  AP Name Bucket  AP FQLN Bucket  User Name Bucket  Default Bucket
-------  --------------  --------------  ----------------  --------------
```

```
MDNS     0               0               0                1
SSDP     0               0               0                4

Internal mDNS and DLNA Thread Statistics
----------------------------------------
#  Thread ID   Query since Last Read  Queries Recv Total  Queries in Queue  Peak Queries in
Queue
-  ---------   ---------------------  ------------------  ----------------  ------------------
---
1  3368556288  0                      488871              0                 6
2  3343378176  0                      92304               0                 10
3  3318200064  0                      74141               0                 2
4  3293021952  0                      109923              0                 11
5  3267843840  0                      72836               0                 2

MDNS CPU and Throttling details
-------------------------------
Current CPU Utilization (%)  Throttling State    Description         Query Pkt Dropped  Resp
Pkt Dropped
---------------------------  ----------------    -----------         -----------------  ------
----------
0.04(3)                      MDNS_NO_THROTTLING  No packets dropped  0                  0

list of controllers in same vlan
--------------------------------
Controller MAC
--------------
00:1a:1e:01:ae:28
00:0b:86:b5:15:97
00:1a:1e:01:99:e0
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bf:70
00:1a:1e:02:07:b0
00:0b:86:9a:4e:77
00:0c:29:10:8c:b8
00:0b:86:b8:e1:d8
00:1a:1e:01:bd:b0

list of local controllers  with AirGroup devices
------------------------------------------------
Controller MAC
--------------
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bd:b0

AirGroup users 13, AirGroup servers 5. Total devices 38
```

The following example displays the DLNA packets sent and received per second by AirGroup:

```
(host) [mynode] #show airgroup internal-state statistics dlna

Time: Tue Jul 12 13:24:01 2016

DLNA Messages
-------------
Opcode  Name             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----             --------------------  ----------  --------------------  ----------
-       SDN              149                   366096      396                   967257
Rx      Query            N/A                   N/A         378                   837862
Rx      Notify Announce  N/A                   N/A         10                    69460
Rx      Notify Bye       N/A                   N/A         0                     6
```

```
Tx      Response         0                    33958       N/A                  N/A

Internal DLNA Statistics
------------------------
Functionality                    Hit Count Since Last Read  Hit Count Total
-------------                    ------------------------  ---------------
Response - Cache Update          10                        73931
Response                         0                         0
Query - prepare records + Policy 0                         14227
Query - Policy                   0                         34360
Query - resp pkt gen & send      0                         14170
Query - Response packet send     10                        74407
Query                            378                       837862

DLNA Multi-controller Cluster Messages
--------------------------------------
Type              Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----              --------------------  ----------  --------------------  ----------
Request with tag  0                     0           0                     0
Raw Response      0                     0           0                     0

Packet Arrival Statistics (per minute)
--------------------------------------
Peak Packet Arrival Rate  Peak Arrival Time  No. Servers  No. Clients
------------------------  -----------------  -----------  -----------
454                       Jul 05 10:34:42    5            16

Cache Bucket Size
-----------------
Service  AP Name Bucket  AP FQLN Bucket  User Name Bucket  Default Bucket
-------  --------------  --------------  ----------------  --------------
SSDP     0               0               0                 4

Internal DLNA Thread Statistics
-------------------------------
#  Thread ID   Query since Last Read  Queries Recv Total  Queries in Queue  Peak Queries in
Queue
-  ---------   ---------------------  ------------------  ----------------  ------------------
---
1  3368556288  180                    489051              0                 6
2  3343378176  60                     92216               0                 10
3  3318200064  36                     73770               0                 2
4  3293021952  54                     109965              0                 11
5  3267843840  48                     72860               0                 2

MDNS CPU and Throttling details
-------------------------------
Current CPU Utilization (%)  Throttling State    Description         Query Pkt Dropped  Resp
Pkt Dropped
---------------------------  ----------------    -----------         -----------------  ------
----------
0.03(3)                      MDNS_NO_THROTTLING  No packets dropped  0                  0
```

The following example displays the mDNS packets sent and received per second by AirGroup:

```
(host) [mynode] #show airgroup internal-state statistics mdns

Time: Tue Jul 12 13:26:03 2016
MDNS Messages
-------------
Opcode  Name                         Sent Since Last Read  Sent Total  Recv Since Last Read
Recv Total
```

```
------  ----                          -------------------  ----------  --------------------  -
---------
7       app                           0                    5           0                       0
-       SDN                           2                    11092       0
4152
Rx      Request                       N/A                  N/A         0
591
Rx      Response                      N/A                  N/A         0
556
Tx      Request-Refresh               2                    10106       N/A
N/A
Tx      Request-discovery             0                    1836        N/A
N/A
Tx      Request-wildcard              0                    0           N/A
N/A
Tx      Response-Solicited            0                    0           N/A
N/A
Tx      Response-Solicited-Fragment   0                    0           N/A
N/A
Tx      Response-Unsolicited          0                    0           N/A
N/A
Tx/Rx   Total                         2                    0           N/A
N/A

Internal MDNS Statistics
------------------------
Functionality                     Hit Count Since Last Read  Hit Count Total
-------------                     -------------------------  ---------------
Response - Cache Update           0                          3176
Response                          0                          556
Query - prepare records + Policy  0                          591
Query - Policy                    0                          12
Query - resp pkt gen & send       0                          0
Query - Response packet send      232                        331371
Query                             0                          591
Multicast Response propagate      0                          0

MDNS Multi-controller Cluster Messages
--------------------------------------
Type                              Sent Since Last Read  Sent Total  Recv Since Last Read  Recv
Total
----                              --------------------  ----------  --------------------  ----
------
Unicast Response with tag         0                     0           0                     0
Request with tag                  0                     0           0                     0
Raw Response                      0                     0           0                     0
Multicast Propagate Raw Response  0                     0           0                     0

Packet Arrival Statistics (per minute)
--------------------------------------
Peak Packet Arrival Rate  Peak Arrival Time  No. Servers  No. Clients
------------------------  -----------------  -----------  -----------
454                       Jul 05 10:34:42    5            16

Cache Bucket Size
-----------------
Service  AP Name Bucket  AP FQLN Bucket  User Name Bucket  Default Bucket
-------  --------------  --------------  ----------------  --------------
MDNS     0               0               0                 1

Internal MDNS Thread Statistics
-------------------------------
```

```
#  Thread ID   Query since Last Read  Queries Recv Total  Queries in Queue  Peak Queries in
Queue
-  ---------   ---------------------  ------------------  ----------------  ------------------
---
1  3368556288  0                      0                   0                 6
2  3343378176  0                      148                 0                 10
3  3318200064  0                      407                 0                 2
4  3293021952  0                      12                  0                 11
5  3267843840  0                      24                  0                 2

MDNS CPU and Throttling details
-------------------------------
Current CPU Utilization (%)  Throttling State    Description         Query Pkt Dropped  Resp
Pkt Dropped
---------------------------  ----------------    -----------         -----------------  ------
----------
0.02(3)                      MDNS_NO_THROTTLING  No packets dropped  0                  0
```

The following example displays the detailed statistics of packets sent and received per second by AirGroup:

```
(host) [mynode] ##show airgroup internal-state statistics verbose

Time: Tue Jul 12 13:27:59 2016
PAPI Messages
-------------
Msg ID  Name                    Sent Since last Read  Sent Total  Recv Since Last Read  Recv
Total
------  ----                    --------------------  ----------  --------------------  ------
----
7062    Set switch ip6          0                     0           0                     1
7064    Set vlan ipv6 info      0                     0           0                     1
65534   sapi getstate response  0                     0           0                     1
7005    Set switch ip           0                     0           0                     1
14001   mdns cli request        0                     0           1                     331

RADIUS Client Messages
----------------------
Type                       Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----                       --------------------  ----------  --------------------  ----------
Auth Req/Resp              0                     30223       0                     13823
RFC3576                    N/A                   N/A         0                     0
CPPM Device-Entry Added    N/A                   N/A         0                     2
CPPM Device-Entry Deleted  N/A                   N/A         0                     0

MDNS Messages
-------------
Opcode  Name                        Sent Since Last Read  Sent Total  Recv Since Last Read
Recv Total
------  ----                        --------------------  ----------  --------------------  -
---------
7       app                         0                     5           0                     0
-       SDN                         0                     11092       0
4152
Rx      Request                     N/A                   N/A         0
591
Rx      Response                    N/A                   N/A         0
556
Tx      Request-Refresh             0                     10106       N/A
N/A
Tx      Request-discovery           0                     1836        N/A
N/A
Tx      Request-wildcard            0                     0           N/A
N/A
```

```
Tx      Response-Solicited           0                    0           N/A
N/A
Tx      Response-Solicited-Fragment  0                    0           N/A
N/A
Tx      Response-Unsolicited         0                    0           N/A
N/A
Tx/Rx   Total                        0                    0           N/A
N/A

DLNA Messages
-------------
Opcode  Name             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
------  ----             --------------------  ----------  --------------------  ----------
-       SDN              0                     366195      8                     967567
Rx      Query            N/A                   N/A         8                     838110
Rx      Notify Announce  N/A                   N/A         0                     69490
Rx      Notify Bye       N/A                   N/A         0                     6
Tx      Response         0                     33958       N/A                   N/A

Internal MDNS Statistics
------------------------
Functionality                    Hit Count Since Last Read  Hit Count Total
-------------                    -------------------------  ---------------
Response - Cache Update          0                          3176
Response                         0                          556
Query - prepare records + Policy 0                          591
Query - Policy                   0                          12
Query - resp pkt gen & send      0                          0
Query - Response packet send     0                          331387
Query                            0                          591
Multicast Response propagate     0                          0

Internal DLNA Statistics
------------------------
Functionality                    Hit Count Since Last Read  Hit Count Total
-------------                    -------------------------  ---------------
Response - Cache Update          0                          73961
Response                         0                          0
Query - prepare records + Policy 0                          14227
Query - Policy                   0                          34360
Query - resp pkt gen & send      0                          14170
Query - Response packet send     0                          74437
Query                            8                          838110

MDNS Multi-controller Cluster Messages
--------------------------------------
Type                             Sent Since Last Read  Sent Total  Recv Since Last Read  Recv
Total
----                             --------------------  ----------  --------------------  ----
------
Unicast Response with tag        0                     0           0                     0
Request with tag                 0                     0           0                     0
Raw Response                     0                     0           0                     0
Multicast Propagate Raw Response 0                     0           0                     0

DLNA Multi-controller Cluster Messages
--------------------------------------
Type              Sent Since Last Read  Sent Total  Recv Since Last Read  Recv Total
----              --------------------  ----------  --------------------  ----------
Request with tag  0                     0           0                     0
Raw Response      0                     0           0                     0
```

```
Packet Arrival Statistics (per minute)
--------------------------------------
Peak Packet Arrival Rate  Peak Arrival Time  No. Servers  No. Clients
------------------------  -----------------  -----------  -----------
454                       Jul 05 10:34:42    5            16

Cache Bucket Size
-----------------
Service  AP Name Bucket  AP FQLN Bucket  User Name Bucket  Default Bucket
-------  --------------  --------------  ----------------  --------------
MDNS     0               0               0                 1
SSDP     0               0               0                 4

Internal mDNS and DLNA Thread Statistics
----------------------------------------
#  Thread ID   Query since Last Read  Queries Recv Total  Queries in Queue  Peak Queries in
Queue
-  ---------   ----------------------  ------------------  ----------------  ------------------
---
1  3368556288  2                       489191              0                 6
2  3343378176  4                       92394               0                 10
3  3318200064  0                       74189               0                 2
4  3293021952  0                       110019              0                 11
5  3267843840  2                       72908               0                 2

MDNS CPU and Throttling details
-------------------------------
Current CPU Utilization (%)  Throttling State    Description         Query Pkt Dropped  Resp
Pkt Dropped
---------------------------  ----------------    -----------         -----------------  ------
----------
0.03(3)                      MDNS_NO_THROTTLING  No packets dropped  0                  0

list of controllers in same vlan
--------------------------------
Controller MAC
--------------
00:1a:1e:01:ae:28
00:0b:86:b5:15:97
00:1a:1e:01:99:e0
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bf:70
00:1a:1e:02:07:b0
00:0b:86:9a:4e:77
00:0c:29:10:8c:b8
00:0b:86:b8:e1:d8
00:1a:1e:01:bd:b0

list of local controllers  with AirGroup devices
------------------------------------------------
Controller MAC
--------------
00:0b:86:9a:4a:37
00:0c:29:d7:6d:e3
00:1a:1e:01:bd:b0

AirGroup users 10, AirGroup servers 5. Total devices 36
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show airgroup multi-controller-table

```
show airgroup multi-controller-table [dlna|mdns|verbose]
```

Description

This command shows the information of all stand-alone controllers participating in an AirGroup domain. This command is applicable only on stand-alone controllers.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA statistics.	—	—
`mdns`	Shows the mDNS statistics.	—	—
`verbose`	Shows the detailed statistics.	–	–

Usage Guidelines

This command shows the information of all stand-alone controllers participating in an AirGroup domain. This command is applicable only on stand-alone controllers. For the remaining parameters, see the command syntax.

Example

The following example shows information of all stand-alone controllers participating in an AirGroup domain:

```
(host) [mynode] #show airgroup multi-controller-table

AirGroup Multi-Controller-Table
-------------------------------
IP-Address
----------
10.15.52.16
Num IP-Address:1
```

The following example shows the DLNA statistics all stand-alone controllers participating in an AirGroup domain:

```
(host) [mynode] #show airgroup multi-controller-table dlna

AirGroup Multi-Controller-Table verbose
---------------------------------------
IP-Address   Type  Request with Tag Tx  Unicast Response with tag Tx  Raw Response Tx  Request
with Tag Rx  Unicast Response with tag Rx  Raw Response Rx
----------   ----  -------------------  ----------------------------  ---------------  -------
------------  --------------------------  ---------------
10.15.52.16  DLNA  448                  N/A                           0                0
             N/A                          0
Num IP-Address:1
```

The following example shows the mDNS statistics all stand-alone controllers participating in an AirGroup domain:

```
(host) [mynode] #show airgroup multi-controller-table mdns

AirGroup Multi-Controller-Table verbose
---------------------------------------
```

```
IP-Address   Type  Request with Tag Tx  Unicast Response with tag Tx  Raw Response Tx  Request
with Tag Rx  Unicast Response with tag Rx  Raw Response Rx
----------   ----  -------------------  ----------------------------  ---------------  -------
------------  ----------------------------  ---------------
10.15.52.16  mDNS  1134                 0                             0                0
             0                           0
Num IP-Address:1
```

The following example shows the detailed statistics all stand-alone controllers participating in an AirGroup domain:

```
(host) [mynode] #show airgroup multi-controller-table verbose

AirGroup Multi-Controller-Table verbose
---------------------------------------
IP-Address   Type  Request with Tag Tx  Unicast Response with tag Tx  Raw Response Tx  Request
with Tag Rx  Unicast Response with tag Rx  Raw Response Rx
----------   ----  -------------------  ----------------------------  ---------------  -------
------------  ----------------------------  ---------------
10.15.52.16  mDNS  1134                 0                             0                0
             0                           0
10.15.52.16  DLNA  448                  N/A                           0                0
             N/A                         0
Num IP-Address:1
```

The output of this command includes the following parameters:

Table 9: *show airgroup multi-controller-table*

Column	Description
`IP-Address`	Shows the IP address of all stand-alone controllers participating in an AirGroup domain.
`Type`	Shows the type of record.
`Request with Tag Tx`	Shows the number of AirGroup queries transmitted with meta-tag information.
`Unicast Response with tag Tx`	Shows the number of AirGroup responses transmitted with meta-tag information.
`Raw Response Tx`	Shows the number of mDNS or DLNA responses transmitted.
`Request with Tag Rx`	Shows the number of AirGroup queries received with meta-tag information.
`Unicast Response with tag Rx`	Shows the number of AirGroup responses received with meta-tag information.
`Raw Response Rx`	Shows the number of mDNS or DLNA responses received.

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on stand-alone controllers

show airgroup policy-entries

```
show airgroup policy-entries [mac {neighborhood <macaddr>}>|<macaddr>]
```

Description

This command shows active AirGroup policies.

Syntax

Parameter	Description
`mac neighborhood <macaddr>`	Shows AP neighborhood to discover the AirGroup server.
`mac <macaddr>`	Shows active AirGroup policies for specified MAC address.

Usage Guidelines

This command shows active AirGroup policies. For the remaining parameters, see the command syntax.

Example

The following example shows the active AirGroup policies:

```
(host) [mynode] #show airgroup policy-entries

AirGroup Device Policy Information
----------------------------------
Device             device-owner  shared location-id AP-name  shared location-id AP-FQLN
------             ------------  --------------------------  --------------------------
aa:aa:aa:aa:aa:aa  N/A
aa:bb:cc:dd:ee:ff  N/A           xyzzy

shared location-id AP-group  shared user-list  shared group-list  shared role-list
---------------------------  ----------------  -----------------  ----------------
                                               sy                 saasa
                                               test

CPPM-Req  CPPM-Resp  source  Auto-Associate  Neighborhood
--------  ---------  ------  --------------  ------------
                     CLI                     1 hop(s)
                     CLI     AP-Name         1 hop(s)
Num Policy Entries:2
```

The output of this command includes the following parameters:

Column	Description
`Device`	Shows the MAC address of the device.
`device-owner`	Shows the device owner information.
`shared AP-name`	Shows the shared AP name information.
`shared AP-FQLN`	Shows the shared AP FQLN information.

Column	Description
shared AP-group	Shows the shared AP group information.
shared users	Shows the shared user information.
shared groups	Shows the shared group information.
shared roles	Shows the shared roles information.
CPPM-Req	Shows the ClearPass Policy Manager requests.
CPPM-Resp	Shows the ClearPass Policy Manager responses.
source	Shows the source (CLI or ClearPass Policy Manager) of the policy.
Auto-associate	Shows the auto association information.
Neighborhood	Shows the neighborhood information.

The following example shows the AP neighborhood to discover the AirGroup server:

```
(host) [mynode] #show airgroup policy-entries mac 00:1a:1e:aa:bb:cc

AirGroup Device Policy Information
----------------------------------
Device             device-owner  shared location-id AP-name  shared location-id AP-FQLN
------             ------------  -------------------------  -------------------------
00:1a:1e:aa:bb:cc  N/A

shared location-id AP-group  shared user-list  shared group-list  shared role-list
---------------------------  ----------------  -----------------  ----------------
                                               test

CPPM-Req  CPPM-Resp  source  Auto-Associate  Neighborhood
--------  ---------  ------  --------------  ------------
                     CLI                     1 hop(s)
Num Policy Entries:1
```

The output of this command includes the following parameters:

Column	Description
Device	Shows the MAC address of the device.
device-owner	Shows the device owner information.
shared AP-name	Shows the shared AP name information.
shared AP-FQLN	Shows the shared AP FQLN information.
shared AP-group	Shows the shared AP group information.
shared users	Shows the shared user information.

Column	Description
`shared groups`	Shows the shared group information.
`shared roles`	Shows the shared roles information.
`CPPM-Req`	Shows the ClearPass Policy Manager requests.
`CPPM-Resp`	Shows the ClearPass Policy Manager responses.
`source`	Shows the source (CLI or ClearPass Policy Manager) of the policy.
`Auto-associate`	Shows the auto association information.
`Neighborhood`	Shows the neighborhood information.

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show airgroup servers

```
show airgroup servers [dlna|mdns|verbose]
```

Description

This command shows the list of AirGroup servers.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA servers.	—	—
`mdns`	Shows the mDNS servers.	—	—
`verbose`	Shows the detailed statistics.	–	–

Usage Guidelines

This command shows the list of AirGroup servers. For the remaining parameters, see the command syntax.

Example

The following example shows the list of AirGroup servers:

```
(host) [mynode] #show airgroup servers

AirGroup Servers
----------------
MAC                IP             Type  Host Name      Service
---                --             ----  ---------      -------
5c:aa:fd:52:5a:f8  10.16.124.224  DLNA                 allowall
                                                        DLNA Media
5c:aa:fd:52:5a:fa  10.16.124.226  DLNA                 DLNA Media
                                                        allowall
f0:4d:a2:83:74:a5  10.16.126.16   DLNA                 DLNA Media
                                                        allowall
11:11:11:11:11:11  0.0.0.0        mDNS  world_cricket  static
a0:02:dc:85:c2:98  10.16.124.181  DLNA  10-16-124-181  DIAL

VLAN  Wired/Wireless  Role      Group  Username  AP-Name
----  --------------  ----      -----  --------  -------
124   wireless        ipad                       7010AP

124   wireless        ipad                       7010AP

126   N/A

0     N/A
124   wireless        x86-role                   arr
Num Servers: 5.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
VLAN	Shows the VLAN ID of the AirGroup server.
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. **NOTE:** The column displays **Wired** when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays **N/A**.
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.

The following example shows the list of AirGroup servers hosting DLNA service:

```
(host) [mynode] #show airgroup servers dlna

AirGroup Servers
----------------
MAC                IP             Type  Host Name      Service
---                --             ----  ---------      -------
5c:aa:fd:52:5a:f8  10.16.124.224  DLNA                 allowall
                                                       DLNA Media
5c:aa:fd:52:5a:fa  10.16.124.226  DLNA                 DLNA Media
                                                       allowall
f0:4d:a2:83:74:a5  10.16.126.16   DLNA                 DLNA Media
                                                       allowall
a0:02:dc:85:c2:98  10.16.124.181  DLNA  10-16-124-181  DIAL

VLAN  Wired/Wireless  Role      Group  Username  AP-Name
----  --------------  ----      -----  --------  -------
124   wireless        ipad                       7010AP

124   wireless        ipad                       7010AP

126   N/A

124   wireless        x86-role                   arr
Num Servers: 4.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
VLAN	Shows the VLAN ID of the AirGroup server.
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. **NOTE:** The column displays **Wired** when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays **N/A**.
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.

The following example shows the list of AirGroup servers hosting mDNS service:

```
(host) [mynode] #show airgroup servers mdns

AirGroup Servers
----------------
MAC                IP             Type  Host Name      Service
---                --             ----  ---------      -------
11:11:11:11:11:11  0.0.0.0        mDNS  world_cricket  static

VLAN  Wired/Wireless  Role      Group  Username  AP-Name
----  --------------  ----      -----  --------  -------
0     N/A
Num Servers: 1.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.
Service	Shows the service hosted by the AirGroup server.
VLAN	Shows the VLAN ID of the AirGroup server.

Column	Description
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. **NOTE:** The column displays **Wired** when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays **N/A**.
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.

The following example shows the detailed statistics of the AirGroup servers:

```
(host) [mynode] #show airgroup servers verbose

AirGroup Servers
----------------
MAC                IP             Type  Host Name      Service
---                --             ----  ---------      -------
5c:aa:fd:52:5a:f8  10.16.124.224  DLNA                 allowall
                                                       DLNA Media

VLAN  Wired/Wireless  Role      Group  Username
----  --------------  ----      -----  --------
124   wireless        ipad

AP-Name  Rec-dropped  Rec-filtered  Rec-responded  Last-query
-------  -----------  ------------  -------------  ----------
7010AP   0            0               0


Query Throttled  Resp Throttled  CPPM-Req  CPPM-Rsp  CoA
---------------  --------------  --------  --------  ---
0                0               1         1         0


CPPM Dev-Added  CPPM Dev-Deleted  Max PPM  Max PPM at        All IP(s)
Controller IP
--------------  ----------------  -------  ----------        ---------                    ------
------
                                  87       Jul 05 11:00:45   10.16.124.224
10.16.125.117
Num Servers: 5.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup server.
IP	Shows the IP address of the AirGroup server.
Type	Shows the type (DLNA/mDNS) of the AirGroup server.
Host Name	Shows the host name of the AirGroup server.

Column	Description
Service	Shows the service hosted by the AirGroup server.
Wired/Wireless	Shows how (wired/wireless) the AirGroup server is connected. **NOTE:** The column displays **Wired** when the server is connected to an untrusted wired port. When the server is connected to a trusted wired port, the column displays **N/A**.
VLAN	Shows the VLAN ID of the AirGroup server.
Role	Shows the user role of the AirGroup server.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup server.
AP-name	Shows the AP name to which the AirGroup server is connected.
Rec-dropped	Shows the number of queries dropped from the AirGroup server.
Rec-filtered	Shows the number of queries filtered as a result of the policies.
Rec-responded	Shows the number of queries responded from the AirGroup server.
Last-query	Shows the time stamp of the last query received.
CPPM-Req	Shows the number of requests sent to the ClearPass Policy Manager server to populate the policy details for the given AirGroup server.
CPPM-Rsp	Shows the number of responses received from the ClearPass Policy Manager server for policy details of the given AirGroup server.
CoA	Shows the number of Change of Authorization (CoA) requests sent by ClearPass Policy Manager server indicating the registered device.
CPPM Dev-Added	Shows the last time stamp when ClearPass Policy Manager policy information was learned.
CPPM Dev-Deleted	Shows the last time stamp when this device entry was deleted from the ClearPass Policy Manager table.
Max PPM	Shows the maximum PPM.
Max PPM at	Shows when the maximum PPM was reached.
All IPs	Shows all IP addresses
Controller IP	Shows IP address of other stand-alone controllers.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show airgroup status

```
show airgroup status
```

Description

This command shows the status of AirGroup.

Syntax

No parameters.

Usage Guidelines

This command shows the status of AirGroup.

Example

The following example shows the status of AirGroup:

```
(host) [mynode] #show airgroup status

AirGroup Information
--------------------
Feature               Status
-------               ------
MDNS                  Disabled
DLNA                  Enabled
Enforce Registration  Disabled
IPV6                  Enabled

AirGroup Service Information
----------------------------
Service     Status
-------     ------
remotemgmt  Disabled
DIAL        Enabled
AmazonTV    Enabled
DLNA Media  Enabled
test        Enabled
static      Enabled
combined    Enabled
DLNA Print  Disabled
allowall    Enabled
sharing     Disabled
chat        Disabled
Daniel      Enabled
itunes      Disabled
airplay     Enabled
airprint    Enabled
googlecast  Enabled
```

The output of this command includes the following parameters:

Column	Description
`Feature`	Shows name of AirGroup feature.
`Status`	Shows status of AirGroup feature.
`Service`	Shows name of AirGorup service.
`Status`	Shows status of AirGroup service.

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show airgroup tracebuf

```
show airgroup tracebuf [msgs [ip <ipaddr>]|[mac <macaddr>]]|pps]
```

Description

This command shows the trace buffer.

Syntax

Parameter	Description	Range	Default
`msgs [ip <ipaddr>]`	Shows the AirGroup trace buffer for the specified IP address.	—	—
`msgs [mac <macaddr>]`	Shows the AirGroup trace buffer for the specified MAC address.	—	—
`pps`	Shows the AirGroup packet arrival trace buffer.	–	–

Usage Guidelines

This command shows the trace buffer. For the remaining parameters, see the command syntax.

Example

The following example shows the trace buffer:

```
(host) [mynode] #show airgroup tracebuf

Airgroup Client(s) Message Trace
--------------------------------
Client(MAC)   Client(IP)   Time   Event
-----------   ----------   ----   -----
Airgroup Packet Arrival Message Trace
-------------------------------------
Time              Event
----              -----
Jul   5 10:35:42  Total Packets 454, MDNS: 0, DLNA: 0, Servers: 5, Users 16, CPU 0.10
Jul   5 10:20:41  Total Packets 286, MDNS: 0, DLNA: 0, Servers: 5, Users 17, CPU 0.07
Jul   5 10:17:40  Total Packets 282, MDNS: 0, DLNA: 0, Servers: 5, Users 18, CPU 0.07
Jul   4 16:01:38  Total Packets 260, MDNS: 0, DLNA: 0, Servers: 5, Users 11, CPU 0.07
Jul   4 16:00:37  Total Packets 222, MDNS: 0, DLNA: 0, Servers: 5, Users 9, CPU 0.06
Jul   4 15:59:37  Total Packets 217, MDNS: 0, DLNA: 0, Servers: 5, Users 6, CPU 0.08
Jul   4 11:29:11  Total Packets 190, MDNS: 0, DLNA: 0, Servers: 2, Users 3, CPU 0.06
Jul   4 11:18:10  Total Packets 85, MDNS: 0, DLNA: 0, Servers: 1, Users 0, CPU 0.03
Jul   4 11:17:10  Total Packets 6, MDNS: 0, DLNA: 0, Servers: 1, Users 0, CPU 0.00
Num Trace Entries:9
```

The output of this command includes the following parameters:

Column	Description
`Client (MAC)`	Shows the MAC address of the client.
`Client (IP)`	Shows the IP address of the client.
`Time`	Shows the time when the event occurred.
`Event`	Shows the details of the event.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup users

```
show airgroup users [dlna|mdns|verbose]
```

Description

This command shows the AirGroup user table.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA users.	—	—
`mdns`	Shows the mDNS users.	—	—
`verbose`	Shows detailed statistics.	–	–

Usage Guidelines

This command shows the AirGroup users. For the remaining parameters, see the command syntax.

Example

The following example shows the AirGroup users:

```
(host) [mynode] #show airgroup users

AirGroup Users
--------------
MAC                IP            Type   Host Name  VLAN  Wired/Wireless  Role  Group  Username
AP-Name
---                --            ----   ---------  ----  --------------  ----  -----  --------
-------
b8:ca:3a:cb:cd:c4  10.16.126.18  DLNA              126   N/A
34:e6:d7:09:d6:41  10.16.126.25  mDNS              126   N/A
34:e6:d7:09:d7:9b  10.16.126.29  DLNA              126   N/A
f8:ca:b8:18:10:58  10.16.126.54  mDNS              126   N/A
Num Users: 4.
```

The output of this command includes the following parameters:

Column	Description
`MAC`	Shows the MAC address of the AirGroup user.
`IP`	Shows the IP address of the AirGroup user.
`Type`	Shows the type of the AirGroup device.
`Host Name`	Shows the host name of the AirGroup user.
`VLAN`	Shows the VLAN ID of the AirGroup user.
`Wired/Wireless`	Shows how the AirGroup user is connected.

Column	Description
Role	Shows the user role of the AirGroup user.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup user.

The following example shows the dlna AirGroup users:

```
(host) [mynode] #show airgroup users dlna

AirGroup Users
--------------
MAC                IP            Type  Host Name  VLAN  Wired/Wireless  Role  Group  Username
AP-Name
---                --            ----  ---------  ----  --------------  ----  -----  --------
-------
b8:ca:3a:cb:cd:c4  10.16.126.18  DLNA             126   N/A
34:e6:d7:09:d7:9b  10.16.126.29  DLNA             126   N/A
Num Users: 2.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup user.
IP	Shows the IP address of the AirGroup user.
Type	Shows the type of the AirGroup device.
Host Name	Shows the host name of the AirGroup user.
VLAN	Shows the VLAN ID of the AirGroup user.
Wired/Wireless	Shows how the AirGroup user is connected.
Role	Shows the user role of the AirGroup user.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup user.

The following example shows the mDNS AirGroup users:

```
(host) [mynode] #show airgroup users mdns

AirGroup Users
--------------
MAC                IP            Type  Host Name  VLAN  Wired/Wireless  Role  Group  Username
AP-Name
---                --            ----  ---------  ----  --------------  ----  -----  --------
-------
34:e6:d7:09:d6:41  10.16.126.25  mDNS             126   N/A
f8:ca:b8:18:10:58  10.16.126.54  mDNS             126   N/A
Num Users: 2.
```

The output of this command includes the following parameters:

Column	Description
MAC	Shows the MAC address of the AirGroup user.
IP	Shows the IP address of the AirGroup user.
Type	Shows the type of the AirGroup device.
Host Name	Shows the host name of the AirGroup user.
VLAN	Shows the VLAN ID of the AirGroup user.
Wired/Wireless	Shows how the AirGroup user is connected.
Role	Shows the user role of the AirGroup user.
Group	Shows the group of the AirGroup user.
Username	Shows the user name of the AirGroup user.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroup vlan

```
show airgroup vlan
```

Description

This command shows a list of AirGroup VLANs.

Syntax

No parameters.

Example

The following example shows a list of AirGroup VLANs:

```
(host) [mynode] #show airgroup vlan

VLAN Table
----------
Vlan-Id  Server Status  User Status
-------  -------------  -----------
1        Allowed        Allowed
9        Allowed        Allowed
50       Allowed        Allowed
124      Allowed        Allowed
default  N/A            N/A
Num Vlans:5
```

The output of this command includes the following parameters:

Column	Description
`Vlan-Id`	Shows the VLAN ID.
`Server Status`	Shows the status of AirGroup server.
`User Status`	Shows the status of AirGroup user.

Command History:

Release	Modification
ArubaOS 6.3	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode

show airgroupprofile

```
show airgroupprofile
   activate
   cppm <name>
   domain <name>
   ipv6 <name>
   service <service-name>
   <profile-name>
```

Description

This command shows the AirGroup profile settings.

Syntax

Parameter	Description
`activate`	Shows the active AirGroup profile.
`cppm <name>`	Shows the AirGroup ClearPass Policy Manager profile.
`domain <name>`	Shows the AirGroup domain profile.
`ipv6 <name>`	Shows the AirGroup IPv6 profile.
`service <service-name>`	Shows the AirGroup service profile.
`<profile-name>`	Shows the AirGroup profile settings ClearPass Policy Manager details. ■ **entries**: Shows information for devices registered in ClearPass Policy Manager. ■ **server-group**: Shows ClearPass Policy Manager server group information.

Usage Guidelines

This command shows the AirGroup profile settings. For the remaining parameters, see the command syntax.

Example

The following example shows the current status of the AirGroup service default-airplay:

```
(host) [mynode] #show airgroupprofile service default-airplay

Airgroup Service Profile "default-airplay"
------------------------------------------
Parameter            Value
---------            -----
Service Id           _airplay._tcp
Service Id           _appletv-v2._tcp
Service Id           _raop._tcp
Service Description  AirPlay
```

Related Commands

Command	Description
airgroupprofile	This command configures an AirGroup profile.

Command History

Command	Description
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airgroupservice

```
show airgroupservice [dlna|mdns|verbose]
```

Description

This command shows information of AirGroup services.

Syntax

Parameter	Description	Range	Default
`dlna`	Shows the DLNA services.	—	—
`mdns`	Shows the mDNS services.	—	—
`Verbose`	Shows additional information of services.	—	—

Usage Guidelines

This command shows the information of AirGroup services. For the remaining parameters, see the command syntax.

Example

The following example shows the information of AirGroup DLNA services:

```
(host) [mynode] #show airgroupservice dlna

AirGroupService Table
---------------------
Service     status    service ID                                          Auto Associate
Description
-------     ------    ----------                                          --------------  --
---------
DIAL        Enabled   urn:dial-multiscreen-org:service:dial:1
DIAL supported by Chromecast, FireTV, Roku etc
                      urn:dial-multiscreen-org:device:dial:1
DLNA Media  Enabled   urn:schemas-upnp-org:device:MediaServer:1
Media
                      urn:schemas-upnp-org:device:MediaServer:2
                      urn:schemas-upnp-org:device:MediaServer:3
                      urn:schemas-upnp-org:device:MediaServer:4
                      urn:schemas-upnp-org:device:MediaRenderer:1
                      urn:schemas-upnp-org:device:MediaRenderer:2
                      urn:schemas-upnp-org:device:MediaRenderer:3
                      urn:schemas-upnp-org:device:MediaPlayer:1
DLNA Print  Disabled  urn:schemas-upnp-org:device:Printer:1
Print
                      urn:schemas-upnp-org:service:PrintBasic:1
                      urn:schemas-upnp-org:service:PrintEnhanced:1
allowall    Enabled   urn:smartspeaker-audio:service:SpeakerGroup:1
Remaining-Services
                      urn:schemas-upnp-org:device:ZonePlayer:1
                      urn:schemas-upnp-org:service:ConnectionManager:1
                      urn:schemas-upnp-org:service:ContentDirectory:1
                      urn:schemas-upnp-org:service:AlarmClock:1
                      urn:schemas-upnp-org:service:MusicServices:1
                      urn:schemas-upnp-org:service:DeviceProperties:1
                      urn:schemas-upnp-org:service:SystemProperties:1
                      urn:schemas-upnp-org:service:ZoneGroupTopology:1
```

```
                    urn:schemas-upnp-org:service:GroupManagement:1
                    urn:schemas-tencent-com:service:QPlay:1
                    urn:schemas-upnp-org:service:RenderingControl:1
                    urn:schemas-upnp-org:service:AVTransport:1
                    urn:schemas-sonos-com:service:Queue:1
                    urn:schemas-upnp-org:service:GroupRenderingControl:1

Num Services:4
Num Service-ID:28
```

The output of this command includes the following parameters:

Column	Description
`Service`	Shows the name of the AirGroup DLNA service.
`Status`	Shows the status of the AirGroup DLNA service.
`service ID`	Shows the AirGroup DLNA service ID.
`Description`	Shows the description of the AirGroup DLNA service.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show airmatch debug advanced stat

```
show airmatch debug advanced stat
   ap
   channel
   deployment
   eirp
   event
   nbr
   radio
```

Description

This command displays detailed statistics about the APs or radios on a Mobility Master.

Syntax

Parameter	Description
`ap`	Statistics related to the APs
`channel`	Statistics related to channel and channel bandwidth assignment
`deployment`	Statistics related to channel and EIRP deployment
`eirp`	Statistics related to the EIRP assignment
`event`	Statistics related to RF events
`nbr`	Statistics related to radio neighbors
`radio`	Statistics related to radios

Examples

The example below indicates the AirMatch statistics related to the APs:

```
(host)#show airmatch debug advanced stat ap

Field                                 Value
-----                                 -----
Number of APs                         2304
+-----------------------------------+
|Number of 5GHz Radios per AP model|
+-----------------------------------+
AP Model                              Count
--------                              -----
AP-205H                               1224
AP-224                                47
AP-225                                976
AP-275                                55
AP-365                                1
+------------------------------------+
|Number of 2.4GHz Radios per AP model|
+------------------------------------+
AP Model                              Count
--------                              -----
AP-205H                               1224
AP-224                                47
AP-225                                976
AP-275                                56
```

```
AP-365                                1
```

The example below indicates the AirMatch statistics related to the radios:

```
(host)#show airmatch debug advanced stat radio
Field                                   Count
-----                                   -----
Radios                                  4607
Active Radios                           4607
Inactive Radios                         0
Radios with Up-to-date Info             4607
Radios with Stale Info                  0
+-----------+
|5GHz Radios|
+-----------+
Field                                   Count
-----                                   -----
Radios                                  2303
Active Radios                           2303
Inactive Radios                         0
Active Radios with Up-to-date Info      0
+-------------+
|2.4GHz Radios|
+-------------+
Field                                   Value
-----                                   -----
Radios                                  2304
Active Radios                           2304
Inactive Radios                         0
Active Radios with Up-to-date Info      0
```

The example below indicates the AirMatch statistics related to the channels:

```
(host)#show airmatch debug advanced stat channel

+====================+
|Channel Distribution|
+====================+
+-----------------------------------+
|5GHz Channel Bandwidth Distribution|
+-----------------------------------+
Channel Bandwidth                     Count
-----------------                     -----
40MHz                                 500
80MHz                                 1803
+-------------------------------+
|5GHz Channel Range Distribution|
+-------------------------------+
Channel Range                         Count
-------------                         -----
36  - 40                              41
44  - 48                              39
52  - 56                              41
60  - 64                              46
100 - 104                             43
108 - 112                             41
116 - 120                             45
124 - 128                             41
132 - 136                             40
140 - 144                             39
149 - 153                             43
157 - 161                             41
36  - 48                              304
52  - 64                              305
```

```
100 - 112                              305
116 - 128                              291
132 - 144                              299
149 - 161                              299
+--------------------------------+
|5GHz Primary Channel Distribution|
+--------------------------------+
Primary Channel                        Count
---------------                        -----
36                                     94
40                                     102
44                                     91
48                                     97
52                                     103
56                                     94
60                                     96
64                                     99
100                                    100
104                                    99
108                                    96
112                                    94
116                                    97
120                                    94
124                                    94
128                                    92
132                                    100
136                                    92
140                                    94
144                                    92
149                                    91
153                                    98
157                                    92
161                                    102
+-------------------------------------+
|2.4GHz Channel Bandwidth Distribution|
+-------------------------------------+
Channel Bandwidth                      Count
-----------------                      -----
20MHz                                  2304
+----------------------------------+
|2.4GHz Primary Channel Distribution|
+----------------------------------+
Primary Channel                        Count
---------------                        -----
1                                      755
6                                      772
11                                     777
+=========================+
|Summary of Channel Reasons|
+=========================+
+--------------------+
|5GHz Channel Reasons|
+--------------------+
Channel Reason                         Count
--------------                         -----
AIRMATCH_INIT                          252
AIRMATCH_NOISE                         7
AIRMATCH_NOISE_CLEARED                 3
AIRMATCH_SOLVER                        2003
RADAR_CLEARED                          30
RADAR_DETECTED                         8
+---- -----------------+
```

```
|2.4GHz Channel Reasons|
+----------------------+
Channel Reason                          Count
--------------                          -----
AIRMATCH_INIT                           556
AIRMATCH_NOISE                          14
AIRMATCH_NOISE_CLEARED                  54
AIRMATCH_SOLVER                         1680
+==========================+
|Summary of Static Channels|
+==========================+
Band                                    Count
----                                    -----
5GHz                                    0
2.4GHz                                  0
```

The example below indicates the AirMatch statistics related to the EIRP assignments:

```
(host)#show airmatch debug advanced stat eirp

+=================+
|EIRP Distribution|
+=================+
+----------------------+
|5GHz EIRP Distribution|
+----------------------+
EIRP(dBm)                               Count
---------                               -----
5                                       10
6                                       4
7                                       13
8                                       10
9                                       22
10                                      34
11                                      57
12                                      133
13                                      263
14                                      221
15                                      216
16                                      270
17                                      280
18                                      308
19                                      167
20                                      107
21                                      65
22                                      44
23                                      42
24                                      13
25                                      6
26                                      7
27                                      2
29                                      2
30                                      7
+------------------------+
|2.4GHz EIRP Distribution|
+------------------------+
EIRP(dBm)                               Count
---------                               -----
4                                       33
5                                       23
6                                       41
7                                       67
```

```
8                                       199
9                                       292
10                                      315
11                                      240
12                                      255
13                                      353
14                                      254
15                                      119
16                                      38
17                                      20
18                                      19
19                                      15
20                                      3
21                                      1
22                                      1
25                                      15
30                                      1
+=============+
|EIRP Reasons|
+=============+
+------------------+
|5GHz EIRP Reasons|
+------------------+
EIRP Reason                             Count
-----------                             -----
AIRMATCH_INIT                           1262
AIRMATCH_SOLVER                         1041
+---- --------------+
|2.4GHz EIRP Reasons|
+-------------------+
EIRP Reason                             Count
-----------                             -----
AIRMATCH_INIT                           1212
AIRMATCH_SOLVER                         1092
+=============+
|Static EIRPs|
+=============+
Band                                    Count
----                                    -----
5GHz                                    0
2.4GHz                                  0
```

The example below indicates the AirMatch statistics related to the radio neighbors:

```
(host)#show airmatch debug advanced stat nbr

+-------------------------------+
|Radio Neighbor Discovery - 5GHz|
+-------------------------------+
Field                                       Count
-----                                       -----
Number of Radios Reporting Neighbors        2290
Number of Interfering Neighbors             184
Average Number of Friend Neighbors*         17
Average Number of Interfering Neighbors*    0
+--------------------------------+
|Radio Neighbor Discovery - 2.4GHz|
+--------------------------------+
Field                                       Count
-----                                       -----
Number of Radios Reporting Neighbors        2301
Number of Interfering Neighbors             2395
```

```
Average Number of Friend Neighbors*          22
Average Number of Interfering Neighbors*     6
```

The example below indicates the AirMatch statistics related to the channel and its EIRP deployments:

```
(host)#show airmatch debug advanced stat deployment

+------------------------------+
|Channel/EIRP Deployment - 5GHz|
+------------------------------+
Field                                       Count
-----                                       -----
Radios with AirMatch deployment             2303
Radios with AirMatch deployment completed    1891
Radios with AirMatch deployment in progress  412
Radios deployed with retries                 0
Radios with Solution from last optimization  428
+-------------------------------+
|Channel/EIRP Deployment - 2.4GHz|
+-------------------------------+
Field                                       Count
-----                                       -----
Radios with AirMatch deployment             2304
Radios with AirMatch deployment completed    1870
Radios with AirMatch deployment in progress  434
Radios deployed with retries                 0
Radios with Solution from last optimization  428
```

The example below indicates the AirMatch statistics related to RF events:

```
(host)#show airmatch debug advanced stat event

+---- -------+
|Radar Events|
+------------+
Duration                                Number of Radios
--------                                ----------------
1 day                                   725
7 days                                  725
+---- ------------+
|5GHz Noise Events|
+-----------------+
Duration                                Number of Radios
--------                                ----------------
1 day                                   35
7 days                                  35
+---- --------------+
|2.4GHz Noise Events|
+-------------------+
Duration                                Number of Radios
--------                                ----------------
1 day                                   26
7 days                                  26
+----------------------------+
|Radar Prone Channels (7 days)|
+----------------------------+
Channel                                 Number of Events
-------                                 ----------------
116                                     130
124                                     93
128                                     84
120                                     54
132                                     41
```

```
136                                 33
60                                  13
100                                 12
140                                 9
104                                 9
144                                 7
108                                 6
64                                  5
112                                 5
52                                  4
+--------------------------+
|Radar Prone Radios (7 days)|
+--------------------------+
Radio Mac          AP Model       Number of Events   AP name
---------          --------       ----------------   -------
a8:bd:27:cf:54:90  AP-335         12                 ARUBA-AP-01
70:3a:0e:61:43:30  AP-335         11                 ARUBA-AP-04
80:3a:0e:59:6f:50  AP-335         10                 ARUBA-AP-21
80:3a:0e:58:d7:d0  AP-335         10                 ARUBA-AP-09
80:3a:0e:5d:20:f0  AP-335         8                  ARUBA-AP-30
80:3a:0e:61:aa:10  AP-335         7                  ARUBA-AP-56
80:3a:0e:61:a2:30  AP-335         6                  ARUBA-AP-61
a9:bd:27:cf:85:50  AP-335         6                  ARUBA-AP-01
80:3a:0e:61:a5:10  AP-335         6                  ARUBA-AP-37
80:3a:0e:58:cb:d0  AP-335         5                  ARUBA-AP-11
+---------------------------------+
|5GHz Noise Prone Channels (7 days)|
+---------------------------------+
Channel                             Number of Events
-------                             ----------------
161                                 9
157                                 8
153                                 7
40                                  6
36                                  5
149                                 3
60                                  3
100                                 2
165                                 1
140                                 1
44                                  1
48                                  1
+-------------------------------+
|5GHz Noise Prone Radios (7 days)|
+-------------------------------+
Radio Mac          AP Model       Number of Events   AP name
---------          --------       ----------------   -------
60:3a:0e:57:df:30  AP-335         5                  ARUBA-AP-89
c5:b5:ad:0c:b3:f0  AP-303H        4                  ARUBA-AP-94
60:3a:0e:60:81:f0  AP-335         4                  ARUBA-AP-128
60:3a:0e:5b:57:d0  AP-335         2                  ARUBA-AP-08
60:3a:0e:52:8d:b0  AP-335         2                  ARUBA-AP-33
60:3a:0e:70:75:d0  AP-303H        1                  ARUBA-AP-109
60:3a:0e:5c:80:f0  AP-335         1                  ARUBA-AP-25
60:3a:0e:5c:a4:10  AP-335         1                  ARUBA-AP-01
c5:b5:ad:10:81:50  AP-303H        1                  ARUBA-AP-30
a4:bd:27:d4:8d:90  AP-335         1                  ARUBA-AP-45
+---------------------------------+
|2.4GHz Noise Prone Channels (7 days)|
+---------------------------------+
Channel                             Number of Events
-------                             ----------------
```

```
1                                   56
11                                  53
6                                   52
+---------------------------------+
|2.4GHz Noise Prone Radios (7 days)|
+---------------------------------+
Radio Mac          AP Model       Number of Events   AP name
---------          --------       ----------------   -------
c3:b5:ad:0c:b6:60  AP-303H        76                 ARUBA-AP-99
10:3a:0e:57:5c:20  AP-335         20                 ARUBA-AP-20
10:3a:0e:5c:7a:00  AP-335         10                 ARUBA-AP-06
10:3a:0e:5b:6e:00  AP-335         4                  ARUBA-AP-2
10:3a:0e:5b:56:80  AP-335         3                  ARUBA-AP-25
10:3a:0e:60:fa:e0  AP-335         3                  ARUBA-AP-26
10:3a:0e:5c:5f:e0  AP-335         3                  ARUBA-AP-21
10:3a:0e:5f:88:e0  AP-335         2                  ARUBA-AP-87
c0:b5:ad:11:4b:60  AP-303H        2                  ARUBA-AP-87
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug amon-stat

```
show airmatch debug amon-stat
```

Description

Display statistics for AMON messages sent from APs to Mobility Master

Syntax

No Parameters

Usage Guidelines

Each AP in a Mobility Master deployment measures its RF environment then sends the managed device AMON messages about the radio feasibility based on that AP's hardware capability, radio and regulatory domain, and RF neighbors. The managed device forwards these messages to Mobility Master, and the Mobility Master adds this information to a database, computes an optimal solution, and deploys the latest RF plan by sending updated settings to the APs. Issue the **show airmatch debug amon-stat** to view details about these AMON messages.

Example

```
(ALPHA-SC) [mm] (config) #show airmatch debug amon-stat
AMON statistics for 10.20.101.12
----------------------------------------
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :              366263
Number of Bytes    :           417539820
Number of Messages :              366263
ID  Fields  Size       Msgs          Bytes        Sequence #        Lost       %
---  ------  ----  -------------  -------------  -------------  -------------  ---
42       2  1004         366263      379448468          10676              0    0
AMON statistics for 10.20.101.13
----------------------------------------
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :              283644
Number of Bytes    :           323354160
Number of Messages :              283644
ID  Fields  Size       Msgs          Bytes        Sequence #        Lost       %
---  ------  ----  -------------  -------------  -------------  -------------  ---
42       2  1004         283644      293855184          22764              0    0
AMON statistics for 10.20.101.20
----------------------------------------
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :              136022
Number of Bytes    :           155065080
Number of Messages :              136022
ID  Fields  Size       Msgs          Bytes        Sequence #        Lost       %
---  ------  ----  -------------  -------------  -------------  -------------  ---
42       2  1004         136022      140918792          17567              0    0
AMON statistics for 182.74.254.28
----------------------------------------
Last Update Time   : 2016-06-04 03:49:41
Number of Packets  :               12599
Number of Bytes    :            14362860
Number of Messages :               12599
ID  Fields  Size       Msgs          Bytes        Sequence #        Lost       %
---  ------  ----  -------------  -------------  -------------  -------------  ---
42       2  1004          12599       13052564             93              0    0
```

The output of this command includes the following parameters:

Parameter	Description
`Last Update Time`	Time the last AMON message information was sent to Mobility Master
`Number of Packets`	Total number of AMON packets sent to Mobility Master since the AMON process started. This counter resets when Mobility Master reboots.
`Number of Bytes`	Total number of AMON bytes sent to Mobility Master since the AMON process started. This counter resets when Mobility Master reboots.
`Number of Messages`	Total number of AMON packets sent to Mobility Master since the AMON process started. This counter resets when Mobility Master reboots.
`ID`	The ID number of the AMON message type. ArubaOS 8.0 supports AMON messages with the message ID of **42.**
`Fields`	Number of fields in the AMON message. AMON messages with the message ID of 42 include two fields.
`Size`	Total number of bytes sent for the AMON message ID.
`Msgs`	Total number of mesages sent for that AMON message ID.
`Bytes`	Total number of bytes sent for that AMON message ID.
`Sequence #`	For Internal use only
`Lost`	Number of lost messages.
`%`	Percentage of lost messages.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug apinfo

```
show airmatch debug apinfo
   ap-name <name>
   ethmac <mac>
```

Description

This command displays information about the AirMatch debug data of an AP.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view AirMatch debug data.
`ethmac <mac>`	Ethernet MAC ID of an AP for which you want to view AirMatch debug data.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug configs

```
show airmatch debug configs
```

Description

This command displays the advanced configuration settings in the AirMatch profile.

Syntax

No parameters

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays the configuration settings.

```
(host)[mm] #show airmatch debug configs
Field                              Value
-----                              -----
Radar Event Period 5GHz            1440
Noise Event Period 5GHz            1440
Noise Event Period 2GHz            1440
Run Now                            0
Deploy hour of day                 5
Deploy mode                        0
EIRP offset
TimeZone string                    PST8PDT,M3.2.0,M11.1.0
Is Active Server                   1
Is RF Planning Auto                1
Quality Threshold                  8
Solver Feas Deploy Threshold       25
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug db-dump status

```
show airmatch debug db-dump status
```

Description

This command displays information about the status of the AirMatch debug database dump.

Syntax

No syntax.

Example

The following example indicates the status of the AirMatch debug database dump:

```
(host)#show airmatch debug db-dump status

dbdump status info
------------------
Field                Value
-----                -----
dbdump status        SUCCESS
Begin time           2018-03-19 15:58:50
End time             2018-03-19 15:58:53
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug feasibility

```
show airmatch debug feasibility
   ap-name <name>
   mac <mac>
```

Description

Display information about an AP's feasibility based on that AP's hardware capability, radio and regulatory domain, and radio events such as radar detection and high noise detection.

Syntax

Parameter	Description
ap-name <name>	Name of an AP for which you want to view AirMatch feasibility data
mac <mac>	MAC address an AP for which you want to view AirMatch feasibility data

Example

The following example displays feasibility information for an AP-345 access point.

```
(host) [mynode] (802.11g radio profile "default") #show airmatch debug feasibility ap-name
ard4
Field                    Value
-----                    -----
Mac                      c8:b5:ad:ba:eb:c0
Updated On               2017-10-19 18:24:48
Current Opmode           DUAL_BAND
HW Supported Opmodes     DUAL_BAND,DUAL_5G
Configured   Opmodes     DUAL_BAND
Feasible     Opmodes     DUAL_BAND
Chan 20MHz               36,44,48,52
Chan 40MHz
Chan 80MHz
Chan 160MHz
Bandwidth                20MHz
Config   BW   range(MHz) 20 - 160
Hardware BW   range(MHz) 20 - 40
Eirp Range Chan  20MHz   52:[12,16] 36:[12,16] 44:[12,16] 48:[12,16]
Eirp Range Chan  40MHz
Eirp Range Chan  80MHz
Eirp Range Chan 160MHz
EIRP(dBm)                0 - 0
Config   EIRP range(dBm) 12 - 16
Hardware EIRP range(dBm) 0 - 0
EIRP Offset(dB)          0
Band                     5GHz
Band Range               BAND_LOWER
Update Reason            Flex Radio Update
Last Update              2017-10-19 18:24:48
AirMatch Radio Feasibility Band 2GHz for current opmode DUAL_BAND
-----------------------------------------------------------------
Field                    Value
-----                    -----
Mac                      c8:b5:ad:ba:eb:c0
Updated On               2017-10-19 18:24:48
Current Opmode           DUAL_BAND
HW Supported Opmodes     DUAL_BAND,DUAL_5G
Configured   Opmodes     DUAL_BAND
```

```
Feasible     Opmodes     DUAL_BAND
Chan 20MHz               1,6,11
Chan 40MHz               1,7
Chan 80MHz
Chan 160MHz
Bandwidth                20MHz,40MHz
Config   BW   range(MHz) 20 - 40
Hardware BW   range(MHz) 20 - 40
Eirp Range Chan  20MHz   6:[11,12] 11:[11,12] 1:[11,12]
Eirp Range Chan  40MHz   1:[11,12] 7:[11,12]
Eirp Range Chan  80MHz
Eirp Range Chan 160MHz
EIRP(dBm)                11 - 12
Config   EIRP range(dBm) 11 - 12
Hardware EIRP range(dBm) 10 - 25
EIRP Offset(dB)          0
Band                     2GHz
Band Range               BAND_FULL
Update Reason            Flex Radio Update
Last Update              2017-10-19 18:24:48
AirMatch Radio Feasibility Band 5GHz for current opmode DUAL_BAND
-----------------------------------------------------------------
Field                    Value
-----                    -----
Mac                      c8:b5:ad:ba:eb:d0
Updated On               2017-10-19 18:24:45
Current Opmode           DUAL_BAND
HW Supported Opmodes     DUAL_BAND,DUAL_5G
Configured   Opmodes     DUAL_BAND
Feasible     Opmodes     DUAL_BAND
Chan 20MHz               44,48
Chan 40MHz               36,44,149,157
Chan 80MHz               52,100,116,132
Chan 160MHz              36
Bandwidth                20MHz,40MHz,80MHz,160MHz,80+80MHz
Config   BW   range(MHz) 20 - 160
Hardware BW   range(MHz) 20 - 160
Eirp Range Chan  20MHz   44:[12,16] 48:[12,16]
Eirp Range Chan  40MHz   36:[12,16] 44:[12,16] 149:[12,16] 157:[12,16]
Eirp Range Chan  80MHz   52:[12,16] 100:[12,16] 116:[12,16] 132:[12,16]
Eirp Range Chan 160MHz   36:[12,16]
EIRP(dBm)                12 - 16
Config   EIRP range(dBm) 12 - 16
Hardware EIRP range(dBm) 0 - 31
EIRP Offset(dB)          0
Band                     5GHz
Band Range               BAND_FULL
Update Reason            Flex Radio Update
Last Update              2017-10-19 18:24:45

AirMatch Radio Feasibility Band 5GHz for alternate opmode DUAL_5G
-----------------------------------------------------------------
Field                    Value
-----                    -----
Mac                      c8:b5:ad:ba:eb:d0
Updated On               2017-10-19 18:24:45
Current Opmode           DUAL_BAND
HW Supported Opmodes     DUAL_BAND,DUAL_5G
Configured   Opmodes     DUAL_BAND
Feasible     Opmodes     DUAL_BAND
Chan 20MHz               100,104,108,112,116,120,124,128,132,136,140,144,149,153,157,161
Chan 40MHz               149,157
```

```
Chan 80MHz                100,116,132
Chan 160MHz
Bandwidth                 20MHz,40MHz,80MHz,80+80MHz
Config   BW   range(MHz) 20 - 160
Hardware BW   range(MHz) 20 - 160
Eirp Range Chan  20MHz   112:[12,16] 140:[12,16] 149:[12,16] 161:[12,16] 116:[12,16] 136:
[12,16] 144:[12,16] 100:[12,16] 153:[12,16] 157:[12,16] 124:[12,16] 128:[12,16] 132:[12,16]
104:[12,16] 108:[12,16] 120:[12,16]
Eirp Range Chan  40MHz   149:[12,16] 157:[12,16]
Eirp Range Chan  80MHz   100:[12,16] 116:[12,16] 132:[12,16]
Eirp Range Chan 160MHz
EIRP(dBm)                 0 - 0
Config   EIRP range(dBm) 12 - 16
Hardware EIRP range(dBm) 0 - 0
EIRP Offset(dB)           0
Band                      5GHz
Band Range                BAND_UPPER
Update Reason             Flex Radio Update
Last Update               2017-10-19 18:24:45
```

The output of this command includes the following parameters:

Parameter	Description
Mac	MAC address of the AP radio
Updated On	The last time the AP radio's feasibility information was updated in the Mobility Master database
Current Opmode	Current operation mode
HW Supported Opmodes	Supported operation modes
Configured Opmodes	Configured operation modes
Feasible Opmodes	Feasible operation modes
Chan 20MHz	List of feasible channels in 20 MHz bandwidth
Chan 40MHz	List of feasible channels in 40 MHz bandwidth
Chan 80MHz	List of feasible channels in 80 MHz bandwidth
Chan 160MHz	List of feasible channels in 160 MHz bandwidth
Bandwidth	List of feasible channel bandwidths
Config BW range(MHz)	List of configured channel bandwidths
Hardware BW range(MHz)	List of channel bandwidths supported by the hardware
Eirp Range Chan 20MHz	Range of EIRPs supported for each channel in a 20 MHz channel bandwidth
Eirp Range Chan 40MHz	Range of EIRPs supported for each channel in a 40 MHz channel bandwidth
Eirp Range Chan 80MHz	Range of EIRPs supported for each channel in a 80 MHz channel bandwidth
Eirp Range Chan 160MHz	Range of EIRPs supported for each channel in a 160 MHz channel bandwidth

Parameter	Description
`EIRP(dBm)`	Current supported EIRP range, in dBm.
`Config EIRP range(dBm)`	Configurable EIRP range, in dBm
`Hardware EIRP range(dBm)`	Hardware EIRP range, in dBm
`EIRP Offset(dB)`	Offset of the EIRP added to the computed EIRP (in dB)
`Band`	Operational Band, in GHz
`Band Range`	Current band range
`Update Reason`	Reason for previous feasibility update, such as a periodic update, radar detection, changes to a regulatory domain profile, or a radio band change for an AP radio that can operate in flex-radio mode. **NOTE:** An AP radio that supports flex mode can operate as a single radio in the 2.4 GHz band, a single radio in the 5 GHz band, or as two radios, operating separately in the 2.4 GHz and 5 GHz bands.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.3.0.0	The following fields were introduced in the command output: ■ **Current Opmode** ■ **HW Supported Opmodes** ■ **Configured Opmodes** ■ **Feasible Opmodes** ■ **Eirp Range Chan 20MHz** ■ **Eirp Range Chan 40MHz** ■ **Eirp Range Chan 80MHz** ■ **Eirp Range Chan 160MHz**
ArubaOS 8.2.0.0	The output in the **EIRP** field can display EIRP values in .1 dBm increments, and the **Update Reason** field can show if an AirMatch update was made due to a radio band change by an AP radio that supports both 1x1 dual radio mode and 2x2 single radio mode.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug history

```
show airmatch debug history
   ap-name <name>
   mac <mac>
```

Description

This command displays a history of AirMatch updates to an AP radio's channel, bandwidth, EIRP or mode.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view AirMatch history data
`mac <mac>`	MAC address an AP for which you want to view AirMatch history data

Example

```
(host)[mm] #show airmatch debug history ap-name West-2-155
2GHz    radio mac 6c:f3:7f:78:e2:80  ap name West-2-155
----------------------------------------------------------------------
Time of Change        Chan      Bandwidth  EIRP(dBm)     Mode       Source
--------------        ----      ---------  ---------     ----       ------
2016-06-07 05:34:45   11->  1   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-06-06 05:34:24    1-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-06-05 05:35:00    6->  1   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-06-04 05:34:55   11->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-06-02 05:34:30    6-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-06-01 05:34:48   11->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-30 05:32:44    6-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-29 05:35:41   11->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-28 05:34:49    1->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-27 05:34:29   11->  1   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-26 05:34:33    6-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-25 05:34:27   11->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-24 05:34:51    6-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-22 05:32:01    1->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-21 05:31:40   11->  1   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-19 05:32:51   11->  1   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-18 05:34:02    1-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-17 05:33:57    6->  1   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-14 05:34:17   11->  6   20-> 20    9.0-> 9.0    AP ->AP    Solver
2016-05-13 05:34:27    1-> 11   20-> 20    9.0-> 9.0    AP ->AP    Solver

5GHz    radio mac 6c:f3:7f:78:e2:90  ap name West-2-155
----------------------------------------------------------------------
Time of Change        Chan      Bandwidth   EIRP(dBm)      Mode       Source
--------------        ----      ---------   ---------      ----       ------
2016-06-07 05:33:45   40->149   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-06-06 05:33:24   44-> 40   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-06-05 05:34:00   52-> 44   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-06-03 05:33:27  161-> 52   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-06-02 05:33:30   40->161   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-05-31 05:33:25  153-> 40   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-05-30 05:31:44   44->153   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-05-29 05:34:41   40-> 44   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-05-28 05:33:49   60-> 36   40-> 40    18.0-> 18.0   AP ->AP    Solver
2016-05-27 05:33:29   64-> 60   40-> 40    18.0-> 18.0   AP ->AP    Solver
```

```
2016-05-26 05:33:33  149-> 64   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-25 05:33:27   56->149   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-24 05:33:50   48-> 56   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-23 05:32:50   36-> 48   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-22 05:31:01   52-> 36   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-21 05:30:40   40-> 52   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-20 05:35:40   40-> 60   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-19 05:31:50   40-> 52   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-18 05:33:02  161-> 40   40-> 40    18.0-> 18.0   AP ->AP   Solver
2016-05-17 05:32:57   56->161   40-> 40    18.0-> 18.0   AP ->AP   Solver
```

The output of this command includes the following parameters:

Parameter	Description
`Time of Change`	Timestamp showing when the change was made.
`Chan`	Previous and current channel assignments .
`Bandwidth`	Previous and current bandwidth assignments.
`EIRP(dBm)`	Previous and current EIRP levels.
`Mode`	Previous and current AP mode. Supported modes are AP and APM (Air Monitor).
`Source`	Source of the confirmation changes. AP changes made as a result of AirMatch calculations appear with the source type of "solver".

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.2.0.0	The output in the **EIRP** field can display EIRP values in .1 dBm increments.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug nbr

```
show airmatch debug nbr
   ap-name <name>
   mac <mac>
```

Description

This command displays information about neighbor APs seen by an AP that is managed over AirMatch.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view AirMatch neighbor data.
`mac <mac>`	MAC address an AP for which you want to view AirMatch neighbor data.

Example

```
(host) [mm] #show airmatch debug nbr  ap-name ssa-155
2GHz   radio mac 6c:f3:7f:78:e3:80  ap name ssa-155
-------------------------------------------------------------------------------------------
-
Nbr Mac            Is Friend  Path Loss(dB)  Channel  Last Update          AP Name
----------------   ---------  -------------  -------  -------------------  -------------------
-
c4:e9:84:67:d4:c0                   49            1    2016-06-08 01:50:16
00:1a:8c:9f:56:a8                   65           11    2016-06-07 23:15:43
00:1a:8c:9f:56:b8                   71            6    2016-06-08 00:48:00
be:d1:d3:91:87:c8                   82            6    2016-06-07 12:57:51
a2:f8:95:b1:a5:10                   83           11    2016-06-06 20:56:47
00:1a:8c:9f:56:c8                   85            1    2016-06-08 01:50:16
e0:98:61:a6:77:c0                   85            1    2016-06-06 17:00:55
00:1a:8c:9f:56:70                   86           13    2016-06-08 01:50:17
70:5a:9e:a6:19:50                   86           11    2016-06-08 00:16:52
c4:e9:84:67:da:68                   87            4    2016-06-08 01:50:17
8a:dc:96:1e:10:f8                   87            6    2016-06-08 01:19:19
```

The output of this command includes the following parameters:

Parameter	Description
`Nbr Mac`	MAC address of the neighbor AP.
`Is Friend`	Indicates whether the neighbor AP is associated to the same Mobility Master as the reporting AP.
`Path Loss(dB)`	Path loss between the neighbor AP and reporting AP, in dB.
`Channel`	Radio channel used by the neighbor AP.
`Last Update`	Date and time the reporting AP last received updated information from the neighbor AP.
`AP Name`	Name of the neighbor AP. The AP name will only appear if the neighbor AP is managed by the same Mobility Master as the reporting AP.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug optimization

```
show airmatch debug optimization
   [last | <seq>]
   [sort-by {ap-name | band | bandwidth | channel | eirp | rf-domain-id}] [descending]
```

Description

This command displays a list of RF debug optimizations performed by AirMatch.

Syntax

Parameter	Description	Range	Default Value
`last`	Last debug optimization.	—	—
`<seq>`	Optimization sequence number.	—	—
`sort-by`	Sorts the results in ascending order and on a per-band basis. Use this after specifying an optimization number or **last** as the value.	—	—
`ap-name`	Sorts results based on the AP name.	—	Ascending order
`band`	Sorts results based on the band.	2 GHz, 5 GHz	Ascending order
`bandwidth`	Sorts results based on the bandwidth.	—	Ascending order
`channel`	Sorts results based on the channel.	—	Ascending order
`eirp`	Sorts results based on the EIRP.	—	Ascending order
`rf-domain-id`	Sorts results based on the RF domain ID.	—	Ascending order
`descending`	Sort results in descending order.	—	—

Example

The following example shows a detailed summary of the RF debug optimization:

```
(host) [mm] #show airmatch debug optimization

Seq   Time                  APs   [5GHz] Radios Cost  Conflict
----- ------------------   -----         ------ ----- --------
#13   2018-03-23_02:45:07       3              3     4         0
#12   2018-03-22_05:35:58       3              3     4         0
#11   2018-03-21_10:15:55       3              3     4         0
#10   2018-03-21_09:17:14       3              3     2         0
#9    2018-03-20_12:00:51       3              3     2         0
#8    2018-03-19_12:00:47       3              3     2         0
#7    2018-03-18_12:00:46       3              3     2         0
#6    2018-03-17_12:00:43       3              3     2         0
#5    2018-03-16_12:00:40       3              3     2         0
#4    2018-03-15_12:00:39       3              3     2         0
#3    2018-03-14_12:00:42       3              3     2         0
```

```
#2    2018-03-14_08:10:32       3              3     2        0
#1    2018-03-14_05:54:50       1              1     2        0


[2GHz] Radios Cost  Conflict    Type                  Computed Computed
       ------ ----- --------    -------------------- -------- --------
         3     4        0              On-demand      Yes       No
         3     4        0              On-demand      Yes       No
         3     4        0              On-demand      Yes       No
         3     4        0              On-demand      Yes       No
         3     4        0              Scheduled      Yes       No
         3     4        0              Scheduled      Yes       No
         3     4        0              Scheduled      Yes       No
         3     4        0              Scheduled      Yes       No
         3     4        0              Scheduled      Yes       No
         3     4        0              Scheduled      Yes       No
         3     4        0              Scheduled      Yes      Yes
         3     4        0              On-demand      Yes       No
         1     4        0              On-demand      Yes       No
* EIRP is always computed in optimization
```

The following example shows a detailed summary of the RF debug optimization for a given sequence number:

```
(host) [mm] #show airmatch debug optimization 10

# Seq #10   2018-03-21_09:17:14     On-demand
# 5GHz   network cost/solution cost: 2.5/2
# 2.4GHz network cost/solution cost: 4/4
# Opmode Computed: false
# Opmode Deployed: false
# Band Radio              RFDom Part   Chan   CBW    EIRP(dBm)     Opmode     APName
ID    ID
---- ----------------- ----- ----- ----- ------ ---------  ----------  ----------
2GHz 70:3a:0e:6e:6e:60   002   000     1     20      12.0t  DUAL_BAND   303H-1
2GHz 6c:f3:7f:be:dc:20   001   000    11     20       9.0   DUAL_BAND   134-1
2GHz c8:b5:ad:bb:00:40   001   000     6     20      11.0t  DUAL_BAND   345-4
5GHz 70:3a:0e:6e:6e:70   002   000    40     40       9.0t  DUAL_BAND   303H-1
5GHz 6c:f3:7f:be:dc:30   001   000   161     40       9.0t  DUAL_BAND   134-1
5GHz c8:b5:ad:bb:00:50   001   000    40     40      10.0t  DUAL_BAND   345-4
[*] regarded frozen | [i] channel ignored because insufficient quality increase | [t] EIRP
truncated
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug pathloss history rep-radio

```
show airmatch debug pathloss history rep-radio
   ap-name <name>
   bssid <radio-bssid>
```

Description

This command displays information about the recent AirMatch debug path loss.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view AirMatch debug path loss history.
`bssid <radio-bssid>`	Shows the debug path loss history for a specific BSSID.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug reporting-radio

```
show airmatch debug reporting-radio
   ap-name <name>
   mac <mac>
```

Description

Displays details for an AP radio reporting AirMatch data to a Mobility Master.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view AirMatch radio data
`mac <mac>`	MAC address an AP for which you want to view AirMatch radio data

Example

```
(host) [mm] #show airmatch debug reporting-radio  ap-name ssa-155
Field                Value
-----                -----
Band                 5GHz
AP Ethernet MAC      9c:1c:12:c0:86:c6
Radio MAC            9c:1c:12:88:6c:70
AP Name              ard4
AP Model             AP-225
LMS IP               10.3.22.222
Last Update          2016-10-24 17:04:44
Channel              161
Bandwidth            40MHz
Channel Reason       AirMatch - Solver
Channel Update Time  2016-10-22 05:04:52
EIRP                 12.0 (dBm)
EIRP Reason          AirMatch - Init
EIRP Update Time     2016-10-12 13:29:03
Is Active            true
Is Static Chan       false
Is Static EIRP       false
Is Static CSR        false
```

The output of this command includes the following parameters:

Parameter	Description
`Band`	Radio band used by the AP
`AP Ethernet MAC`	MAC address of the Ethernet interface
`Radio MAC`	MAC address of the AP radio
`AP Name`	Name of the AP
`AP Model`	AP model type
`LMS IP`	IP address of the controller to which the AP is associated

Parameter	Description
Last Update	Timestamp showing the date and time the AP last sent an update to Mobility Master
Channel	Channel used by the AP radio
Bandwidth	Bandwidth used by the AP radio
Channel Reason	Reason why the channel was modified
Channel Update Time	Timestamp showing the date and time that the channel was updated
EIRP	Radio EIRP, in dBm.
EIRP Reason	Reason why the EIRP setting was modified
EIRP Update Time	Timestamp showing the date and time that the EIRP setting was updated
Is Active	Indicates if the AP is active on the network.
Is Static Chan	Indicates if the AP has been assigned to a static channel
Is Static EIRP	Indicates if the AP has been assigned to a static EIRP level
Is Static CSR	Indicates if the AP has been assigned to a static Cell Size Reduction (CSR) value. Cell Size Reduction settings control Rx sensitivity for the AP. When it is set to a specific value, the radio will not receive any frames with SNR/RSSI below this configured value.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.2.0.0	The output in the **EIRP** field can display EIRP values in .1 dBm increments.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug solver feasibility

```
show airmatch debug solver feasibility
   optimization <seq> {ap-name <ap-name> | bssid <bssid>}
```

Description

Display the feasibility information used by AirMatch Solver for a particular AP or MAC address during optimization.

Syntax

Parameter	Description
`optimization`	Displays the optimization history.
`<seq>`	Specify a sequence number to view details for a specific AirMatch solution.
`ap-name <name>`	Specify the name of an AP with the <ap-name> parameter to view AirMatch solver for the radios on that AP.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host) [mm] #show airmatch debug solver feasibility optimization 284 ap-name AP345_DEV4
Field                    Value
-----                    -----
Mac                      c8:b5:ad:ba:bc:40
AP Name                  AP345_DEV4
Band                     5GHz
Optimization ID          284
Computed On              2018-02-26_04:45:31
Chan 20MHz               36,40,44,48
Chan 40MHz               36,44
Chan 80MHz               36
Chan 160MHz
Bandwidth                20MHz,40MHz,80MHz

Field                    Value
-----                    -----
Mac                      c8:b5:ad:ba:bc:50
AP Name                  AP345_DEV4
Band                     5GHz
Optimization ID          284
Computed On              2018-02-26_04:45:31
Chan 20MHz               149,153,157,161,165
Chan 40MHz               149,157
Chan 80MHz               149
Chan 160MHz
Bandwidth                20MHz,40MHz,80MHz
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch debug static-radios

```
show airmatch debug static-radios
   band 2ghz|5ghz
```

Description

Show AirMatch data for AP radios that have been assigned static settings.

Syntax

Parameter	Description
band	Radio band for which want to view static radio data
2 ghz	View data for 2Ghz static radios
5 ghz	View data for 5Ghz static radios

Example

```
(host) *[mynode] (802.11g radio profile "default") #show airmatch debug static-radios
Static Radios for Band 5GHz
Radio Base Mac     Chan EIRP Oper    /BW    /EIRP Static /BW     Flag Last Update Time     AP Name
Channel             Channel
------------------ ---- ---- ------------------ ------------- ---- ------------------- -------
84:d4:7e:d2:10:90 Yes  Yes        36/  160/   5       36/  160      2016-10-24 17:06:30 ap315-1
18:64:72:7e:4d:90 Yes  Yes       149/   20/   5      149/   20      2016-10-24 17:04:47 x4p3
Flag column indicates '*' if Operating Channel is different from Static Channel configured
Note: Operating Channel can be different from Static Channel during Radar event
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch event

```
show airmatch event [{all-events|noise|radar} [all-aps | ap-name <ap-name> | bssid <bssid>]
<yyyy-mm-dd>]
```

Description

Displays radar and noise event information for a specific AP or all APs.

Syntax

Parameter	Description
`all-events|noise|radar`	Show radar and noise events of the APs in the database.
`all-aps`	Display list of all the APs in the database.
`ap-name <ap-name>`	Specify the name of an AP to display its radar and noise events.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`<yyyy-mm-dd>`	Show date in YYYY-MM-DD format.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example displays the noise and radar event information for all APs in the database.

```
(host) [mynode] #show airmatch event all-events all-aps
```

```
Band Event Type   Radio             Timestamp           Chan    CBW      APName
---- ------------ ----------------- ------------------- ------- -------- ----------
5GHz RADAR_DETECT c8:b5:ad:ba:eb:c0 2018-02-14_18:06:17      52    80MHz 345
5GHz RADAR_DETECT c8:b5:ad:ba:eb:d0 2018-02-13_10:35:55     140    80MHz 345
5GHz RADAR_DETECT c8:b5:ad:ba:eb:d0 2018-02-13_05:59:46     140    80MHz 345
5GHz RADAR_DETECT 9c:1c:12:88:6a:90 2018-02-10_04:06:02     100    80MHz 225
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-09_16:17:35      11    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-09_16:17:34       6    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-08_15:00:39      11    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-08_13:53:13       1    40MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:48:21       1    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:48:20       6    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:10:47      11    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_14:10:44       1    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_13:18:31      11    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-07_13:18:30       6    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-06_14:29:50       1    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-06_14:29:48       6    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-05_14:02:46      11    20MHz 345
5GHz RADAR_DETECT 9c:1c:12:88:6a:90 2018-02-05_11:57:42      52    80MHz 225
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-05_01:51:37       1    20MHz 345
5GHz NOISE_DETECT c8:b5:ad:ba:eb:c0 2018-02-05_01:51:34      11    20MHz 345
2GHz NOISE_DETECT 6c:f3:7f:7c:67:40 2018-02-05_00:27:21       6    20MHz 275
2GHz NOISE_DETECT 6c:f3:7f:7c:67:40 2018-02-04_23:53:55      11    20MHz 275
2GHz NOISE_DETECT 6c:f3:7f:7c:67:40 2018-02-04_23:09:19       1    20MHz 275
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile .
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch tech-support

```
show airmatch tech-support
   ap-name <name>
   mac <mac>
```

Description

This command collects the output for the AP or the radio, of a series of related AirMatch commands.

Usage Guidelines

Issue this command to collect the output for further support or engineering analysis. You can add a file name at the end of this command to capture the output to the flash.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view AirMatch technical support data.
`mac <mac>`	MAC ID of an AP for which you want to view AirMatch technical support data.

Example

The following example displays the output of the **show airmatch tech-support mac ac:a3:1e:59:b4:c0** command:

```
(host) [mynode] #show airmatch tech-support mac ac:a3:1e:59:b4:c0

show airmatch debug reporting-radio MAC ac:a3:1e:59:b4:c0
Field                Value
-----                -----
Band                 2GHz
AP Ethernet MAC      ac:a3:1e:cd:9b:4c
Radio MAC            ac:a3:1e:59:b4:c0
AP Name              F-16-a-QCA
AP Model             AP-325
LMS IP               192.168.200.15
Switch IP            192.168.200.15
Last Update          2017-11-16 02:57:57
Channel              7
Bandwidth            20MHz
Channel Reason       AirMatch - Solver
Channel Update Time  2017-11-14 10:42:53
EIRP                 10.0 (dBm)
EIRP Reason          AirMatch - Solver
EIRP Update Time     2017-11-16 02:55:19
Is Active            true
Is Static Chan       false
Is Static EIRP       false
Is Static CSR        false
Deploy Hour          N/A
Retries              5
Last Retry Time      2017-11-14 09:00:38
Local Time           PST8PDT,M3.2.0,M11.1.0
show airmatch debug optimization MAC ac:a3:1e:59:b4:c0
# 2017-11-15_08:00:36     Scheduled
# 5GHz   network cost/solution cost: 6.8/5.4
```

```
# 2.4GHz network cost/solution cost: 16.2/14.1
# Band Radio             RFDom Part  Chan  CBW    EIRP(dBm)  APName
ID    ID
---- ----------------- ----- ----- ----- ------ ---------  ----------
2GHz ac:a3:1e:59:b4:c0   001   000     3i    20i     10.0   F-16-a-QCA
[*] regarded frozen | [i] channel ignored because insufficient quality increase | [t] EIRP
truncated

show airmatch debug solution MAC ac:a3:1e:59:b4:c0
# Band Radio              Chan/Opt#     CBW      EIRP(dBm)/Opt# Chan Time           EIRP Time
         Confirm Time        Retries  APName
---- -----------------  ------------- -------- -------------- ------------------- ------------
------- ------------------- -------  ----------
2GHz ac:a3:1e:59:b4:c0        7 / 193       20     10.0 / 193 2017-11-14_10:42:46 2017-11-14_
10:42:46 2017-11-14_10:57:46       0  F-16-a-QCA
[*] regarded frozen | [#] result adjusted to match feasibility
show airmatch debug feasibility MAC ac:a3:1e:59:b4:c0
AirMatch Radio Feasibility Band 2GHz for current opmode DUAL_BAND
-----------------------------------------------------------------
Field                    Value
-----                    -----
Mac                      ac:a3:1e:59:b4:c0
Updated On               2017-11-16 02:37:28
Current Opmode           DUAL_BAND
HW Supported Opmodes     DUAL_BAND
Configured   Opmodes     DUAL_BAND,DUAL_5G
Feasible     Opmodes     DUAL_BAND
Chan 20MHz               3,7,9
Chan 40MHz
Chan 80MHz
Chan 160MHz
Bandwidth                20MHz
Config   BW   range(MHz) 20 - 20
Hardware BW   range(MHz) 20 - 40
Eirp Range Chan  20MHz   3:[9,12] 7:[9,12] 9:[9,12]
Eirp Range Chan  40MHz
Eirp Range Chan  80MHz
Eirp Range Chan 160MHz
EIRP(dBm)                9 - 12
Config   EIRP range(dBm) 6 - 12
Hardware EIRP range(dBm) 9 - 26
EIRP Offset(dB)          0
Band                     2GHz
Band Range               BAND_FULL
Update Reason            Periodic Update
Last Update              2017-11-16 02:37:28

show airmatch debug solver feasibility optimization 194 MAC ac:a3:1e:59:b4:c0
Field                    Value
-----                    -----
Mac                      ac:a3:1e:59:b4:c0
AP Name                  F-16-a-QCA
Band                     2GHz
Optimization ID          194
Computed On              2017-11-15_07:46:32
Chan 20MHz               3,7,9
Chan 40MHz
Chan 80MHz
Chan 160MHz
Bandwidth                20MHz

show airmatch debug nbr MAC ac:a3:1e:59:b4:c0
```

```
2GHz   radio mac ac:a3:1e:59:b4:c0  ap name F-16-a-QCA
-------------------------------------------------------------------------------------------------
---
Nbr Mac             Is Friend  Path Loss(dB)  Channel      Last Update          AP Name
-----------------  ---------  -------------  ---------    -------------------  ---------------
-----
70:3a:0e:52:23:a0      *           56               9    2017-11-16 02:55:19  F-17-QCA
ac:a3:1e:53:b8:00      *           57               7    2017-11-16 02:55:19  F-16-b-QCA
70:3a:0e:52:28:e0      *           61               7    2017-11-16 02:55:19  F-15-a
ac:a3:1e:59:c7:80      *           62               3    2017-11-16 02:55:19  F-16-c-QCA
ac:a3:1e:59:a0:00      *           64               3    2017-11-16 02:55:19  1344-2-AP04
70:3a:0e:52:22:40      *           66               9    2017-11-16 02:55:19  F-PP-b
ac:a3:1e:59:9d:00      *           67               3    2017-11-16 02:55:19  F-RVR-e
18:64:72:7e:af:20      *           68               3    2017-11-16 02:55:19  F-15-b-QCA
18:64:72:fd:67:a0      *           68               9    2017-11-16 02:55:19
18:64:72:c7:d6:7a
18:64:72:7e:c5:c0      *           69               3    2017-11-16 02:55:19  F-15-c-QCA
a8:bd:27:d0:69:e0      *           70               7    2017-11-16 02:55:19  F-PP-a-QCA
ac:a3:1e:59:b7:40      *           71               9    2017-11-16 02:55:19  F-RVR-g
70:3a:0e:6e:5e:20      *           72               7    2017-11-16 02:55:19  F-RVR-b
ac:a3:1e:59:97:e0      *           72               9    2017-11-16 02:55:19  F-RVR-d
a8:bd:27:59:f4:e0      *           75               3    2017-11-16 02:55:19  F-18-b
a8:bd:27:59:fc:00      *           76               9    2017-11-16 02:55:19  F-18-c
a8:bd:27:d0:94:a0      *           76               7    2017-11-16 02:55:19  F-18-a
ac:a3:1e:59:9a:c0      *           76               9    2017-11-16 02:55:19  F-14-QCA
ac:a3:1e:59:98:20      *           77               9    2017-11-16 02:55:19  F-Multiclient-a
ac:a3:1e:59:9e:00      *           77               3    2017-11-16 02:55:19  F-12
18:64:72:d3:81:00      *           78               7    2017-11-16 02:55:19  F-11-BRCM
ac:a3:1e:59:aa:a0      *           78               3    2017-11-16 02:55:19  F-13
9c:1c:12:87:33:60      *           79               9    2017-11-16 02:55:19  F-4-BRCM
a8:bd:27:d0:5f:c0      *           79               3    2017-11-16 02:55:19  F-19-b
a8:bd:27:d0:5e:80      *           81               3    2017-11-16 02:55:19  F-19-a
9c:1c:12:8c:6e:a0      *           84               7    2017-11-16 02:55:19  Fremont-
sniffer-225
a8:bd:27:59:fc:e0      *           84               9    2017-11-16 02:55:19  F-19-c
ac:a3:1e:59:9e:80      *           88               9    2017-11-16 02:55:19  F-front-door-1
c8:b5:ad:bb:13:c0      *           90              11    2017-11-13 15:44:15  F3-345
a8:bd:27:59:fb:e0      *           91               3    2017-11-14 22:03:56
a8:bd:27:cd:9f:be
c8:b5:ad:bb:15:00      *           96              11    2017-11-13 15:44:15  F8-345
b4:5d:50:6c:a6:c0                  42               1    2017-11-16 02:55:19
70:3a:0e:32:b7:08                  53               1    2017-11-14 16:18:53
70:3a:0e:32:b7:00                  62               1    2017-11-16 02:55:19
70:3a:0e:52:10:80                  63               1    2017-11-16 02:55:19
84:d4:7e:61:f9:a0                  67               6    2017-11-16 02:55:19
ac:a3:1e:b4:a3:00                  67               1    2017-11-16 02:55:19
40:e3:d6:bf:12:a0                  67               1    2017-11-15 16:57:15
c8:b5:ad:1f:c5:c8                  67              11    2017-11-14 08:55:52
34:fc:b9:fd:4b:a8                  68              11    2017-11-14 08:55:52
34:fc:b9:fd:4b:a0                  69              11    2017-11-16 02:55:19
b4:5d:50:6c:a6:c8                  69              11    2017-11-14 08:55:52
b4:5d:50:83:43:60                  70               1    2017-11-16 02:55:19
c8:b5:ad:1f:c5:c0                  70               6    2017-11-16 02:55:19
b4:5d:50:83:43:68                  71               1    2017-11-16 02:55:19
b4:5d:50:6c:a8:00                  71               1    2017-11-16 00:49:09
9c:1c:12:8c:6d:08                  72              11    2017-11-13 16:15:59
9c:1c:12:8c:6d:00                  74              11    2017-11-16 02:55:19
c8:b5:ad:bb:01:28                  74               6    2017-11-14 08:55:52
34:fc:b9:d3:53:80                  75               1    2017-11-16 02:55:19
b4:5d:50:db:f0:c0                  75              11    2017-11-16 02:55:19
18:64:72:25:76:a0                  76              11    2017-11-16 00:49:10
70:3a:0e:32:b9:a0                  78               1    2017-11-15 06:26:42
```

```
24:de:c6:2f:64:c0                  79                6    2017-11-16 02:55:19
08:ea:44:83:a4:50                  79                1    2017-11-13 15:44:15
08:ea:44:99:ad:10                  80                6    2017-11-16 02:55:19
24:de:c6:2f:65:40                  81                6    2017-11-16 02:55:19
34:fc:b9:fd:4c:40                  87                1    2017-11-14 11:35:13
84:d4:7e:61:f9:a8                  87                6    2017-11-14 08:55:52
ac:a3:1e:55:80:a0                  89                1    2017-11-16 02:55:19
00:21:43:46:2b:30                  92                6    2017-11-14 16:50:00
f0:5c:19:1c:6a:a0                  93               11    2017-11-14 10:31:24
f0:5c:19:1c:6a:a8                  93               11    2017-11-14 10:31:24
c8:b5:ad:bb:01:20                  93                6    2017-11-14 08:55:52
a8:bd:27:d0:65:20                  94               11    2017-11-14 08:55:52
a8:bd:27:d0:65:28                  94               11    2017-11-14 08:55:52
a8:bd:27:59:f0:20                  96                6    2017-11-14 10:31:24
a8:bd:27:59:f0:28                  96                6    2017-11-14 10:31:24
6c:f3:7f:e7:67:e0                  97                6    2017-11-14 09:59:29
40:e3:d6:7f:48:08                  97                6    2017-11-14 09:27:25
0a:8d:db:84:92:10                  97               11    2017-11-14 08:01:17
0c:8d:db:84:92:10                  97               11    2017-11-14 08:01:17
40:e3:d6:7f:48:00                  98               11    2017-11-14 08:55:52
6c:f3:7f:e7:67:e8                  98               11    2017-11-14 08:55:52
94:b4:0f:f3:1d:00                  98               11    2017-11-14 08:55:52
94:b4:0f:f3:1d:08                  98               11    2017-11-14 08:55:52
ac:a3:1e:b4:a3:08                  98                6    2017-11-14 08:55:52
b4:5d:50:6c:a2:c0                  99                1    2017-11-15 00:09:35
d8:50:e6:58:9b:48                 101               10    2017-11-16 02:55:19
e2:55:7d:78:75:48                 102                6    2017-11-14 17:52:51
f8:32:e4:54:8a:f8                 104                6    2017-11-16 02:55:19
ac:9e:17:a9:be:30                 107               10    2017-11-14 05:55:07
24:a4:3c:04:03:28                 107                1    2017-11-13 07:46:59
2e:a4:3c:04:03:28                 107                1    2017-11-13 07:46:59
32:a4:3c:04:03:28                 108                1    2017-11-13 15:44:15
2e:a4:3c:04:01:70                 109               11    2017-11-14 09:59:29
00:1e:e5:2c:87:38                 109               11    2017-11-13 15:44:15
70:77:81:45:42:68                 109                6    2017-11-13 07:46:59
2a:a4:3c:04:00:a8                 110                6    2017-11-13 09:23:08
2e:a4:3c:04:00:a8                 110                6    2017-11-13 07:46:59
32:a4:3c:04:00:a8                 110                6    2017-11-13 07:46:59
2a:a4:3c:04:01:70                 111               11    2017-11-14 08:55:52
32:a4:3c:04:01:70                 111               11    2017-11-14 08:55:52
24:a4:3c:04:01:70                 111               11    2017-11-14 08:01:17
c8:6c:87:fe:94:40                 111                1    2017-11-13 14:09:39
24:a4:3c:04:00:a8                 111                6    2017-11-13 07:46:59
00:90:4a:c1:01:f0                 112               11    2017-11-14 08:55:52

show airmatch debug history MAC ac:a3:1e:59:b4:c0
2GHz   radio mac ac:a3:1e:59:b4:c0  ap name F-16-a-QCA
--------------------------------------------------------------------------------------------
--
Time of Change       Chan              Bandwidth      EIRP(dBm)      Mode      Source
------------------   ---------------   ------------   ------------   --------  ---------------
--
2017-11-14 15:42:46        3->      7     20->   20     9.0-> 10.0   AP ->AP   Solver
2017-11-14 15:25:34        6->      1     20->   20    10.0->  9.0   AP ->AP   Solver
2017-11-14 13:26:47       11->      6     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-11-13 13:08:15        6->     11     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-11-12 21:00:52        6->      6     20->   20    11.0-> 10.0   AP ->AP   Solver
2017-11-11 21:00:42        6->      6     20->   20    10.0-> 11.0   AP ->AP   Solver
2017-11-08 21:00:41        6->      6     20->   20    11.0-> 10.0   AP ->AP   Solver
2017-11-06 21:00:41        6->      6     20->   20    10.0-> 11.0   AP ->AP   Solver
2017-11-05 21:00:42        6->      6     20->   20    11.0-> 10.0   AP ->AP   Solver
2017-11-03 21:00:31        6->      6     20->   20    10.0-> 11.0   AP ->AP   Solver
```

```
2017-11-02 20:26:18        1->      6     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-28 02:14:06        6->      1     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-28 02:09:35        1->      6     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-27 13:00:27        1->      1     20->   20     9.0-> 10.0   AP ->AP   Solver
2017-10-26 21:53:06        6->      1     20->   20    10.0->  9.0   AP ->AP   Solver
2017-10-25 20:31:48        1->      6     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-25 18:40:22        6->      1     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-25 18:29:11       11->      6     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-25 17:59:59        1->     11     20->   20    10.0-> 10.0   AP ->AP   Solver
2017-10-25 17:06:55       11->      1     20->   20     9.0-> 10.0   AP ->AP   Solver
show airmatch event radar MAC ac:a3:1e:59:b4:c0
No events found for bssid ac:a3:1e:59:b4:c0
show airmatch event noise MAC ac:a3:1e:59:b4:c0
No events found for bssid ac:a3:1e:59:b4:c0
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch network-tech-support

```
show airmatch network-tech-support
   ap-name <name>
   band <bandname> {2.4GHz|5GHz} <rf-domain>
   mac <mac>
```

Description

This command collects the output for all the radios that are in the same partition for a specified radio AP name. This command also lists and describes the AP radios that will be handled further.

Usage Guidelines

Issue this command to collect the output for further support or engineering analysis. You can add a file name at the end of this command to capture the output to the flash.

Syntax

Parameter	Description	Range	Default
`ap-name <name>`	Name of an AP for which you want to view AirMatch network support data	—	—
`band`	Radio type based on which the AP operates	2.4GHz to 5GHz	—
`mac <mac>`	MAC address an AP for which you want to view AirMatch network support data	—	—

Example

The following example displays a partial output of the **show airmatch network-tech-support ap-name F-16-a-QCA** command:

```
(host) [mynode]#show airmatch network-tech-support ap-name F-16-a-QCA
# Summary of included radios
# AP Name: F-16-a-QCA  Radio: ac:a3:1e:59:b4:c0  Band: 2GHz  RF domain: 001  partition: 000
# Num radios: 40  New radios: false
# Radio              AP Name
-----------------  -----------
ac:a3:1e:59:b4:c0  F-16-a-QCA
a8:bd:27:d0:69:e0  F-PP-a-QCA
9c:1c:12:8c:6e:a0  Fremont-sniffer-225
ac:a3:1e:59:9e:00  F-12
70:3a:0e:52:22:40  F-PP-b
ac:a3:1e:59:c7:80  F-16-c-QCA
ac:a3:1e:59:97:e0  F-RVR-d
ac:a3:1e:59:98:20  F-Multiclient-a
70:3a:0e:52:23:a0  F-17-QCA
a8:bd:27:d0:5e:80  F-19-a
70:3a:0e:52:28:e0  F-15-a
18:64:72:7e:af:20  F-15-b-QCA
a8:bd:27:59:fc:e0  F-19-c
a8:bd:27:59:fc:00  F-18-c
a8:bd:27:59:f4:e0  F-18-b
ac:a3:1e:59:aa:a0  F-13
a8:bd:27:d0:5f:c0  F-19-b
```

```
ac:a3:1e:53:b8:00  F-16-b-QCA
ac:a3:1e:59:b7:40  F-RVR-g
a8:bd:27:59:fb:e0  a8:bd:27:cd:9f:be
18:64:72:fd:67:a0  18:64:72:c7:d6:7a
18:64:72:d3:81:00  F-11-BRCM
ac:a3:1e:59:9e:80  F-front-door-1
9c:1c:12:87:33:60  F-4-BRCM
ac:a3:1e:59:9d:00  F-RVR-e
ac:a3:1e:59:9a:c0  F-14-QCA
70:3a:0e:6e:5e:20  F-RVR-b
a8:bd:27:d0:94:a0  F-18-a
ac:a3:1e:59:a0:00  1344-2-AP04
18:64:72:7e:c5:c0  F-15-c-QCA
# AP Name: F-16-a-QCA  Radio: ac:a3:1e:59:b4:d0  Band: 5GHz  RF domain: 001  partition: 000
# Num radios: 49  New radios: false
# Radio              AP Name
-----------------  -----------
```

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History

Release	Modification
ArubaOS 8.2.1.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch optimization

```
show airmatch optimization <seq>
```

Description

This command displays list of recent RF optimization jobs performed by AirMatch.

Syntax

Parameter	Description
`<seq>`	Specify a sequence number to view details for a specific AirMatch solution.

Example

The following example shows the history AirMatch solutions for 5 GHz and 2 Ghz radios.

```
(host) *[mynode] #show airmatch optimization
Seq  Time                APs  [5GHz] Radios Cost  Conflict Deploy     [2GHz] Radios Cost
Conflict Deploy    Type
---- ----------------   ---         ------ ----- -------- ------            ------ ----- ----
---- ------    ---------
#14  20161025_05:04:53     3              3   2.2      0.0 No                     0   0.0
0.0 No        Scheduled
#13  20161024_05:04:53     3              3   2.2      0.0 No                     0   0.0
0.0 No        Scheduled
#12  20161023_05:04:50     3              3   2.2      0.0 No                     0   0.0
0.0 No        Scheduled
#11  20161022_05:04:50     3              3   2.2      0.0 Yes                    0   0.0
0.0 No        Scheduled
#10  20161020_10:12:59     2              2   2.0      0.0 Yes                    0   0.0
0.0 Yes       On-demand
#9   20161020_09:20:23     2              2   2.0      0.0 Yes                    0   0.0
0.0 Yes       Quick
#8   20161020_09:19:27     2              2   2.0      0.0 Yes                    0   0.0
0.0 Yes       On-demand
```

The output of the **show airmatch optimization** command includes the following parameters:

Parameter	Description
`Seq`	Sequence number of the solution. The solution with the highest sequence number is the most recent.
`Time`	Timestamp showing the date and time AirMatch sent the solution update
`APs`	Number of APs updated with the new solution
`Radios`	Number of 5 Ghz or 2 Ghz AP radios updated with the new solution.
`Capacity`	**Capacity** is an internal metric to track the quality of a solution. The higher the capacity, the better the solution.
`Cost`	**Cost** is an internal metric to track the cost of a solution or a network state. The lower the cost, the better the solution. It is a measure of the overall quality of the solution or the network state.

Parameter	Description
Conflict	**Conflict** is an internal metric to track the quality of a solution. The lower the conflict, the better the solution.
Deploy	This column displays a status of **Yes** if the improvement in the radio band met or exceeded the threshold for deployment. If this column displays a status of **No**, the solution was below the quality threshold and was not deployed.

To see the detail of channel and EIRP plan for all the radios in the network, append the solution sequence number in the same command.

```
(host) [mm/mynode] #show airmatch optimization 14
# 20161025_05:04:53     Scheduled
# 5GHz   capacity/network cost/solution cost/improvement: 11.0/2.2/2.2/0.0%
# 2.4GHz capacity/network cost/solution cost/improvement: 0.0/0.0/0.0/0.0%
# Band Radio               Mode Chan  CBW    EIRP(dBm)  APName
---- -----------------  ---- ----- ------ ---------  ----------
5GHz 84:d4:7e:d2:10:90  AP     36*   160*        5*  ap315-1
5GHz 9c:1c:12:88:6c:70  AP    157i    40i       12.  ard4
5GHz 18:64:72:7e:4d:90  AP    149*    20*        5*  x4p3
[*] regarded frozen | [.] no change | [i] channel ignored because insufficient quality
increase
```

A radio is regarded frozen if any of the following are true:

- The CLI command "airmatch ap freeze" command has been used to configure and freeze radio settings
- The radio's regulatory domain profile leads to a single feasible channel by allowing only single valid channel, channel pair, or channel group.
- Neighboring radar and/or channel noise makes only a single channel feasible.

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch profile

```
show airmatch profile
```

Description

This command displays the configuration settings in the AirMatch profile.

Syntax

No parameters

Example

In this example, the output has been divided into multiple sections to better fit on the pages of this document. In the actual CLI, the output appears in a single, long table.

```
(host)[mm] #show airmatch profile
AirMatch profile (Predefined (changed))
---------------------------------------
Parameter          Value
---------          -----
schedule           Enabled
deploy-hour        5 o'clock
quality-threshold  15 percent
```

The output of this command includes the following parameters:

Parameter	Description
`Schedule`	Indicates if AirMatch scheduled updates are enabled. If the AirMatch updates are changed from the default **enabled** setting to **disabled**, the Mobility Master continues to receive RF updates from the APs, but no channel and EIRP changes are executed by the Mobility Master at the scheduled time.
`deploy-hour <0-23>`	Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format).
`eirp-offset`	Manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm
`quality-threshold`	The **quality-threshold** parameter represents the percentage of channel quality improvement that will trigger an AirMatch RF update. If a proposed channel change does not produce an improvement that meets or exceeds this threshold, AirMatch will not trigger a channel change.

Related Commands

Command	Description
airmatch profile	This command configures the AirMatch profile.
airmatch ap	A radio set with the **airmatch ap freeze** command uses a static radio configuration until those settings get explicitly canceled with the **airmatch ap unfreeze** command.

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The **quality-threshold** parameter is introduced.
ArubaOS 8.1.0.0	The **eirp-offset** parameter is deprecated. EIRP offset values can now be configured for AP groups via the rf dot11a-radio-profile and rf dot11g-radio-profile commands.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show airmatch solution

```
show airmatch solution
   ap-name <ap-name>
   list-all
   lms-ip <lms-ip>
   mac <mac-addr>
```

Description

This command displays history of AirMatch solution updates.

Syntax

Parameter	Description
`ap-name <ap-name>`	Specify the name of an AP with the <ap-name> parameter to view AirMatch solutions for the radios on that AP.
`list-all`	Show AirMatch solutions for all devices
`lms-ip <lms-ip>`	Show AirMatch solutions for APs associated to a specific controller by entering the IP address of that controller.
`mac <mac-adddr>`	Show AirMatch solutions for a specific AP radio by entering the MAC address of the radio.

Example

The following example shows the history of AirMatch solutions.

```
 (RagSC) ^[mynode] #show airmatch solution list-all
#Band Radio               Chan/Opt# CBW      EIRP(dBm)/Opt#  APName
---- -----------------  --------- -------- --------------  ----------
2GHz 00:24:6c:b1:9a:40      11/NA       20           6/NA  RAP_105
5GHz 00:24:6c:b1:9a:48     161/NA       40           12/3  RAP_105
2GHz 6c:f3:7f:a3:9b:80        6/7       20            6/7  RAP135-1
5GHz 6c:f3:7f:a3:9b:90      44/NA       40           12/7  RAP135-1
2GHz 70:3a:0e:8a:8b:c0        6/7       20           6/NA  AP315
5GHz 70:3a:0e:8a:8b:d0      40/NA       80           13/7  AP315
2GHz 9c:1c:12:3e:86:00        1/7       20           6/NA  RAP3
```

The output of the **show airmatch solution** command includes the following parameters:

Parameter	Description
`Band`	Frequency band used by the radio
`Radio`	MAC address of an AP radio
`Chan/Opt#`	Channel from optimization Opt #, and the new optimization sequence ID applied by the solution. If no change was made, the **Opt#** column displays the value "NA".
`CBW`	Channel bandwidth used by the radio.

Parameter	Description
`EIRP/Opt#`	EIRP from optimization Opt #, and the optimization sequence ID applied by the solution. If no change was made, the **Opt#** column displays the value "NA".
`AP_name`	Name of the AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The output of this command is updated to include capacity, network cost, solution cost and improvement data for each radio band.
ArubaOS 8.1.0.0	The output of this command has been modified to include channel and EIRP information. The information that appeared in the output of this command in previous versions of ArubaOS now appear in the command show airmatch optimization.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ale-configuration

```
show ale-configuration
```

Description

This command displays ALE configuration on the Mobility Master.

Syntax

No parameters.

Example

To display the ALE configuration:

```
(host) [mynode] (config) #show ale-configuration

Anonymization:  false
ALE Server-1:   none
ALE Server-2:   none
ALE Server-3:   none
ALE Server-4:   none
ALE Server-5:   none
nbapi_publish:  true
ale_sta_assoc:  false
```

Related Command

Command	Description
ale-configuration	Enable ALE configuration and its parameters on the Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show amon msg-buffer-size

```
show amon msg-buffer-size
```

Description

This command displays the size of AMON packets on the managed device.

Example

The following command displays size of AMON packet:

```
(host) [mynode] #show amon msg-buffer-size
amon msg-buffer-size :1264
```

Related Commands

Release	Modification
amon msg-buffer-size	Modifies the size of AMON packets on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show amon-receiver

```
show amon-receiver [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-stats-inst-
1] | [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] | [dest-stats-inst-5] |
[dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] | [error-counters] | [error-counters-
all] | [interest-table] | [list-details] | [parameter] | [set-debug-level-dest] | [src-stats-
all] | [stats-counters] | [stats-counters-all]]
```

Description

This command displays AMON receiver information.

Syntax

Parameter	Description
`dest-stats`	Shows destination statistics
`dest-stats-all`	Shows all destination statistics
`dest-stats-inst-0`	Shows destination statistics instance 0
`dest-stats-inst-1`	Shows destination statistics instance 1
`dest-stats-inst-2`	Shows destination statistics instance 2
`dest-stats-inst-3`	Shows destination statistics instance 3
`dest-stats-inst-4`	Shows destination statistics instance 4
`dest-stats-inst-5`	Shows destination statistics instance 5
`dest-stats-inst-6`	Shows destination statistics instance 6
`dest-stats-inst-7`	Shows destination statistics instance 7
`dest-table`	Shows destination table
`error-counters`	Shows error counters
`error-counters-all`	Show all error counters
`interest-table`	Show interest table
`list-details`	Show list details
`parameter`	Shows parameter String
`set-debug-level-dest`	Shows the set debug level for destination
`src-stats-all`	Shows all source statistics
`stats-counters`	Shows stats counters
`stats-counters-all`	Shows all stats counters

Example

The following command displays AMON receiver information for destination statistics instance 0:

```
(host) [mynode] #show amon-receiver dest-stats-inst-0

AMON-RECEIVER
dest_id  0: port 15260
-------------------------------------------------------------------
 Id: MsgName                          Mode      NoOfMsgs     NoOfBytes
-------------------------------------------------------------------
  0: RADIO_STATS                      UDS          44807      48570788
  1: VAP_STATS                        UDS          32958      31730709
  2: STATION_STATS                    UDS        1733704    2136005092
 10: USER_INFO                        UDS          26735      22146508
 11: AP_INFO                          UDS             18         13662
 12: RADIO_INFO                       UDS             22          2952
 13: VAP_INFO                         UDS             17          3138
 47: CLUSTER_SELF_NODE_INFO           UDS          26919       3822498
 48: CLUSTER_SELF_NODE_STATS          UDS          26913       4225341
 49: CLUSTER_PEER_NODE_INFO           UDS          80757      13163391
 50: CLUSTER_PEER_NODE_STATS          UDS          26913       7158858
 67: HWMON_TEMP_DETAIL                UDS          30881      15625786
 68: HWMON_FAN_DETAIL                 UDS          30881       6176200
 69: HWMON_SENSOR_THRS                UDS          30881       4539507
 70: HWMON_SENSOR_VAL                 UDS          30881       5280651
 71: HWMON_SYS_INFO                   UDS          48802      47923564
 72: FPAPPS_PORTS_INFO                UDS         107618      12914160
 73: FPAPPS_PORT_DETAIL               UDS         538030     497677750
 74: FPAPPS_PC_DETAIL_MESSAGE         UDS         860947     846310901
 75: FPAPPS_CTRL_INFO                 UDS         107617      10008381
 76: FPAPPS_CTRL_IP                   UDS         107619       8824758
-------------------------------------------------------------------
Total [ 21 messages]                              3893920    3722124595
-------------------------------------------------------------------

reclaim_reason_conn_not_ready : 0
no_of_times_punished          : 0

Start time        : Thu Jul  7 09:29:17 2016
Last Cleared time : Thu Jul  7 09:29:17 2016
Current time      : Wed Jul 13 15:06:07 2016 (Elapsed time: 538610)
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show amon-sender

```
show amon-sender [[dest-stats] | [dest-stats-all] | [dest-stats-inst-0] | [dest-stats-inst-1]
| [dest-stats-inst-2] | [dest-stats-inst-3] | [dest-stats-inst-4] | [dest-stats-inst-5] |
[dest-stats-inst-6] | [dest-stats-inst-7] | [dest-table] | [error-counters] | [error-counters-
all] | [interest-table] | [list-details] | [parameter] | [set-debug-level-dest] | [src-stats-
all] | [stats-counters] | [stats-counters-all]]
```

Description

This command displays AMON sender information. This command must be issued on the managed device.

Syntax

Parameter	Description
`dest-stats`	Shows destination statistics
`dest-stats-all`	Shows all destination statistics
`dest-stats-inst-0`	Shows destination statistics instance 0
`dest-stats-inst-1`	Shows destination statistics instance 1
`dest-stats-inst-2`	Shows destination statistics instance 2
`dest-stats-inst-3`	Shows destination statistics instance 3
`dest-stats-inst-4`	Shows destination statistics instance 4
`dest-stats-inst-5`	Shows destination statistics instance 5
`dest-stats-inst-6`	Shows destination statistics instance 6
`dest-stats-inst-7`	Shows destination statistics instance 7
`dest-table`	Shows destination table
`error-counters`	Shows error counters
`error-counters-all`	Show all error counters
`interest-table`	Show interest table
`list-details`	Show list details
`parameter`	Shows parameter String
`set-debug-level-dest`	Shows the set debug level for destination
`src-stats-all`	Shows all source statistics
`stats-counters`	Shows stats counters
`stats-counters-all`	Shows all stats counters

Example

The following command displays AMON receiver information for destination statistics instance 0:

```
(host) [mynode] # logon 192.0.1.12
```

```
(host) [MDC] # show amon-sender dest-stats-inst-0

AMON SENDER STATS
-----------------
AMON-SENDER
dest_id  0: 192.0.1.12
-----------------------------------------------------------------
 Id: MsgName                          Mode     NoOfMsgs    NoOfBytes
-----------------------------------------------------------------
  0: RADIO_STATS                       UDP        17979     19489236
  1: VAP_STATS                         UDP         9578     11258881
  2: STATION_STATS                     UDP       325693    401740468
  7: FW_AGG_SESSIONS                   UDP       190028    217222300
  9: FW_APP                            UDP          507       625776
 10: USER_INFO                         UDP         2443      2087840
 11: AP_INFO                           UDP           16        12144
 12: RADIO_INFO                        UDP           15         2064
 13: VAP_INFO                          UDP           13         2460
 18: AP_SYSTEM_STATS                   UDP         9578       756824
 26: FW_APP_CATEGORY                   UDP            2         1784
 27: FW_WEB_CC_CATEGORY                UDP            5         5500
 29: DHCP_STATION_INFO                 UDP        39048     37218948
 32: DOT1X                             UDP         1579       687868
 33: WPA_KEY_HANDSHAKE                 UDP         1527       282978
 36: PASSIVE_CTRL_STA_STATS            UDP          173        36916
 45: GEN_DATA                          UDP         4483      5254076
 47: CLUSTER_SELF_NODE_INFO            UDP         9005      1278710
 48: CLUSTER_SELF_NODE_STATS           UDP         9002      1413314
 49: CLUSTER_PEER_NODE_INFO            UDP        27022      4404586
 50: CLUSTER_PEER_NODE_STATS           UDP         9002      2394904
 67: HWMON_TEMP_DETAIL                 UDP         8149      4123394
 68: HWMON_FAN_DETAIL                  UDP         8149      1629800
 69: HWMON_SENSOR_THRS                 UDP         8149      1197903
 70: HWMON_SENSOR_VAL                  UDP         8149      1393479
 71: HWMON_SYS_INFO                    UDP         8149      8002318
 72: FPAPPS_PORTS_INFO                 UDP        18000      2160000
 73: FPAPPS_PORT_DETAIL                UDP       108000     99900000
 74: FPAPPS_PC_DETAIL_MESSAGE          UDP       144000    141552000
 75: FPAPPS_CTRL_INFO                  UDP        18000      1674000
 76: FPAPPS_CTRL_IP                    UDP        18000      1476000
-----------------------------------------------------------------
Total [ 31 messages]                              1003443    969286471
-----------------------------------------------------------------

reclaim_reason_conn_not_ready : 0
no_of_times_punished          : 0

Start time        : Sat Jul  9 23:23:47 2016
Last Cleared time : Sat Jul  9 23:23:47 2016
Current time      : Sat Jul 16 05:32:16 2016 (Elapsed time: 540509)

(host) [mynode] # logon 0: 2001:0000:0000:0000:0000:0000:0000:0002
(host) [MDC] # show amon-sender dest-stats-inst-0
AMON-SENDER
dest_id  0: 2001:0000:0000:0000:0000:0000:0000:0002
-----------------------------------------------------------------
Id: MsgName                           Mode     NoOfMsgs    NoOfBytes
-----------------------------------------------------------------
0: RADIO_STATS                       DTLS       333707    377756324
1: VAP_STATS                         DTLS       167371    143436947
2: STATION_STATS                     DTLS      1296493   1120169952
7: FW_AGG_SESSIONS                   DTLS      3382882   3903824624
9: FW_APP                            DTLS          522       644827
10: USER_INFO                         DTLS      1081366   1124538944
11: AP_INFO                           DTLS         5152      3951584
```

```
12: RADIO_INFO                    DTLS          266       291560
13: VAP_INFO                      DTLS          398       452952
26: FW_APP_CATEGORY               DTLS            2         1784
27: FW_WEB_CC_CATEGORY            DTLS            5         5500
35: PASSIVE_AP_STATION_STATS      DTLS        12543      2865738
36: PASSIVE_CTRL_STA_STATS        DTLS         2156      2153130
42: MCELL_REPORT                  DTLS       210661    224143304
45: GEN_DATA                      DTLS         3832      4491104
65: STATION_RSSI_INFO_V2          DTLS       232798    247697072
66: AP_NEIGHBORS_V2               DTLS       117511    125031704
67: HWMON_TEMP_DETAIL             DTLS          110        55660
68: HWMON_FAN_DETAIL              DTLS          110        22000
69: HWMON_SENSOR_THRS             DTLS          110        16170
70: HWMON_SENSOR_VAL              DTLS          110        18810
71: HWMON_SYS_INFO                DTLS          110       108020
72: FPAPPS_PORTS_INFO             DTLS          242        29040
73: FPAPPS_PORT_DETAIL            DTLS         1452      1343100
74: FPAPPS_PC_DETAIL_MESSAGE      DTLS         1936      1903088
75: FPAPPS_CTRL_INFO              DTLS          242        22506
76: FPAPPS_CTRL_IP                DTLS          242        19844
-----------------------------------------------------------------
Total [ 27 messages]                         6852329   7284995288
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The following parameters were modified to accept IPv6 address: ■ **dest-stats-all** ■ **dest-stats-inst-0-7** ■ **interest-table**

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show amon source-interface

```
show amon source-interface
```

Description

This command displays the source VLAN interface of AMON packets on the controller.

Syntax

No parameters.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays the source VLAN interface of the AMON feed:

```
(host) [mynode] #show amon source-interface
amon source-interface:vlan 501
```

Related Commands

Release	Modification
amon source-interface	Specifies the IPv4 address of the VLAN as the source IP address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show ap active

```
show ap active
   ap-name <ap-name> [details] [dot11a] [dot11g] [voip-only]
   arm-edge [details] [dot11a] [dot11g] [voip-only]
   counters [ap-name <ap-name>] [arm-edge] [dot11a] [dot11g] [essid <essid>] [ip-addr <ip-
   addr>] [ip6-addr <ip6-addr>] [type]
   details
   dot11a [details]
   dot11g [details]
   essid <essid>
   ip-addr <ip-addr> [details] [dot11a] [dot11g] [voip-only]
   ip6-addr <ip6-addr> [details] [dot11a] [dot11g] [voip-only]
   type {access-point [details] [dot11a] [dot11g] [voip-only]}|{air-monitor [details] [dot11a]
   [dot11g] [voip-only]}|{ap-monitor [details] [dot11a] [dot11g] [voip-only]}|{spectrum
   [details] [dot11a] [dot11g] [voip-only]}
   voip-only [details]
```

Description

This command shows Access Points registered to a Mobility Master.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows data for specified AP name.
`arm-edge`	Shows state of ARM edge Access Points.
`counters`	Shows counters.
`dot11a`	Shows 802.11a radio information.
`dot11g`	Shows 802.11g radio information.
`essid <essid>`	Shows data for specified ESSID.
`ip-addr <ip-addr>`	Shows data of an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows data of an AP for specified IPv6 address.
`type`	Shows information filtered by type of AP.
`access-point`	Shows information for Access Points only.
`air-monitor`	Shows information for Air Monitors only.
`ap-monitor`	Shows information for AP Monitors only.
`spectrum`	Shows spectrum sensor information.
`voip-only`	Shows information filtered by associated/active VoIP clients.

Usage Guidelines

This command shows Access Points registered to a Mobility Master. For the remaining parameters, see the command syntax.

Example

The following example shows Access Points registered to a Mobility Master:

```
(host) [mynode] #show ap active

Active AP Table
---------------
Name              Group   IP Address    AP Type   Flags   Uptime          Outer IP
----              -----   ----------    -------   -----   ------          --------
AP344-Pilot-NEW   AP344   172.16.0.2    344       RAaKW   4d:3h:37m:18s   172.16.0.200
AP225             AP225   172.16.0.58   225       A2aK    4d:3h:34m:2s    N/A
AP335             AP335   172.16.0.60   335       E2aK    4d:3h:35m:39s   N/A
AP345             AP345   172.16.0.22   345       E2aKW   4d:3h:36m:29s   N/A
AP207             AP207   172.16.0.23   207       2aKf    4d:3h:36m:8s    N/A
AP345-B0          AP345   172.16.0.55   345       ME2aK   4d:3h:36m:35s   N/A


Radio 0 Band Ch/EIRP/MaxEIRP/Clients  Radio 1 Band Ch/EIRP/MaxEIRP/Clients
------------------------------------  ------------------------------------
AP:5GHz-VHT:157E/18.0/31.7/0          AP:5GHz-VHT:36S/8.5/23.7/0
AP:5GHz-VHT:44E/18.0/30.2/0           AP:2.4GHz-HT:11/7.0/25.0/0
AP:5GHz-VHT:36E/12.0/28.5/0           AP:2.4GHz-HT:1/12.0/25.0/0
AP:5GHz-VHT:161E/18.0/31.7/0          AP:5GHz-VHT:36S/20.0/0.0/0
AP:5GHz-VHT:48E/18.0/29.0/0           AP:2.4GHz-HT:11/6.0/23.7/0
AP:5GHz-VHT:149E/12.0/31.7/4          MPP+AP:2.4GHz-HT:6/10.2/26.0/0

Flags: 1 = 802.1x authenticated AP; 2 = Using IKE version 2;
   A = Enet1 in active/standby mode;  B = Battery Boost On; C = Cellular;
   D = Disconn. Extra Calls On; E = Wired AP enabled; F = AP failed 802.1x authentication;
   H = Hotspot Enabled; K = 802.11K Enabled; L = Client Balancing Enabled; M = Mesh;
   N = 802.11b protection disabled; P = PPPOE; R = Remote AP;
   S = AP connected as standby; X = Maintenance Mode;
   a = Reduce ARP packets in the air; d = Drop Mcast/Bcast On; u = Custom-Cert RAP;
   i = Provisioned as Indoor; o = Provisioned as Outdoor;
   r = 802.11r Enabled; f = No Spectrum FFT support;
   Q = DFS CAC timer running; T = Flex Radio Mode is 2.4GHz+5GHz;
   U = Flex Radio Mode is 5GHz; V = Flex Radio Mode is 2.4GHz; e = custom EST cert; W = Dual
   5GHz Mode Enabled

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Channel flags: +/- = 40 MHz, E = 80 MHz, S = 160 MHz, E+E = 80 + 80 MHz (i.e. 36E+149E)

Num APs:6
```

In releases prior to ArubaOS 8.3.0.0, the output of this command included 2.4 GHz and 5 GHz as output parameters. In ArubaOS 8.3.0.0, these output parameters are modified to display the radio IDs, bands, EIRP, Maximum EIRP, and number of clients.

The output of this command includes the following information:

Column	Description
Name	Name of an AP
Group	The AP is associated with this AP group.

Column	Description
`IP address`	IP address of the AP, in dotted decimal format.
`AP Type`	AP model type.
`Flags`	This column displays any flags for this AP. The list of flag abbreviations is also included in the output of the **show ap active** command. ■ 1 = 802.1X authenticated AP ■ 2 = Using IKE version 2; ■ A = Enet1 in active/standby mode ■ B = Battery Boost On ■ C = Cellular; ■ D = Disconn. Extra Calls On ■ E = Wired AP enabled ■ F = AP failed 802.1X authentication ■ H = Hotspot Enabled ■ K = 802.11K Enabled ■ L = Client Balancing Enabled ■ M = Mesh ■ N = 802.11b protection disabled ■ P = PPPOE ■ R = Remote AP ■ S = AP connected as standby ■ X = Maintenance Mode ■ a = Reduce ARP packets in the air ■ d = Drop Mcast/Bcast On ■ u = Custom-Cert RAP ■ i = Provisioned as indoor ■ o = Provisioned as outdoor ■ r = 802.11r Enabled ■ Q = DFS CAC timer running ■ T = Flex Radio Mode is 2.4GHz+5GHz ■ U = Flex Radio Mode is 5GHz ■ V = Flex Radio Mode is 2.4GHz ■ W = Dual 5 GHz Mode Enabled
`Uptime`	Number of hours, minutes and seconds since the last Mobility Master reboot or bootstrap, in the format *hours:minutes:seconds*.
`Outer IP`	The outer IP address of a Remote AP is used to establish an IPsec VPN tunnel to the terminating Mobility Master. The RAP acquires an outer IP address from the locally connected network, usually via DHCP. (A Remote AP is typically behind a NAT device whose public IP is seen as the outer IP for the Remote AP).
`Radio 0 Band Ch/EIRP/MaxEIRP/Clients`	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 0.
`Radio 1 Band Ch/EIRP/MaxEIRP/Clients`	Radio ID, channel, EIRP, Maximum EIRP, and the number of clients using Radio 1.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.3.0.0	New flags, **T**, **U**, **V**, and **W** were introduced. In addition, the output parameters for this command were modified to show the radio ID (that is, Radio 0 and Radio 1), radio band, and the debug details such as APs' operation mode for the dual 5GHz mode settings.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show ap-group

```
show ap-group [default|NoAuthApGroup|<profile-name>]
```

Description

This command shows configuration for an AP group.

Syntax

Parameter	Description
`default`	Shows setting for default AP group.
`NoAuthApGroup`	Shows setting for NoAuthAP group.
`<profile-name>`	Shows setting for specified AP group.

Usage Guidelines

Issue this command without the optional parameters to display the entire AP group list, including profile status for each profile. Include an AP group name to display detailed configuration for that AP group.

Example

The following example shows the AP group list:

```
(host) [mynode] #show ap-group

AP group List
-------------
Name            Profile Status
----            --------------
default
NoAuthApGroup   Predefined (changed)

Total:2
```

The following example shows the configuration of an AP group named **default**:

```
(host) [mynode] #show ap-group default

AP group "default"
------------------
Parameter                                 Value     Set
---------                                 -----     ---
Virtual AP                                N/A
802.11a radio profile                     default
802.11g radio profile                     default
Ethernet interface 0 port configuration   default
Ethernet interface 1 port configuration   default
Ethernet interface 2 port configuration   shutdown
Ethernet interface 3 port configuration   shutdown
Ethernet interface 4 port configuration   shutdown
AP system profile                         default
AP multizone profile                      default
802.11a Traffic Management profile        N/A
802.11g Traffic Management profile        N/A
Regulatory Domain profile                 default
```

```
RF Optimization profile                  default
RF Event Thresholds profile              default
IDS profile                              default
Mesh Radio profile                       default
Mesh Cluster profile                     N/A
AM filter profile                        default
Provisioning profile                     N/A
AP authorization profile                 N/A
```

The output of this command includes the following parameters:

Parameter	Description
Virtual AP	Virtual AP profile that which configures a specified WLAN.
802.11a radio profile	Profile that defines 802.11a radio settings for the AP group.
802.11g radio profile	Profile that defines 802.11g radio settings for the AP group.
Wired AP profile	Profile that defines wired port settings for APs assigned to the AP group.
Ethernet interface 0 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
Ethernet interface 1 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
AP system profile	Name of the AP system profile for the AP group.
802.11a Traffic Management profile	Name of the 802.11a WLAN traffic management profile for the AP group.
802.11g Traffic Management profile	Name of the 802.11g WLAN traffic management profile for the AP group.
Regulatory Domain profile	Name of the regulatory domain profile for the AP group.
SNMP profile	Name of the SNMP profile for the AP group.
RF Optimization profile	Name of the RF optimization profile for the AP group.
RF Event Thresholds profile	Name of the RF event thresholds profile for the AP group.
IDS profile	IDS profile for the AP group.
Mesh Radio profile	Mesh radio profile assigned to the AP group.
Mesh Cluster profile	Mesh cluster profile assigned to the AP group.

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap-name

```
show ap-name [<profile-name>]
```

Description

This command shows the list of AP names.

Syntax

Parameter	Description
[<profile-name>]	Shows detailed configuration information for the specified AP name.

Usage Guidelines

Issue this command without the optional parameter to show the list of AP names. Include <profile-name> to show detailed configuration information for that AP name.

Example

The following example shows the AP name list:

```
(host) [mynode] #show ap-name

AP name List
------------
Name  Profile Status
----  --------------
corp1

Total:1
```

The following example shows the configuration settings for an AP named corp1:

```
(host) [mynode] #show ap-name corp1

AP name "corp1"
-------------
Parameter                                       Value
---------                                       -----
Virtual AP                                      N/A
802.11a radio profile                           default
802.11g radio profile                           default
Ethernet interface 0 port configuration         default
Ethernet interface 1 port configuration         default
Ethernet interface 2 port configuration         shutdown
Ethernet interface 3 port configuration         shutdown
Ethernet interface 4 port configuration         shutdown
AP system profile                               default
AP multizone profile                            default
802.11a Traffic Management profile              N/A
802.11g Traffic Management profile              N/A
Regulatory Domain profile                       default
RF Optimization profile                         default
RF Event Thresholds profile                     default
IDS profile                                     default
Mesh Radio profile                              default
Mesh Cluster profile                            N/A
```

```
AM filter profile                              default
Provisioning profile                           N/A
AP authorization profile                       N/A
```

The output of this command includes the following parameters:

Parameter	Description
Virtual AP	Virtual AP profile that which configures a specified WLAN.
Excluded Virtual AP	Excludes the specified mesh cluster profile from this AP.
802.11a radio profile	Profile that defines 802.11a radio settings for the AP.
802.11g radio profile	Profile that defines 802.11g radio settings for the AP.
Wired AP profile	Profile that defines wired port settings for APs assigned to the AP.
Ethernet interface 0 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
Ethernet interface 1 link profile	Profile that defines the duplex and speed of the Ethernet 0 interface on the AP.
AP system profile	Name of the AP system profile for the AP.
802.11a Traffic Management profile	Name of the 802.11a WLAN traffic management profile for the AP group.
802.11g Traffic Management profile	Name of the 802.11g WLAN traffic management profile for the AP.
Regulatory Domain profile	Name of the regulatory domain profile for the AP.
RF Optimization profile	Name of the RF optimization profile for the AP.
RF Event Thresholds profile	Name of the RF event thresholds profile for the AP.
IDS profile	IDS profile for the AP.
Mesh Radio profile	Mesh radio profile assigned to the AP.
Mesh Cluster profile	Mesh cluster profile assigned to the AP.
Excluded Mesh Cluster profile	Excludes the specified mesh cluster profile from this AP.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap allowed-channels

```
show ap allowed-channels
   ap-name <ap-name>
   country-code <country-code> [ap-type <ap-type>]
   ip-addr <ip-addr>
```

Description

This command shows the allowed channels on a specific AP name, country code, or IP address.

Syntax

Parameter	Description
`ap-name <ap-name>`	Specifies name of an AP.
`country-code <country-code> [ap-type <ap-type>]`	Specifies country code. If you specify the optional **ap-type <ap-type>** parameter, the output shows allowed channels for the specified AP type in that country code. The **<ap-type>** parameter is the two or three digit model number of the AP, such as **135** for AP-135 or **225** for AP-225**.** For remote APs, like RAP-3WN, specify the prefix RAP- before the AP model number. If the AP model number includes an alphabetic suffix, such as the AP-175AC, specify the suffix after the model number. Note that the suffix may be case-sensitive.
`<ip-addr>`	Specifies the IP address of an AP.

Usage Guidelines

Specify the country code for your controller during initial setup. Changing the country code causes the valid channel lists to be reset to the defaults for that country.

Examples

The following command shows all allowed channels for the country code **US.**

```
(host) [mynode]# show ap allowed-channels US

Allowed Channels for Country Code "US" Country "United States"
--------------------------------------------------------------
PHY Type                 Allowed Channels
--------                 ----------------
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
144 149 153 157 161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140
144 149 153 157 161 165
802.11g 40MHz (indoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 116-120 124-128 132-136 140-
144 149-153 157-161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  36-40 44-48 52-56 60-64 100-104 108-112 116-120 124-128 132-136 140-
144 149-153 157-161
802.11a 80MHz (indoor)   36-48 52-64 100-112 116-128 132-144 149-161
```

```
802.11a 80MHz (outdoor)  36-48 52-64 100-112 116-128 132-144 149-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 144
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap allowed-max-eirp

```
show ap allowed-max-EIRP {ap-name <ap-name>}|{ip-addr <ip-addr>}
```

Description

The output of this command shows the regulatory power limits per channel for a specified AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the maximum EIRP setting per country per AP type for specified AP name.
`ip-addr <ip-addr>`	Shows the maximum EIRP setting per country per AP type for specified IP address.

Usage Guidelines

The values showed in the output of this command include the antenna gain for that device, regardless of whether the AP antenna is internal or external. MIMO gain (if applicable) is also accounted for in the maximum EIRP limits.

Examples

The output of this example shows the allowed per-channel EIRP maximums for an AP-325. In the following example, the output is divided into two parts to better fit on the pages of this document. In the ArubaOS CLI, the output appears in a single, long table.

```
(host)# show ap allowed-max-eirp ap-name local-ap-325

Max EIRP setting for AP-325
---------------------------
Channel  1   2   3   4   5   6   7   8   9   10  11  12  13  14  36  40  44  48  52  56  60
-------  -   -   -   -   -   -   -   -   -   --  --  --  --  --  --  --  --  --  --  --  --
b        19  19  19  19  19  19  19  19  19  19  19  19  19  *   *   *   *   *   *   *   *
g/a      19  19  19  19  19  19  19  19  19  19  19  19  19  *   22  22  22  22  22  22  22
HT 20    19  19  19  19  19  19  19  19  19  19  19  19  19  *   22  22  22  22  22  22  22
HT 40    19  19  19  19  19  19  19  19  19  19  19  19  19  *   22  22  22  22  22  22  22
VHT 80   *   *   *   *   *   *   *   *   *   *   *   *   *   *   22  22  22  22  22  22  22

64  100  104  108  112  116  120  124  128  132  136  140  144  149  153  157  161  16
--  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  --
*   *    *    *    *    *    *    *    *    *    *    *    *    *    *    *    *    *
22  *    *    *    *    *    *    *    *    *    *    *    *    22   22   22   22   22
22  *    *    *    *    *    *    *    *    *    *    *    *    22   22   22   22   22
22  *    *    *    *    *    *    *    *    *    *    *    *    22   22   22   22   22
22  *    *    *    *    *    *    *    *    *    *    *    *    22   22   22   22   22
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap am-filter-profile

```
show ap am-filter-profile
   default
   <profile-name>
```

Description

This command shows the AM filter for an AP.

Syntax

Parameter	Description	Range	Default
<profile-name>	Shows AM filter for specified profile name.	–	–

Usage Guidelines

This command shows the AM filter for an AP. For the remaining parameters, see the command syntax.

Example

The following example shows the AM filter for an AP:

```
(host) [mynode] #show ap am-filter-profile

AM Filter List
--------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1
```

The following example shows the AM filter for a default AP:

```
(host) [mynode] #show ap am-filter-profile default

AM Filter "default"
-------------------
Parameter               Value     Set
---------               -----     ---
Filtering               Disabled
Allow AP's Group        Disabled
Allow Frames from Self  Disabled
Allowed AP Group        N/A
Allowed AP              N/A
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap ap-cert-mgr

```
show ap ap-cert-mgr
log {ap-name <ap-name>[<page>]|ip-addr <ip-addr>[<page>]}
```

Description

This command displays the contents of the debug log file for an AP.

Syntax

Parameter	Description
`log`	Show debug log for an AP.
`ap-name <ap-name>|ip-addr <ip-addr>`	Specify name or IP address of the AP .
`<page>`	Specify page number of the log file.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays the debug logs for an AP.

```
(host) [mynode] ##show ap ap-cert-mgr log ip-addr 192.168.1.25
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap ap-group

```
show ap ap-group {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show the AP group settings for an individual AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Usage Guidelines

Use this command to display the contents of an AP's group profile. If you know the name of the group whose profile settings you want to view, use the command **show ap-group <profile-name>**. To view a list of all configured AP groups on your Mobility Master, use the command **show ap-group**.

Examples

In the example below, the output of this command lists the profiles associated with the AP group **Corp13**.

```
(host) [mynode] #show ap ap-group AP2

AP group "corp13"
-------------------
Parameter                                 Value
---------                                 -----
Virtual AP                                N/A
802.11a radio profile                     default
802.11g radio profile                     default
Ethernet interface 0 port configuration   default
Ethernet interface 1 port configuration   default
Ethernet interface 2 port configuration   shutdown
Ethernet interface 3 port configuration   shutdown
Ethernet interface 4 port configuration   shutdown
AP system profile                         default
AP multizone profile                      default
802.11a Traffic Management profile        N/A
802.11g Traffic Management profile        N/A
Regulatory Domain profile                 default
RF Optimization profile                   default
RF Event Thresholds profile               default
IDS profile                               default
Mesh Radio profile                        default
Mesh Cluster profile                      N/A
AM filter profile                         default
Provisioning profile                      N/A
AP authorization profile                  N/A
```

Related Commands

Command	Description
ap-group	Configure your AP groups and AP group profiles.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm client-match debug state

```
show ap arm client-match debug state
   {bssid <bssid>|client-mac <client-mac>|radio-bssid <radio-bssid>}
```

Description

If the Client Match feature is enabled, the output of this command displays the debug information for internal state of objects.

Syntax

Parameter	Description
`bssid <bssid>`	The BSSID for VAPs.
`client-mac <client-mac>`	The MAC address for stations.
`radio-bssid <radio-bssid>`	The BSSID for radios.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host)#show ap arm client-match debug state bssid 00:1a:1e:aa:bb:cc
```

Related Commands

Use the following command to enable the client match feature:

- rf arm-profile client-match

The following commands display additional statistics for the client match feature:

- show ap arm client-match probe-report
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary
- show ap arm client-match history

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm client-match history

```
show ap arm client-match history
   advanced
   client-mac <macaddr>
```

Description

If the client match feature is enabled, the output of this command shows the history of AP association changes triggered by the client match feature.

Syntax

Parameter	Description
`advanced`	Provides additional client-match history information, including: ■ **Eff_Signal** ■ **EIRP** ■ **ESSID**
`client-mac <macaddr>`	MAC address of a client for which you want to view a history of AP association changes triggered by the client match feature.

Example

The following command displays information on the Client Match history.

```
(AP-7010) # show ap arm client-match history

S: Source, T: Target, A: Actual, As: Actual Assoc req sig
Unit of Roam Time: second
Unit of Signal: dBm

ARM Client match History
------------------------
Time of Change       Station            Reason      Status/Roam Time/Mode Signal(S/T/A/As)
Band(S/T/A)  Radio Bssid(S/T/A)                                  AP Name(S/T/A)
-------------       -------            ------      -------------------- -------------  -----
------  ------------------                                 --------------
2014-08-13 14:41:20  84:38:38:20:df:68  User-action Success/0/11v-BTM     -0/-0/-0
5G/5G/5G     d8:c7:c8:46:e0:10/6c:f3:7f:e7:1d:30/6c:f3:7f:e7:1d:30  ap135/ac/ac
```

The output of this command includes the following parameters:

Parameter	Description
`Time of Change`	Timestamp showing the date and time the client match feature associated the client to a different AP radio.
`Station`	The station MAC address.

Parameter	Description
Reason	Reason why the client match feature made the change. Possible reasons include: ■ **Sticky**: A mobile roaming client was staying associated (sticking) to a sub-optimal AP for too long. ■ **Band steer**: A dual-band capable client was steered toward a 5Ghz radio on a dual-band AP. ■ **Band Balance**: A dual-band capable client was steered toward a different radio to balance the load between the two radios on a single AP. ■ **Load Balance**: Client match moved the client to a different AP, based upon the load on APs in the client's RF neighborhood, and the SNR levels the client detected from each underutilized AP.
Status/Roam Time/Mode	The status, roam time, and mode of client steering using Client Match.
Signal (S/T/A/As)	The output of this column shows the following values: ■ S: Radio signal strength of the source AP ■ T: Radio signal strength of the target AP ■ A: Radio signal strength of the AP that the client is actually associated to ■ AS : Radio signal strength of the target AP at steer completion
Band (S/T/A)	The output of this column shows the following values: ■ S: Radio frequency band of the source AP (e.g. 2.4GHz and 5GHz) ■ T: Radio frequency band of the target AP ■ A: Radio frequency band of the AP that the client is actually associated to
Radio BSSID (S/T/A)	The output of this column shows the following values: ■ S: MAC address of the source AP radio ■ T: MAC address of the target AP radio ■ A: MAC address of the AP radio that the client is actually associated to
AP Name (S/T/A)	The output of this column shows the following values: ■ S: Name of the source AP ■ T: Name of the target AP ■ A: Name of the AP that the client is actually associated to

The advanced command provides additional information on the Client Match history.

```
(host) #show ap arm client-match history advanced

S: Source, T: Target, A: Actual, As: Actual Assoc req sig
Unit of Roam Time: second
Unit of Eff_Signal, Signal, EIRP: dBm

ARM Client match History
------------------------
Time of Change       Station            Reason       Status/Roam Time    Eff_Signal(S/T/A/As)
Signal(S/T/A/As)  EIRP(S/T/A)  Band(S/T/A)              Radio Bssid(S/T/A)
                 AP Name(S/T/A)     Essid(S/A)
--------------       -------            ------       ----------------    ------------------  --
-----------  -----------  -----------               ------------------
            --------------     ----------
2014-05-13 16:30:08  f8:f1:b6:03:0d:ff  Band-steer   Success/1           -35/-50/-50        -
35/-50/-50    21/21/21     2.4G/5G/5G
6c:f3:7f:e7:2d:40/6c:f3:7f:e7:2d:50/6c:f3:7f:e7:2d:50  ap225/ap225/ap225  jxie2/jxie2
```

The output of this command includes the following additional parameters:

Parameter	Description
`Eff_Signal (S/T/A)`	The output of this column shows the following values: ■ S: The relative received signal strength indicator (RSSI) of the source AP radio. This value is derived from the transmit power of the source AP radio and received power from the client. ■ T: The relative RSSI of the target AP radio. This value is derived from the transmit power of the target AP radio and received power from the client. ■ A: The relative RSSI of the AP radio that the client is actually associated to. This value is derived from the transmit power of the AP radio and received power from the client.
`EIRP (S/T/A)`	The output of this column shows the following values: ■ S: The amount of power transmitted from an antennae in the source AP ■ T: The amount of power transmitted from an antennae in the target AP ■ A: The amount of power transmitted from an antennae in the AP that the client is actually associated to
`Essid (S/A)`	The output of this column shows the following values: ■ S: The identifying name of the source wireless network ■ A: The identifying name of the wireless network the client is actually associated to

Related Commands

Use the following command to enable the client match feature:

- rf arm-profile client-match

The following commands display statistics for the client match feature:

- show ap arm client-match probe-report
- show ap arm client-match neighbors
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.3.0.0	A new output value, **AS** was introduced for the **Signal** output column.

Command Information

Platforms	Licensing	Command Mode
All platforms	base operating system	Enable or Config mode on Mobility Master

show ap arm client-match neighbors

```
show ap arm client-match neighbors
   ap-name <name>
   ip-addr <ipaddr>
   ip6-addr <ipaddr>
```

Description

If the client match feature is enabled, the output of this command displays the BSSID of other APs seen by clients in the select AP's RF neighborhood.

Syntax

Parameter	Description
`ap-name <name>`	View neighboring clients for an AP with a specified name
`ip-addr <ipaddr>`	View neighboring clients for an AP with a specified IP address.
`ipv6-addr <ipaddr>`	View neighboring clients for an AP with a specified IPv6 address.

Usage Guidelines

Issue this command to view a list of other APs seen by clients currently associated to the selected AP.

Example

The example below indicates that the clients currently associated to the AP can detect signals from three other APs.

```
(host)#show ap arm client-match neighbors ap-name <ap-name>

Client View
------------
BSSID              Channel
-----              -------
d8:c7:c8:37:84:70  132
d8:c7:c8:88:b6:50  132
d8:c7:c8:37:84:10  124
Num Neighbors:3
```

The output of this command includes the following parameters:

Parameter	Description
`Client MAC`	AP name of the AP from which the client can detect a signal.
`Signal`	Signal strength, in dBm, of the probe request received from Client
`Assoc`	A "Y" in this field indicates that the client is currently associated to that AP radio.
`Sec since last heard`	Time elapsed since the AP radio heard from the client.

Parameter	Description
`Sec since last reported`	Time elapsed since the AP radio heard from the client.
`Last heard`	Date and time at which the AP last heard from the client

Related Commands

Use the following command to enable the client match feature:

- rf arm-profile client-match

The following commands display additional statistics for the client match feature:

- show ap arm client-match probe-report
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary
- show ap arm client-match history

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm client-match probe-report

```
show ap arm client-match probe-report
   ap-name <name>
   ip-addr <ipaddr>
   ip6-addr <ip6-addr>
   assoc
   phy-type 802.11a|802.11b|80211g
```

Description

If ClientMatch is enabled, the output of this command displays the client probe report for the specified AP.

Syntax

Parameter	Description
`ap-name <name>`	Name of the AP for which you want to view a client report.
`ip-addr <ip-addr>`	IPv4 address of an AP for which you want to view a client probe report.
`ip6-addr <ip6-addr>`	IPv6 address of an AP for which you want to view a client probe report.
`assoc`	Show information for associated clients only.
`phy-type`	Show information for one of the following phy types: ■ 802.11a ■ 802.11b ■ 80211g

Usage Guidelines

APs using ClientMatch maintain a table of clients that have sent probe requests, and the signal-to-noise ratio (SNR) of the frame the AP received from the client. The AP sends these reports to the managed device every 30 seconds, and the managed device uses the information in these reports to steer each client to its optimal AP.

Example

```
(host)#show ap arm client-match probe-report ap-name <ap-name>

AP Client Probe Report for Wifi0
--------------------------------
Client MAC         Signal  Assoc  Sec since    Sec since       Last heard
                                  last heard   last reported
----------         ------  -----  ------------ ----------     ----------
00:24:d7:40:ca:88  15      0      49           10             Wed Apr 10 01:20:46 2013
00:26:c6:4d:2b:74  21      0      23           10             Wed Apr 10 01:21:12 2013
00:1e:65:2b:7a:3e  23      0      55           10             Wed Apr 10 01:20:40 2013
74:e5:43:4b:3b:ff  34      0      20           10             Wed Apr 10 01:21:15 2013
AP Client Probe Report for Wifi1
--------------------------------
Client MAC         Signal  Assoc  Sec since    Sec since      Last heard
            last heard   last reported
----------         ------  -----  ------------ -------------- ----------
22:33:44:55:66:77  50      0      6            9              Wed Apr 10 01:21:29 2013
c8:f7:33:29:82:db  41      0      60           9              Wed Apr 10 01:20:35 2013
ac:81:12:59:5c:12  32      0      50           9              Wed Apr 10 01:20:45 2013
00:24:d7:40:bb:b0  31      0      58           9              Wed Apr 10 01:20:37 2013
```

```
00:1a:73:15:8c:5f  32      0      57           9             Wed Apr 10 01:20:38 2013
```

The output of this command includes the following parameters:

Parameter	Description
`Client MAC`	AP name of the AP from which the client can detect a signal.
`Signal`	Signal strength, in dBm, of the probe request received from the client.
`Assoc`	A "Y" in this field indicates that the client is currently associated to that AP radio.
`Sec since last heard`	Time elapsed since the AP radio heard from the client.
`Sec since last reported`	Time elapsed since the AP radio heard from the client.
`Last heard`	Date and time at which the AP last heard from the client

Related Commands

Use the following command to enable ClientMatch:

- rf arm-profile client-match

The following commands display additional statistics for ClientMatch:

- show ap arm client-match neighbors
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary
- show ap arm client-match history

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm client-match restriction-table

```
show ap arm client-match restriction-table
   ap-name <name>
   ip-addr <ipaddr>
   ip6-addr <ip6-addr>
```

Description

If ClientMatch is enabled, the output of this command displays the list of clients that ClientMatch has restricted from the specified AP.

Syntax

Parameter	Description
`ap-name <name>`	Name of the AP for which you want to view the list of restricted clients
`ip-addr <ipaddr>`	IPv4 address of the AP for which you want to view the list of restricted clients
`ip6-addr <ipaddr>`	IPv6 address of the AP for which you want to view the list of restricted clients

Usage Guidelines

If ClientMatch is enabled, the managed devices send APs a list of clients that should not be allowed to associate to that AP. These lists of restricted clients help the client associate to the best AP, by preventing the client from associating with a sub-optional AP radio. The output of this command shows a list of all clients that were ever blacklisted from the specified AP.

Example

```
(host)[node] #show ap arm client-match restriction-table ap-name <ap-name>

   Client Restriction Table for Wifi0
   ----------------------------------
   Client MAC         Time last restricted     Restricted(Cur/Last)
   ----------         --------------------     --------------------
   24:77:03:32:88:ec  Wed Apr 10 03:51:00 2014  0

   PS deauth  Probe(home/scan/bc_ssid)  Auth(home/scan)
   ---------  ------------------------  ---------------
   -          2/0/no                    4/0

   Time since last restriction(sec)  Radio Bssid
   --------------------------------  -----------
   18603                             00:1a:1e:89:c0:d0

   Client Restriction Table for Wifi1
   ----------------------------------
   Client MAC         Time last restricted    Restricted(Cur/Last)
   ----------         --------------------    --------------------
   24:77:03:32:7b:cc  Wed Apr 10 03:47:16 2014  0

   PS deauth  Probe(home/scan/bc_ssid)  Auth(home/scan)
   ---------  ------------------------  ---------------
   0/0/no     0/0/no                    0/0
```

```
Time since last restriction(sec)  Radio Bssid
--------------------------------  -----------
3866                              00:1a:1e:89:c0:c0
```

The output of this command includes the following parameters:

Parameter	Description
`Client MAC`	Displays the MAC address of the client that Client Match is attempting to steer.
`Time last restricted`	Displays the date and time at which the client was last steered in the vicinity of this radio.
`Restricted(Cur/Last)`	A "1" in this field indicates that the client is currently in the process of being steered to another radio.
`PS deauth`	Displays if the client is in power save mode when client match is attempting to steer the client.
`Probe(home/scan/bc_ssid)`	Displays the number of probe requests received on home channel, AP scanning, and SSID broadcast probe.
`Auth(home/scan)`	Displays the number of probe requests received on home channel and AP scanning for 802.11 authentication frames.
`Time since last restricted`	Display the time (in seconds) since the client was last steered in the vicinity of this radio.
`Radio Bssid`	Displays the unique hard-wireless MAC address of the AP. A unique BSSID applies to each frequency– 802.11a and 802.11g–used from the AP.

Related Commands

Use the following command to enable ClientMatch

- rf arm-profile client-match

The following commands display additional statistics for ClientMatch

- show ap arm client-match probe-report
- show ap arm client-match neighbors
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary
- show ap arm client-match history

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm client-match summary

```
show ap arm client-match summary [client-mac <macaddr>]|[advanced]|[brief]
```

Description

If the client match feature is enabled, the output of this command shows the history of AP association changes triggered by the client match feature.

Syntax

Parameter	Description
`client-mac <macaddr>`	MAC address of a client for which you want to view a history of AP association changes triggered by the client match feature.
`advanced`	Displays advanced debugging information. Include this parameter only under the supervision of Aruba support.
`brief`	Displays brief statistical information containing the final calculated data of the output parameters.

Example

The following command displays information on the Client Match summary.

```
((host) [mynode](config) #show ap arm client-match summary

SM: Sticky Moves, BM: Bandsteer Moves, LM: Load Balance Moves, MU: MUsteer Moves, VoM: Voice
Roam Moves
T: Total, S: Success
ACC: Accept, REJ#: Reject with reason #, TO: Timeout FA: False Accept
11v Move Format: (T/ACC/REJ1/REJ2/REJ3/REJ4/REJ5/REJ6/REJ7/REJ8/TO/FA)
Client Match Summary
---------------------
MAC                 SM (T/S)   LM (T/S)   BM (T/S)   MU (T/S)   VoM (T/S)   Moves (T/S)   Last Move
(Time/Rsn/Dur))           Device Type  11v Moves
---                 --------   --------   --------   --------   ---------   -----------   -----------
--------------          -----------  ---------
ac:fd:ce:5e:af:a6  24/22      0/0        0/0        0/0        0/0         24/22         Feb 24
17:15:30 2018/Sticky/0      Linux         24/23/0/0/0/0/0/0/0/0/1/0
00:04:20:2c:22:7a  37/36      0/0        0/0        0/0        0/0         37/36         Mar  6
03:22:00 2018/Sticky/0      Linux         0/0/0/0/0/0/0/0/0/0/0/0
00:04:20:2c:76:62  3/3        0/0        0/0        0/0        0/0         3/3           Feb 28
17:30:35 2018/Sticky/0      Unknown       0/0/0/0/0/0/0/0/0/0/0/0
00:04:20:2b:fe:6f  13/13      0/0        0/0        0/0        0/0         13/13         Mar  4
15:12:54 2018/Sticky/0      Unknown       0/0/0/0/0/0/0/0/0/0/0/0
58:94:6b:57:31:cc  4/4        0/0        1/1        0/0        0/0         5/5           Mar  3
22:50:13 2018/Band-steer/4  Unknown       0/0/0/0/0/0/0/0/0/0/0/0
11v Move Format: (T/ACC/REJ1/REJ2/REJ3/REJ4/REJ5/REJ6/REJ7/REJ8/TO/FA)
```

The output of this command includes the following parameters:

Parameter	Description
`MAC`	MAC address of the client that was moved to a different AP radio.

Parameter	Description
SM (T/S) Sticky Moves	The output of this column shows the following two values: ■ T: Total number of times the client match feature attempted to move a mobile roaming client because it was staying associated (sticking) to a sub-optimal AP. ■ S: Number of times the client match successfully moved a mobile roaming client because it was staying associated (sticking) to a sub-optimal AP.
LM (T/S) Load Balance Moves	The output of this column shows the following two values: ■ T: Total number of times the client match feature attempted to move an AP to a different radio on dual-radio AP to balance the client load between the AP radios. ■ S: Number of times the client match feature successfully moved an AP to a different radio on dual-radio AP to balance the client load between the AP radios.
BM (T/S) Bandsteer Moves	The output of this column shows the following two values: ■ T: Total number of times the client match feature attempted to steer a dual-band client to a 5GHz radio. ■ S: Number of times the client match feature successfully moved a dual-band client to a 5GHz radio.
MU (T/S) MU steer Moves	The output of this column shows the following two values: ■ T: Total number of times the Client Match feature attempted to steer and align MU-MIMO-capable clients with MU-MIMO-capable radios. ■ S: Number of times the client match feature successfully moved an AP to a different radio.
VoM (T/S) Voice Roam Moves	The output of this column shows the following two values: ■ T: Total number of times the client match feature attempted to move a voice client roaming from one AP BSS to another AP BSS using the same SSID. ■ S: Number of times the client match feature successfully moved a roaming voice client roaming from one AP BSS to another using AP BSS the same SSID.
Moves(T/S)	The output of this column shows the following two values: ■ T: Total number of times the client match feature attempted to move an AP to a different radio. ■ S: Number of times the client match feature successfully moved an AP to a different radio.
Last Move	This column shows the date and time the client was steered to a different AP radio, the reason why the client match feature made the change, and the number of seconds it took for the change to take place. Possible reasons include: ■ **Sticky**: A mobile roaming client was staying associated (sticking) to a sub-optimal AP for too long. ■ **Band steer**: A dual-band capable client was steered toward a 5Ghz radio on a dual-band AP. ■ **Band Balance**: A dual-band capable client was steered toward a different radio to balance the load between the two radios on a single AP. ■ **Load Balance**: Client match moved the client to a different AP, based upon the load on APs in the client's RF neighborhood, and the SNR levels the client detected from each underutilized AP. ■ **VHT Steer:** A client was steered to a very-high-throughput radio that supports 802.11ac.
Device type	Type of client, if the value can be determined.

Parameter	Description
`11v Moves (T/ACC/REJ1/REJ2/REJ3/REJ4 /REJ5/REJ6/REJ7/REJ8/TO/FA)`	The output of this column shows the following values: ■ T: Total number of times the client match feature attempted to move an AP to a different radio using the 802.11v BSS transition management request. ■ ACC: Number of times a client returned a 802.11v accept message. ■ REJ1: Move Rejected; unspecified reject reason ■ REJ2: Move Rejected; Insufficient Beacons ■ REJ3: Move Rejected; Insufficient capacity ■ REJ4: Move Rejected; BSS Termination undesired ■ REJ5: Move Rejected; BSS Termination Delay requested ■ REJ6:Move Rejected; STA BSS Trans List provided ■ REJ7: Move Rejected; No Suitable candidate ■ REJ8: Move Rejected; Leaving ESS ■ TO: Number of times the dot11v BSS transition management request timed out because the client failed to acknowledge the 802.11v BSS transition management request from the AP. ■ FA: Number of false accepts, where the client responds to a move request with an accept message, but fails to move to the destination radio and remains on the same radio.

Related Commands

Use the following command to enable the client match feature:

- rf arm-profile client-match

The following commands display additional statistics for the client match feature:

- show ap arm client-match probe-report
- show ap arm client-match neighbors
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match history

Command History

Command	Description
ArubaOS 8.3.0.0	A new parameter, **brief**, was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	base operating system	Enable or Config mode on Mobility Master

show ap arm client-match unsupported

```
show ap arm client-match unsupported
```

Description

If the client match feature is enabled, the output of this command displays a list of clients that failed to be steered to a more optimal AP, and the reason the initial steering request was triggered,.

Syntax

No parameters.

Usage Guidelines

The controller also keeps track of the number of times the client match feature failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If the client match feature attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as unsteerable for that specific trigger.

Example

```
(host) #show ap arm client-match unsupported

Client Match Unsteerable Clients
--------------------------------
MAC  Unsteerable Flags  Last Steer Time  Expiry Time                    Total
steers/successful
---  -----------------  ---------------  -----------                    ---------------------
--
S: Sticky L: Load Balance V: VHT steer B: Bandsteer I: IOS T: Temporary

Total Unsteerable Clients:0
```

The output of this command includes the following parameters:

Parameter	Description
MAC	MAC address of the client that could not be steered to a different AP radio.
Unsteerable Flags	The client is marked unsteerable under specific client steer triggers. These triggers include: ■ **Sticky:** A mobile roaming client was staying associated (sticking) to a sub-optimal AP for too long. ■ **Band steer:** A dual-band capable client was steered toward a 5GHz radio on a dual-band AP. ■ **Load Balance:** Client match moved the client to a different AP, based upon the load on APs in the client's RF neighborhood, and the SNR levels the client detected. from each underutilized AP. ■ **IOS:** An IOS device is temporarily prevented from steering to avoid blacklisting the ESS. ■ **Temporary:** A client is temporarily prevented from steering after undergoing a successful band steer, then reverting back to a 2.4GHz radio.
Last Steer Time	Timestamp showing the date and time the client match feature failed to associate the client to a different AP radio.

Parameter	Description
`Expiry Time`	The amount of time before a client steer attempt expires.
`Total steers/successful`	The total number of client steer attempts, and the number of successful client steer attempts.

Related Commands

Use the following commands to enable the client match feature:

- rf arm-profile client-match

The following commands display additional statistics for the client match feature:

- show ap arm client-match probe-report
- show ap arm client-match neighbors
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary
- show ap arm client-match history

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	base operating system	Enable or Config mode on Mobility Master

show ap arm history

```
show ap arm history {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

For each interface on an AP, show the history of channel and power changes due to Adaptive Radio Management (ARM).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show ARM history for an AP with a specific name.
`bssid <bssid>`	Show ARM history for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show ARM history for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

Adaptive Radio Management (ARM) can automatically change channel and power levels based on a number of factors such as noise levels and radio interference. The output of the **show ap arm history** command shows you an AP's channel and power changes over time, and the reason why those changes took place.

```
(host)[node]#show ap arm history ap-name AP-16
Interface :wifi0
ARM History
-----------
Reason  Old channel  New channel  Old Power  New Power  Last change
------  -----------  -----------  ---------  ---------  -----------
P-      153-         153-         12         9          3d:14h:56m:48s
P+      153-         153-         9          12         3d:13h:44m:7s
P+      153-         153-         12         15         3d:13h:23m:5s
P+      153-         153-         15         18         3d:13h:16m:32s
P+      153-         153-         18         21         3d:11h:42m:42s
P-      153-         153-         21         15         3d:8h:16m:12s

Interface :wifi1
ARM History
-----------
Reason  Old channel  New channel  Old Power  New Power  Last change
------  -----------  -----------  ---------  ---------  -----------
P-      11           11           15         12         3d:18h:22m:28s
P+      11           11           12         15         3d:18h:17m:27s
P-      11           11           15         12         3d:18h:9m:9s
P+      11           11           12         15         3d:17h:48m:41s
P+      11           11           15         18         3d:17h:44m:34s
P-      11           11           18         15         3d:17h:39m:11s
P-      11           11           15         12         3d:17h:32m:39s
P+      11           11           12         15         3d:17h:26m:15s
I: Interference, R: Radar detection, N: Noise exceeded, E: Error threshold exceeded, INV:
Invalid Channel, G: Rogue AP Containment, M: Empty Channel, P+: Increase Power, P-: Decrease
Power, OFF: Turn off Radio, ON: Turn on Radio
```

The output of this command includes the following information:

Parameter	Description
`Reason`	This column displays one of the following code to indicate why the channel or power change was made. ■ **I**: Interference ■ **R**: Radar detected ■ **N**: Noise exceeded ■ **E**: Error threshold exceeded ■ **INV**: Invalid Channel ■ **G**: Rogue AP Containment ■ **M**: Empty Channel ■ **P+**: Increase Power ■ **P-**: Decrease Power ■ **OFF**: Turn off Radio ■ **ON**: Turn on Radio The Reason key appears at the bottom of the ARM History table.
`Old Channel`	Channel number used by the AP interface before the ARM change.
`New Channel`	Channel number used by the AP interface after the ARM change.
`Old Power`	Power level of the AP interface before the ARM change.
`New Power`	Power level of the AP interface after the ARM change.
`Last Change`	Time elapsed since the change, in the format *days:hours:minutes:seconds*.

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm neighbors

```
show ap arm neighbors {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the ARM settings for an AP's neighbors.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows ARM neighbor information for AP name **ap70_1**.

```
(host)[node]# show ap arm neighbors ap-name ap70_1

BSSID: BSSID of discovered radio
ESSID: ESSID of discovered radio/Src BSSID through which the neighbor is discovered
Channel: Channel of operation of discovered radio
SNR: Signal to noise ratio of discovered radio
tx-power: Tx Power of disovered radio (if known)
PL: Path loss to discovered radio (using txpower and SNR)
AP Flags: Active: Discovered using OTA updates
          Passive: Discovered using passive scan
          Indirect: Two hop neighbors discovered using neighbors OTA update
Last Update: Timestamp when last OTA update was received (total OTA updates)

ARM Neighbors
-------------
BSSID              ESSID      Channel  SNR  Tx-power  PL (dB)  AP Flags  Last Update (Total
updates)
-----              -----      -------  ---  --------  -------  --------  ----------------------
------
6c:f3:7f:b6:68:14  ssid-ap1   153      49   22        69       Passive
18:64:72:93:6a:f2  ssid-ap2   132      48   24        68       Passive
18:64:72:02:24:30  ssid-ap3   153      47   18        63       Passive
18:64:72:01:f8:f0  ssid-ap4   36       60   22        0        Indirect  2015-03-12 16:38:26
9c:1c:12:fe:96:e4  ssid-ap5   11       33   18        123      Indirect  2015-03-13 08:37:18
6c:f3:7f:4b:64:23  ssid-ap6   6        51   20        125      Active    2015-03-12 14:05:48
```

The output of this command includes the following information:

Parameter	Description
BSSID	BSSID of the discovered radio of the AP.
ESSID	ESSID of the discovered radio of the AP or source BSSID through which the neighbor is discovered.
Channel	Channel of operation of the discovered radio of the AP.
SNR	Signal to noise ratio of the discovered radio of the AP.
Tx-power	Transmitter power of the discovered radio of the AP (if known).
PL (dB)	Path loss to the discovered radio (using tx-power and SNR)
AP Flags	■ **Active**: Discovered using Over-The-Air (OTA) updates ■ **Passive**: Discovered using passive scan ■ **Indirect**: Two hop neighbors discovered using neighbors OTA update
Last Update	Time stamp when last OTA update was received (total OTA updates)

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm rf-summary

```
show ap arm rf-summary {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} [verbose]
```

Description

Show the state and statistics for all channels being monitored by an individual AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show channel data for an AP with a specific name.
`bssid <bssid>`	Show channel data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show channel data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.
`verbose`	(Optional) Include the channel quality history for all channels on the AP's radios in the output of this command.

Examples

The output of this command shows detailed information for the individual channels being monitored and statistics for each AP interface. Use this command verify an AP's RF health, or to determine why multiple APs in the same area are on the same channel.

```
(host)[node] #show ap arm rf-summary ap-name AP-205
Channel Summary
---------------
channel  retry  phy-err  mac-err  noise  util(Qual)     cov-idx(Total)  intf_idx(Total)
-------  -----  -------  -------  -----  ----------     --------------  ---------------
36       0      0        0        92     0/0/0/0/95     0/0(0)          118/18//0/0(136)
40       0      0        0        89     8/1/2/1/95     0/0(0)          139/47//0/0(186)
44       0      0        0        89     7/0/2/2/95     0/0(0)          117/36//0/0(153)
48       0      0        0        89     10/3/2/0/96    0/0(0)          175/109//0/0(284)
52       0      0        0        90     9/2/2/2/95     0/0(0)          328/87//0/0(415)
56       0      0        0        90     6/0/2/3/96     0/0(0)          81/128//0/0(209)
60       0      0        0        89     8/1/2/0/95     0/0(0)          385/49//0/0(434)
64       0      0        0        90     8/1/2/1/95     0/0(0)          65/0//0/0(65)
149      0      0        0        92     7/3/0/0/94     0/0(0)          349/48//0/0(397)
153      0      0        0        93     6/6/0/0/95     0/0(0)          428/105//0/0(533)
157      0      0        0        92     10/3/2/0/95    0/0(0)          290/229//0/0(519)
161      0      0        9        92     4/1/0/6/95     7/0(7)          308/114//0/0(422)
11       0      0        10       91     58/51/1/0/94   7/0(7)          1064/284//0/0(1348)
Columns:util(Qual): ch-util/rx/tx/ext-ch-util/quality
HT Channel Summary
------------------
channel_pair  Pairwise_intf_index
------------  -------------------
149-153       930
157-161       941
Interface Name           :wifi0
Current ARM Assignment   :161-/21
Covered channels a/g     :1/0
Free channels a/g        :3/0
```

```
ARM Edge State           :disable
Last check channel/pwr   :7m:13s/22s
Last change channel/pwr  :32m:22s/10h:15m:40s
Next Check channel/pwr   :33s/4m:43s
Assignment Mode          :Single Band
Interface Name           :wifi1
Current ARM Assignment   :11/21
Covered channels a/g     :0/1
Free channels a/g        :0/0
ARM Edge State           :disable
Last check channel/pwr   :3m:25s/2m:1s
Last change channel/pwr  :10h:15m:40s/10h:15m:40s
Next Check channel/pwr   :1m:4s/3m:59s
Assignment Mode          :Single Band
```

The output of this command includes the following information:

Parameter	Description
`channel`	Number of a radio channel used by the AP.
`retry`	Number of 802.11 retry frames sent because a client failed to send an ACK.
`phy-err`	Number of PHY errors on the AP's current channel seen during the last second.
`mac-err`	Number of MAC errors on the AP's current channel seen during the last second.
`noise`	Current noise level, in -dBm.
`util(Qual)`	The quality of the channel based on the channel utilization.
`cov-idx`	The AP uses this metric to measure RF coverage. The coverage index is calculated as x+y, where "x" is the AP's weighted calculation of the Signal-to-Noise Ratio (SNR) on all valid APs on a specified 802.11 channel, and "y" is the weighted calculation of the Aruba APs SNR the neighboring APs see on that channel.
`intf_idx`	The AP uses this metric to measure co-channel and adjacent channel interference. The Interference Index is calculated as a/b//c/d, where: ■ Metric value "a" is the channel interference the AP sees on its selected channel. ■ Metric value "b" is the interference the AP sees on the adjacent channel. ■ Metric value "c" is the channel interference the AP's neighbors see on the selected channel. ■ Metric value "d" is the interference the AP's neighbors see on the adjacent channel. ■ To calculate the total Interference Index for a channel add "a+b+c+d".
`Interface Name`	Name of the gigabit Ethernet interface
`Current ARM Assignment`	Current channels assigned by the AP's ARM profile.
`Target Coverage Index`	Ideal value of coverage index an AP tries to achieve on its channel.
`Covered channels a/g`	Number of channels that are currently being used by an AP's BSSIDs.
`Free channels a/g`	Number of channels that are available to an AP because that channel has a lower interference index.

Parameter	Description
`ARM Edge State`	If enabled, ARM-enabled APs on the network edge will not become Air Monitors.
`Last check channel/pwr`	Time elapsed since the AP checked its channel and power settings, in *hour:minute:second* format.
`Last change channel/pwr`	Time elapsed since the AP changed its channel and power settings, in *hour:minute:second* format.

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm scan-times

```
show ap arm scan-times {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Shows channel scan times for an individual AP and information on the channel being scanned.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show channel scan data for an AP with a specific name.
`bssid <bssid>`	Show channel scan data for a specific Basic Service Set Identifier (BSSID) on an AP.
`ip-addr <ip-addr>`	Show channel scan data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Examples

The output of this command shows scan times for every channel on AP-225.

```
(host)[node]#show ap arm scan-times ap-name AP-225

Channel Scan Time
-----------------
channel  assign-time(ms)  scans-attempted  scans-rejected  scans-deferred  dos-scans  flags
   timer-tick
-------  ---------------  ---------------  --------------  --------------  ---------  -----
   ----------
44       796070           7237             0               0               0          DACLYS
   183703
140      704550           6405             0               0               0          DALY
   183715
144      395780           3598             0               0               0          DAUY
   183689
149      14550890         7399             0               0               0
DVACLYFETS  183695
14       488400           4440             0               0               0          DA
   183713

Channel Flags: D: All-Reg-Domain Channel, C: Reg-Domain Channel, A: Activity Present
L: Scan Secondary Above, U: Scan Secondary Below, Y: Scan 80MHz, Z: Rare Channel
V: Valid, T: Valid 20MHZ Channel, F: Valid 40MHz Channel,  P: Valid 40MHZ Channel Pair
E: Valid 80MHz Channel (lower 20M), B: Belongs to valid 80MHz channel
O: DOS Channel, K: DOS 40MHz Upper, H: DOS 40MHz Lower, N: Split Channel Scan
R: Radar detected in last 30 min, X: DFS required, S: Transmit Allowed
J: Unconventional Scan 40MHz Above, M: Unconventional Scan 40MHz Below

WIFI Channel Scanning State
---------------------------
Scan mode   channel  current-scan-channel  last-dos-channel  timer-milli-tick  next-scan-
milli-tick (jitter)  scans (Tot:Rej:Eff(%):Last intvl(%))
---------   -------  --------------------  ----------------  ----------------  ---------------
-------------  ------------------------------------
Aggressive  153E     161E                  0                 180855370         180855550 (-
219)               181716:0:100:100
```

```
Aggressive  11       3+                    0                 180855370         180855960 (163)
              181658:0:100:100

Group Scan Time
-----------------
channels         assign-time(ms)  scans-attempted  scans-rejected  scans-deferred  group-width
 timer-tick
--------         ---------------  ---------------  --------------  --------------  -----------
 ----------
34               113960           1036             0               0               20MHz
 183544
36,40,44,48      3184390          28949            0               0               80MHz
 183711
38               114070           1037             0               0               20MHz
 183575
42               114070           1037             0               0               20MHz
 183591
```

The output of this command includes the following parameters:

Parameter	Description
`channel`	Displays the channels in the group.
`assign-time (ms)`	The cumulative time spent on the channel.
`scans-attempted`	The number of times an AP attempted to scan a channel.
`scans-rejected`	The number of times an AP attempted to scan a channel, but was unable to scan because the scan was halted by the power save, VoIP aware, or load aware ARM features.
`scans-deferred`	The number of times an AP deferred to scan a channel due to an event such as a radar detection.
`dos-scans`	The number of times an AP visited the channel to contain a rogue device.
`flags`	Displays additional information about the channel. The flags key is displayed at the bottom of the Channel Scan Time table.
`group_width`	The channel width of the group.
`timer-tick`	The timer-tick of the last scan.

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm split-scan-history

```
show ap arm split-scan-history {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show scanning information for a "split-scan", where ARM performs an additional scans on each channel within a 40 MHz channel pair or 80 MHz channel set.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show scan data for an AP with a specific name.
`bssid <bssid>`	Show scan data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show scan data for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Usage Guidelines

If ARM reports a high noise floor on a channel within a 40 MHz channel pair or 80 MHz channel set, ARM performs an additional 20 MHz scan on each channel within that channel pair or set, to determine the actual noise floor of each affected channel. This allows ARM to avoid assigning the overutilized channel, while still allowing channel assignments to the other unaffected channels in that channel pair or set.

Examples

The output of this command shows information about one split-scan performed on channel 161E.

```
(host)[node]# show ap arm split-scan-history ap-name 1242-ac
Interface :wifi0
Split Scan History
------------------
Time of setup        Channel scan  Number of Split scans  Noise Floor
-------------        ------------  ---------------------  -----------
2013-10-08 03:11:40  161E          4                      69
Interface :wifi1
```

The output of this command includes the following parameters:

Parameter	Description
`Time of setup`	Timestamp showing the date and time the scan was performed
`Channel Scan`	The channel pair or channel set scanned
`Number of Split Scans`	The number of times ARM performed an additional split scan.
`Noise Floor`	Noise floor recorded on the primary channel within that channel pair or channel set.

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm state

```
show ap arm state [ap-name <ap-name>|dot11a|dot11g|ip-addr <ip-addr>]
```

Description

Display Adaptive Radio Management (ARM) information for an individual AP's neighbors, or show all available data for any neighboring AP using an 802.11a or 802.11g radio type.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show aggregate ARM Neighbor Information for a specific AP.
`dot11a`	Show aggregate ARM Neighbor Information for all APs using an 802.11a radio.
`dot11g`	Show aggregate ARM Neighbor Information for all APs using an 802.11g radio.
`ip-addr <ip-addr>`	Show aggregate ARM Neighbor Information for a AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

The output of the **show ap arm state** command shows 802.11a and 802.11g information for all APs. Include an AP name or IP address to show data for just a single AP, or use the **dot11a** or **dot11g** keywords to show data for all APs using that radio type.

Examples

The output of this command shows 802.11a information for all neighboring APs.

```
(host)[node]# show ap arm state

show ap arm state ap-name AP49
AP-1249:10.100.139.233:52:21:26-Edge:disable : Client Density:13
Neighbor Data
-------------
Name               IP Address SNR  Assignment  Neighbor Density
----               ----------      ---  ----------  ----------------
AP42               10.100.139.249  41   52/21       13/17/100/76
AP09               10.100.139.224  22   56/21       3/5/23/60
AP48               10.100.139.241  36   60/21       9/11/69/81
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP.
`IP address`	IP address of an AP.
`SNR`	Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.

Column	Description
`Assignment`	The AP's current channel assignment.
`Neighbor Density`	The neighborhood density for the specified AP is listed with the values A/B/C/D, where: ■ A= Number of the AP's clients heard in the AP neighbor's client list ■ B= Number of clients in AP neighbor's client list ■ C= Density percentage, (AP clients heard in in the AP neighbor client list / AP client density * 100). ■ D= Density Percentage (AP clients heard in the AP neighbor's client list / neighbor client density * 100)

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm status

```
show ap arm status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Issue this command under the supervision of Aruba support to display detailed debugging Adaptive Radio Management (ARM) information and ARM status counters for an individual AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show ARM status for an AP with a specific name.
`bssid <bssid>`	Show ARM status for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show ARM status for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Usage Guidelines

The output of the **show ap arm status** command shows internal ARM status counters that can be used by Aruba support for debugging purposes.

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap arm virtual-beacon-report

```
show ap arm virtual-beacon-report
   ap-name <name>
   ip-addr <ipaddr>
   ip6-addr <ip6-addr>
   phy-type 80211a|80211b|80211g
```

Description

If the client match feature is enabled, the output of this command displays the virtual beacon report for an AP with a specific IP or MAC address.

Syntax

Parameter	Description
`ap-name <name>`	Name of an AP for which you want to view a virtual beacon report.
`ip-addr <ipaddr>`	IPv4 address of an AP for which you want to view a virtual beacon report.
`ip6-addr <ipv6addr>`	IPv6 address of an AP for which you want to view a virtual beacon report.
`phy-type`	Display virtual beacon report data for an AP radio with one of the following phy types: ■ 80211a ■ 80211b ■ 80211g

Usage Guidelines

If the client match feature is enabled, the managed device sends APs a list of clients that should not be allowed to associate to that AP.

Example

```
(host)[node] #show ap arm virtual-beacon-report ap-name 1263-ac

Interface:wifi0
Rx VBR Reports:683

Client MAC:24:77:03:cf:fa:5c
Dual band:Yes
Active Voice:No
Steerable:Yes
Dual network capable:No
Current Association:6c:f3:7f:e7:5a:b0

Virtual Beacon Report
---------------------
AP                 Channel  Signal (dBm)  EIRP  Assoc
--                 -------  ------------  ----  -----
9c:1c:12:fd:d2:10  60       -76           12
9c:1c:12:fd:d2:00  1        -66           12
9c:1c:12:fe:13:50  52       -73           21
9c:1c:12:fe:0f:d0  52       -74           24
9c:1c:12:fd:f7:b0  44       -49           20
6c:f3:7f:e7:5a:b0  60       -73           12    Y
```

```
9c:1c:12:fd:f2:30  60       -69          12
9c:1c:12:fd:f7:a0  1        -55          12
9c:1c:12:fd:f2:20  1        -65          12
9c:1c:12:fe:13:40  1        -68          12
```

The output of this command includes the following parameters:

Parameter	Description
`AP`	MAC address of the AP from which the client can detect a signal
`Channel`	Channel on which the signal was deteched
`Signal`	Signal strength, in dBm, of the probe request received from Client
`EIRP`	Amount of power transmitted from the AP antennae
`Assoc`	A "Y" in this field indicates that the client is currently associated to that AP radio

Related Commands

Use the following command to enable the client match feature

- rf arm-profile client-match

The following commands display additional statistics for the client match feature

- show ap arm client-match probe-report
- show ap arm client-match neighbors
- show ap arm client-match restriction-table
- show ap arm virtual-beacon-report
- show ap arm client-match unsupported
- show ap arm client-match summary
- show ap arm client-match history

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap association

```
show ap association
   anyspot
   ap-group <ap-group>
   ap-name <ap-name>
   bssid <bssid>
   channel <channel>
   client-mac <client-mac>
   dormant
      ap-group <ap-group>
      ap-name <ap-name>
      bssid <bssid>
      channel <channel>
      essid <essid>
      remote {[ap-group <ap-group>] | [ap-name <ap-name>] | [bssid <bssid>] | [channel <chan-
      nel>] | [essid <essid>]}
   essid <essid>
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
   phy <phy>
   remote
      ap-group <ap-group>
      ap-name <ap-name>
      bssid <bssid>
      channel <channel>
      essid <essid>
   voip-only
```

Description

This command shows the AP association table.

Syntax

Parameter	Description
`anyspot`	Shows AP associations for anyspot virtual AP.
`ap-group <ap-group>`	Shows AP associations for the specified AP group.
`ap-name <ap-name>`	Shows AP associations for the specified AP name.
`bssid <bssid>`	Shows AP associations for the specified Basic Service Set Identifier (BSSID). The BSSID is usually the MAC address of an AP.
`channel <channel>`	Shows AP associations for the specified channel.
`client-mac <client-mac>`	Shows AP associations for the specified MAC address of a client.
`dormant`	Shows AP associations for the specified dormant station.
`essid <essid>`	Shows AP associations for the specified Extended Service Set Identifier (ESSID). An ESSID is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, enclose the ESSID in quotation marks.

Parameter	Description
`ip-addr <ip-addr>`	Shows AP associations for the specified IP address of an AP.
`ip6-addr <ip-addr>`	Shows AP association for the specified IPv6 address of an AP.
`phy`	Shows AP association for the specified PHY radio type (802.11a, 802.11b or 802.11g) Use the corresponding keywords **a**, **b**,or **g**.
`remote`	Shows AP association for bridge mode AP.
`voip-only`	Shows AP association for VoIP-only clients.

Usage Guidelines

Use this command to check if user is connected to an AP. This command validates whether the client is associated and indicates the last AP to which it was connected. If the flags column shows an 'A', the client is currently associated with that AP. Alternately, if the client is not currently associated, the AP with the smallest value of association time is the last AP used by the client.

Example

Use the **show ap association client-mac** command to verify that a user has associated with an AP, or to determine last AP to which the client was connected. The output of this command in the example below shows the association table for the client with the MAC address 00:1a:1e:aa:bb:cc. If the flags column in the output of this command shows an '*A*', the client associated last to that AP. Alternately, the AP with the smallest value of association time is the last AP to which the client had associated.

In the example below, the output of this command has been broken into two separate tables to better fit this page. In the actual output of the command, this information is shown in a single, wide table.

```
(host) #show ap association client-mac 00:1a:1e:aa:bb:cc


Flags: W: WMM client, A: Active, R: RRM client
PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHzss:  spatial streams

Association Table
-----------------
Association Table
-----------------
-----------------
Name  bssid              mac               auth  assoc  aid  l-int  essid
----  -----              ---               ----  -----  ---  -----  -----
AL12  00:1a:1e:11:5f:11  00:21:5c:50:b1:ed  y     y      12   10     ethersphere-wpa2AL5
00:1a:1e:88:88:31  00:19:7d:d6:74:93  y     y      6    10     ethersphere-wpa2

vlan-id  tunnel-id  phy            assoc. time  num assoc  Flags
-------  ---------  ---            -----------  ---------  -----
65       0x10c4     a-HT-40sgi-2ss  35m:41s      1          WA65       0x1072     a
                                                                24m:29s      1          WA
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP

Column	Description
bssid	The AP Basic Service Set Identifier (BSSID)
mac	MAC address of the AP
auth	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
assoc	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
aid	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
1-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Name that uniquely identifies the AP's Extended Service Set Identifier (ESSID).
vlan-id	Identification number of the AP's VLAN.
tunnel-id	Identification number of the AP's tunnel.
assoc. time	Amount of time the client has associated with the AP, in the format *hours:minutes:seconds*.
num assoc	Number of clients associated with the AP.
flags	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the **show ap association** command.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap association remote

```
show ap association remote [ap-name <ap-name>|ap-group <ap-group>|bssid <bssid>|channel
<channel>|essid <essid>
```

Description

Display the association table for an individual AP or group of APs in bridge mode.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show AP associations for a specific remote AP.
`ap-group <ap-group>`	Show AP associations for a specific group of remote APs.
`bssid <bssid>`	Show the AP associations for an specific AP Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`channel <channel>`	Show remote AP associations for a specific channel.
`essid <essid>`	Show remote AP associations for an Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.

Examples

The output of the command below shows the association table for clients in the AP group **group1**.

```
show ap association remote ap-group group1

Flags: W: WMM client, A: Active, R: RRM client
PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz ss:  spatial streams

Association Table
-----------------
Name    bssid
essid  vlan-id  tunnel-id phy  assoc.time  num assoc  Flags
----    -----
-  -------  --------- ---  ----------  ---------  -----
AP71 00:0b:23:c1:d6:11 00:12:6d:03:1c:f1        y              y                          1
                        a                       23s
Num Clients:1
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP
`bssid`	The AP Basic Service Set Identifier (BSSID)
`mac`	MAC address of the AP

Column	Description
auth	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
assoc	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
aid	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
1-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Name that uniquely identifies the AP's Extended Service Set Identifier (ESSID).
vlan-id	Identification number of the AP's VLAN.
tunnel-id	Identification number of the AP's tunnel.
phy	The RF band in which the AP should operate: **g** = 2.4 GHz **a** = 5 GHz
assoc. time	Amount of time the client has associated with the AP, in the format *hours:minutes:seconds*.
num assoc	Number of clients associated with the AP.
flags	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the **show ap association remote** command.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap assoc-throttle-counters

```
show ap assoc-throttle-counters
```

Description

This command shows counters related to association request throttling.

Syntax

No parameters.

Usage Guidelines

This command shows counters related to association request throttling.

Example

The following example shows counters related to association request throttling:

```
(host) [mynode] #show ap assoc-throttle-counters

Association Throttle Counters
-----------------------------
Counter                       Value
-------                       -----
Dropped association requests  0
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap authorization-profile

```
show ap authorization-profile [<profile-name>]
```

Description

This command shows information for AP authorization profiles.

Syntax

Parameter	Description
<profile-name>	The name of an an existing AP authorization profile.

Usage Guidelines

The AP authorization profile specifies which configuration should be assigned to a remote AP that has been provisioned but not yet authenticated at the remote site. By default, these yet-unauthorized APs are put into the temporary AP group **authorization-group** and assigned the predefined profile **NoAuthApGroup**. This configuration allows the user to connect to an unauthorized remote AP via a wired port then enter a corporate username and password. Once a valid user has authorized the AP and the remote AP will be marked as authorized on the network. The remote AP will then download the configuration assigned to that AP by it's permanent AP group.

Issue this command without the **<profile-name**> option to display the entire AP authorization profile list, including profile status and the number of references to each profile. Include a profile name to display the authorization group defined for that profile.

Examples

The following example lists all AP authorization profiles. The **References** column lists the number of other profiles with references to that authorization profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined AP authorization profiles will not have an entry in the **Profile Status** column.

```
(host) #show ap authorization-profile

AP Authorization profile List
-----------------------------
Name           References  Profile Status
----           ----------  --------------
Noauthprofile  1
default        2                   Predefined (editable)
Total:2
```

To display the authentication group for an individual profile, include the <profile> parameter. The example below shows the profile details for the AP authorization profile **Default**.

```
(host) #show ap authorization-profile default

AP Authorization profile "default" (Predefined (editable))
----------------------------------------------------------
Parameter               Value
---------               -----
AP authorization group  NoAuthApGroup
```

The output of the **show ap authorization** command includes the following parameters:

Parameter	Value
`AP authorization group`	Name of a configuration profile to be assigned to the group unauthorized remote APs.

Related Commands

Command	Description	Mode
ap authorization-profile	This command defines a temporary configuration profile for remote APs that are not yet authorized on the network.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap blacklist-clients

```
show ap blacklist-clients
```

Description

Show a list of clients that have been denied access.

Usage Guidelines

Use the stm CLI command to add or remove users from a blacklist. Additionally, the **dot1x authentication**, **VPN authentication** and **MAC authentication** profiles allow you to automatically blacklist a client if machine authentication fails.

Examples

The output of this command shows that the controller has a single user-defined blacklisted client.

```
(host)# show ap blacklist-clients

Blacklisted Clients
-------------------
STA                reason        block-time(sec)   remaining time(sec)
---                ------        ---------------   -------------------
00:1E:37:CB:D4:52  user-defined  45                3555
```

The output of this command includes the following information:

Column	Description
STA	MAC address of the blacklisted client.
reason	The reason that the user was blacklisted. ■ **ARP-attack**: Blacklisted for an ARP attack. ■ **user-defined:** Blacklisted due to blacklist criteria were defined by the network administrator ■ **mitm-attack**: Blacklisted for a man in the middle (MITM) attack; impersonating a valid enterprise AP. ■ **gratuitous-ARP-attack**: Blacklisted for a gratuitous ARP attack. ■ **ping-flood**: Blacklisted for a ping flood attack. ■ **session-flood**: Blacklisted for a session flood attack. ■ **syn-flood**: Blacklisted for a syn flood attack. ■ **session-blacklist:** User session was blacklisted ■ **IP spoofing**: Blacklisted for sending messages using the IP address of a trusted client. ■ **ESI-blacklist**: An external virus detection or intrusion detection application or appliance blacklisted the client. ■ **CP-flood**: Blacklisting for flooding with fake AP beacons. ■ **UNKNOWN**: Blacklist reason unknown.
block-time (sec)	Amount of time the client has been blocked, in seconds.
remaining time(sec)	Amount of time remaining before the client will be allowed access to the network again.

Related Commands

Command	Description	Mode
stm add-blacklist-client stm remove-blacklist-client <macaddr>	Manually add or remove clients from a blacklist.	Config mode

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap blacklist-time

```
show ap blacklist-time
```

Description

This command shows the AP blacklist time.

Syntax

No parameters.

Usage Guidelines

This command shows the amount of blacklist time of the STA when it is blacklisted in between disconnection and user-timeout.

Example

The following example shows the AP blacklist time:

```
(host) [mynode] #show ap blacklist-time

ap blacklist-time:3600
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap bss-table

```
show ap bss-table
   ap-name <ap-name>
      counters
      details
      essid <essid>
      standby
   bssid <bssid>
      counters
      details
      essid <essid>
      standby
   counters
      ap-name <ap-name>
      bssid <bssid>
      essid <essid>
      ip-addr <ip-addr>
      ip6-addr <ip6-addr>
      port <slot/port>
   details
   essid <essid>
      ap-name <ap-name>
      ip-addr <ip-addr>
      ip6-addr <ip6-addr>
      port <slot/port>
   ip-addr <ip-addr>
      counters
      details
      essid <essid>
      standby
   ip6-addr <ip6-addr>
      counters
      details
      essid <essid>
      standby
   port <slot/port>
   standby
      ap-name <ap-name>
      bssid <bssid>
      details
      ip-addr <ip-addr>
      ip6-addr <ip6-addr>
      port <slot/port>
```

Description

This command shows the Basic Service Set (BSS) table of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the BSS table for the specified AP name.
`bssid <bssid>`	Shows the BSS table for the specified Basic Service Set Identifier (BSSID) of an AP. The BSSID is usually the MAC address of an AP.

Parameter	Description
counters	Shows the BSS table of counters for the specified AP.
details	Shows the BSS table with detailed columns.
essid <essid>	Show the BSS table for the specified Extended Service Set Identifier (ESSID) of an AP. An ESSID is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, enclose the ESSID in quotation marks.
ip-addr <ip-addr>	Shows the BSS table for the specified IP address of an AP.
ip6-addr <ip6-addr>	Shows the BSS table for the specified IPv6 address of an AP.
port <slot/port>	Shows the BSS table for the specified port of an AP.
standby	Show the BSS table for the specified AP in standby mode.

Usage Guidelines

The output of the **show ap bss-table** command shows the Aruba AP BSS table for all APs. To filter this information and view BSS table data for an individual AP or a specific port and slot number, include the **ap-name**, **bssid**, **essid**, **ip-addr** or **port** keywords.

Example

The example shows the BSS table for the active APs:

```
(host) [mynode] #show ap bss-table

fm (forward mode): T-Tunnel, S-Split, D-Decrypt Tunnel, B-Bridge (s-standard, p-persistent, b-
backup, a-always), n-anyspot
Aruba AP BSS Table
------------------
bss                ess          port  ip            phy    type  ch/EIRP/max-EIRP  cur-cl  ap
name  in-t(s)  tot-t            mtu   acl-state  acl  fm
---                ---          ----  --            ---    ----  ----------------  ------  ---
----  -------  -----            ---   ---------  ---  --
9c:1c:12:fd:ec:e0  qa_testing   N/A   172.16.10.20  g-HT   ap    6/19/19           0       204
     0        27d:21h:54m:23s  1578  -          58   T
9c:1c:12:fd:ec:e1  qa_testing1  N/A   172.16.10.20  g-HT   ap    6/19/19           0       204
     0        27d:21h:54m:23s  1578  -          58   Tn
9c:1c:12:fd:ec:f0  qa_testing   N/A   172.16.10.20  a-VHT  ap    36/10/20          2       204
     0        27d:21h:54m:23s  1578  -          58   T
9c:1c:12:fd:ec:f1  qa_testing1  N/A   172.16.10.20  a-VHT  ap    36/10/20          0       204
     0        27d:21h:54m:23s  1578  -          58   Tn

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:4
Num Associations:2
```

The output of this command includes the following information:

Column	Description
bss	The AP Basic Service Set Identifier (BSSID). This is usually the MAC address of the AP

Column	Description
ess	The AP Extended Service Set Identifier (ESSID).
port	The slot and port used by the controller, in the format <slot>/<module>/<port>.
ip	IP address of an AP.
phy	An AP radio type. Possible values are: ■ a—802.11a ■ a-HT—802.11a high throughput ■ g— 802.11g ■ g-HT—802.11g high throughput
type	Shows whether the AP is working as an access point (AP) or air monitor (AM).
ch/EIRP/max-EIRP	Radio channel used by the AP/current effective Isotropic Radiated Power (EIRP) /maximum EIRP.
cur-cl	Current number of clients on the AP.
ap name	Name of the AP.
in-t(s)	Number of seconds that an AP has been inactive.
tot-t	An AP's total active time, in seconds.
mtu	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
acl-state	An ACL can enable or disable an AP during specific time ranges. ■ **Disabled**: An ACL with time restrictions is currently **disabled** (so the AP is enabled). ■ **Enabled**: An ACL with time restrictions is currently **enabled** (so the AP is disabled). ■ This data column will display a dash (**-**) if no ACLs are currently configured for the AP.
acl	The ACL id is displayed based on the role set.
fm	Listed below are the forwarding modes available: ■ **T-Tunnel** ■ **S-Split** ■ **D-Decrypt Tunnel** ■ **B-Bridge** (s-standard, p-persistent, b-backup, a-always) **NOTE:** If anyspot is enabled for a particular BSSID, then it is represented as **n** in the **Forwarding Mode** parameter.

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

show ap bw-report

```
show ap bw-report {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show the bandwidth reporting table for a specific AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show bandwidth data for an AP with a specific name.
`bssid <bssid>`	Show bandwidth data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show bandwidth data for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Examples

The output of the following command shows the Aruba AP bandwidth table for an AP with the IP address 192.0.2.170.

```
show ap bw-report ip-addr 192.0.2.170

Bandwidth report for AP "AL16" radio 0
--------------------------------------
Virtual AP                Allocated Share  Actual Share  Offered Load  Delivered Load
----------                ---------------  ------------  ------------  --------------
corp1344-guest            0%               0%            0 kbps        0 kbps
corp1344-ethersphere-wpa2 0%               0%            0 kbps        0 kbps
Average Throughput:0 kbps

Bandwidth report for AP "AL16" radio 1
--------------------------------------
Virtual AP                  Allocated Share  Actual Share  Offered Load  Delivered Load
----------                  ---------------  ------------  ------------  --------------
corp1344-guest              0%               0%            0 kbps        0 kbps
corp1344-ethersphere-voip   0%               0%            0 kbps        0 kbps
corp1344-ethersphere-vocera 0%               0%            0 kbps        0 kbps
Average Throughput:0 kbps
```

The output of this command includes the following information for all radios on the AP:

Column	Description
`Virtual AP`	Name of a Virtual AP
`Allocated Share`	Maximum percentage of total bandwidth available to that Virtual AP.
`Actual Share`	Actual percentage of total bandwidth used by a Virtual AP.

Column	Description
`Offered Load`	Attempted throughput for the Virtual AP, in kbps.
`Delivered Load`	Actual throughput for the Virtual AP, in kbps. This value may be less than the offered load if the Virtual AP has used all its allocated bandwidth.
`Average Throughput`	Average throughput for the virtual AP, in kbps.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap client status

```
show ap client status <client-mac>
```

Description

Show the current status of a specific client.

Syntax

Parameter	Description
`<client-mac>`	MAC address of a client

Examples

The output of the command shows the status of an individual client in the STA (station) table.

```
(host) #show ap client status  00:13:fd:42:32:38

STA Table
---------
bssid              auth  assoc  aid  l-int  essid      vlan-id  tunnel-id
-----              ----  -----  ---  -----  -----      -------  ---------
00:1a:1e:a3:02:c9  y     y      7    10     corp-wpa2  65       0x10c0
State Hash Table
----------------
bssid              state       reason
-----              -----       ------
00:1a:1e:a3:02:c9  auth-assoc  0
```

The output of this command includes the following information:

Column	Description
`bssid`	Basic Service Set ID (BSSID) of the client.
`auth`	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
`assoc`	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
`aid`	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
`l-int`	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
`essid`	Extended Service Set ID (ESSID) of the client.
`vlan-id`	VLAN ID of the VLAN used by the client
`tunnel-id`	Identification number for the tunnel

Column	Description
`state`	If the client has been both authorized and associated, this data column will display **auth-assoc**. If the client has only been authorized, this data column will display **auth**.
`Reason`	If the client failed to authenticate, this data column lists the reason code for 802.11 authentication failure

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap client trail-info

```
show ap client trail-info [<client-mac>]
```

Description

Use this command to show client activity for debugging purposes.

Syntax

Parameter	Description
<client-mac>	MAC address of the client.

Usage Guidelines

Use this command to view client activity, including reasons for client deauthentication, the history of how that client moved between different APs, and any alerts or errors encountered by that client. Include the optional **<client-mac>** parameter to show additional details for that specific client.

Client-trail information may be available for clients that are no longer active, as the controller saves a limited amount of client data in a buffer. The maximum number of clients for which trail-information is saved is determined by is determined by the controller platform. Each controller saves client trail information for twice the number of active clients supported by that controller platform.

Examples

The following example shows client-trail information for all clients associated with the controller.

```
(host) #show ap client trail-info

Client Trail Info
-----------------
MAC                BSSID              ESSID   AP-name   VLAN   Deauth-reason    Alert
-----------------  -----------------  ------  --------  -----  ---------------  -------------
00:11:22:33:44:55  00:0b:86:11:22:33  corp    ap1       10     AP-Down          Auth-failure
00:12:32:43:54:65  00:0b:86:11:22:34  corp    ap2       10     AP-Down          Auth-failure
00:31:42:53:64:75  00:0b:86:11:22:35  corp    ap3       10     AP-Down          Auth-failure
```

This example shows client-trail information for a specific user that includes information about AP alerts and mobility trails.

```
(host) #show ap client trail-info 00:11:22:33:44:55
MAC                BSSID              ESSID   AP-name  VLAN    Deauth-reason   Alert
-----------------  -----------------  -----   -------  ----    -------------   ------------
00:11:22:33:44:55  00:0b:86:11:22:33  corp    ap1      10      AP-down         Auth-failure
Deauth Reason
Reason             Timestamp
------------       --------------------------
AP-Down            Apr-12-2013 08:12:34
Alert
Reason             Timestamp
--------------     ------------------
Auth-Failure       Apr-10-2013 03:45:11
Mobility Trail
AP-name      BSSID              ESSID     Timestamp
-------      -----------------  -----     --------------------
Ap1          00:0b:86:11:11:11  corp      Apr-10-2013 03:45:11
AP2          00:0b:86:22:22:22  abc       Apr-10-2013 03:45:11
```

The output of these commands include the following information:

Column	Description
MAC	MAC address of the client
BSSID	BSSID of the client
ESSID	ESSID to which the client associated
AP-name	Name of the AP to which the client associated
VLAN	VLAN ID of the VLAN to which the client associated.
Deauth-reason	Reason why the client was deauthorized.
Alert	Reason why alerts were triggered by the client
Timestamp	If you include the optional <client-mac> parameter, the output will include a timestamp that indicates the time each alert or deauthorization was triggered.
Mobility-Trail	If you include the optional <client-mac> parameter, the output will include the AP name, BSSID and ESSID of the APs to which the cient connected, as well as a timestamp showing when the connections were initiated.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap cluster-tech-support

```
show ap cluster-tech-support {ap-name <ap-name>} [<filename>]
```

Description

This command shows cluster information of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows cluster information of an AP for specified AP name.
`<filename>`	Stores output in specified filename.

Usage Guidelines

This command shows cluster information for an AP. For the remaining parameters, see the command syntax.

Example

The following example shows cluster information for an AP named ap-205:

```
(host) [mynode] #show ap cluster-tech-support ap-name ap-205

Jul  1 23:05:01|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
Jul  1 23:06:01|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
Jul  1 23:07:02|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
Jul  1 23:08:02|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
Jul  1 23:09:02|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
Jul  1 23:10:02|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
Jul  1 23:11:02|--:--:--:--:--:--|---.---.---.---|AMON|send_ap_amp_payload:139|mgmt-servers:1,
STA hash table enties:0, AGR table enties:0
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap config

```
show ap config {ap-group <ap-group>}|{ap-name <ap-name>}|{essid <essid>}
```

Description

Show a large list of configuration settings for an ap-group or an individual AP.

Syntax

Parameter	Description
`ap-group <ap-group>`	Display configuration settings for an AP group.
`ap-name <ap-name>`	Display configuration settings for an AP with a specific name.
`essid <essid>`	Display configuration settings for an AP with a specific ESSID. An ESSID is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.

Examples

The example output below shows just some of the configuration settings displayed in the output of this command.

```
show ap config ap-group apgroup14
-------------------------------------------------
Parameter                              802.11g         802.11a         Source
---------                              -------         -------         ------
LMS IP                                 N/A             N/A             ap system-profile
"default"
Backup LMS IP                          N/A             N/A             ap system-profile
"default"
LMS Preemption                         Disabled        Disabled        ap system-profile
"default"
LMS Hold-down Period                   600 sec         600 sec         ap system-profile
"default"
Master controller IP address           N/A             N/A             ap system-profile
"default"
RF Band                                g               g               ap system-profile
"default"
Double Encrypt                         Disabled        Disabled        ap system-profile
"default"
Native VLAN ID                         1               1               ap system-profile
"default"
SAP MTU                                N/A             N/A             ap system-profile
"default"
Bootstrap threshold                    8               8               ap system-profile
"default"
Request Retry Interval                 10 sec          10 sec          ap system-profile
"default"
Maximum Request Retries                10              10              ap system-profile
"default"
Keepalive Interval                     60 sec          60 sec          ap system-profile
"default"
Dump Server                            N/A             N/A             ap system-profile
"default"
Telnet                                 Disabled        Disabled        ap system-profile
"default"
```

```
FIPS enable                          Disabled        Disabled        ap system-profile
"default"
SNMP sysContact                      N/A             N/A             ap system-profile
"default"
RFprotect Server IP                  N/A             N/A             ap system-profile
"default"
RFprotect Backup Server IP           N/A             N/A             ap system-profile
"default"
AeroScout RTLS Server                N/A             N/A             ap system-profile
"default"
RTLS Server configuration            N/A             N/A             ap system-profile
"default"
Remote-AP DHCP Server VLAN           N/A             N/A             ap system-profile
"default"
Remote-AP DHCP Server Id             192.168.11.1    192.168.11.1    ap system-profile
"default"
Remote-AP DHCP Default Router        192.168.11.1    192.168.11.1    ap system-profile
"default"
Remote-AP DHCP Pool Start            192.168.11.2    192.168.11.2    ap system-profile
"default"
Remote-AP DHCP Pool End              192.168.11.254  192.168.11.254  ap system-profile
"default"
Remote-AP DHCP Pool Netmask          255.255.255.0   255.255.255.0   ap system-profile
"default"
Remote-AP DHCP Lease Time            0 days          0 days          ap system-profile
"default"
Heartbeat DSCP                       0               0               ap system-profile
"default"
Session ACL                          N/A             N/A             ap system-profile
"default"
Image URL                            N/A             N/A             ap system-profile
"default"
Maintenance Mode                     Disabled        Disabled        ap system-profile
"default"
...
```

The output of this command includes the following parameters.

Parameter	Description
`LMS IP`	The IPv4 address of the LMS - the Aruba managed device which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
`LMS IPv6`	The IPv6 address of the LMS - the Aruba managed device which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
`Backup LMS IP`	For networks with multiple managed devices, this parameter displays the IPv4 address of a backup to the IP address specified with the **lms-ip** parameter.
`Backup LMS IP`	For networks with multiple managed devices, this parameter displays the IPv6 address of a backup to the IP address specified with the **lms-ip** parameter.
`LMS Preemption`	When this parameter is enabled, the LMS automatically reverts to the primary LMS IP address when it becomes available.

Parameter	Description
LMS Hold-down Period	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover.
Number of IPsec retries	Shows the number of times the AP will attempt to recreate an IPsec tunnel with Mobility Master before the AP will reboot. The supported range is 0-1000 retries, and the default value is 360. A value of 0 disables the reboot.
LED operation mode	The operating mode for the LEDs (11n APs only) ■ normal: Normal mode ■ off: All LEDs off
Master controller IP address	For networks with multiple managed devices, this parameter displays the IP address of Mobility Master.
RF Band	For dual-band radios, this parameter displays the RF band in which the AP should operate: ■ **g** = 2.4 GHz ■ **a** = 5 GHz
Double Encrypt	This parameter applies only to remote APs. Double encryption is used for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel.
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).
SAP MTU	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
Bootstrap threshold	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the managed device, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
Request Retry Interval	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.
Maximum Request Retries	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either reboots or tries the IP address specified by the backup LMS IP address (if configured).
Keepalive Interval	Time, in seconds, between keepalive messages from the AP
Dump Server	(For debugging purposes.) Displays the server to receive the core dump generated if an AP process crashes.
Telnet	Reports whether telnet access the AP is enabled or disabled.
SNMP sysContact	SNMP system contact information.

Parameter	Description
AeroScout RTLS Server	Displays whether or not the AP will send RFID tag information to an AeroScout RTLS server.
RTLS Server configuration	Displays whether or not the AP will send RFID tag information to an RTLS server.
Remote-AP DHCP Server VLAN	Shows the VLAN ID of the remote-AP DHCP server used when the managed device is unreachable.
Remote-AP DHCP Server Id	Shows the IP Address of the DHCP DNS Server.
Remote-AP DHCP Default Router	Shows the IP Address of the DHCP Default Router.
Remote-AP DHCP Pool Start	Shows the IP Address used as start of DHCP Pool.
Remote-AP DHCP Pool End	Shows the IP Address used as end of DHCP Pool.
Remote-AP DHCP Pool Netmask	Shows the netmask of DHCP Pool.
Remote-AP DHCP Lease Time	Shows the length of leases, in days (0 means infinite).
Remote-AP uplink total bandwidth	This is the total reserved uplink bandwidth (in Kilobits per second)
Remote-AP bw reservation	Session ACLs with uplink bandwidth reservation in kilobits per second. You can specify up to three session ACLs to reserve uplink bandwidth.
Heartbeat DSCP	DSCP value of AP heartbeats (0-63).
Session ACL	Shows the ACL applied on the uplink of a remote AP.
Maintenance Mode	Shows if Maintenance mode is enabled or disabled. If enabled, APs stop flooding unnecessary traps and syslog messages to NMS systems or network operations centers when deploying, maintaining, or upgrading the network. The managed device still generates debug syslog messages if debug logging is enabled.
Remote-AP Local Network Access	Enable or disable local network access across VLANs in a Remote-AP.
Radio enable	Shows if the AP's radio is enabled or disabled.
Mode	Shows the operating modes for the AP. ■ **ap-mode**: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. ■ **am-mode**: Device behaves as an AM to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc. ■ spectrum-mode: Device behaves as a spectrum monitor, sending spectrum analysis data to the managed device. Spectrum monitors do not serve clients.
High throughput enable (radio)	Shows if high-throughput (802.11n) features on the 2.4 GHz frequency band are enabled or disabled.

Parameter	Description
Channel	Shows the channel number for the AP's 802.11a or 802.11n physical layer.
Beacon Period	Shows the time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	Enabling this setting introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air.
Transmit EIRP	Shows the current transmission power level.
Advertise 802.11d and 802.11h Capabilities	This column reports whether or not the AP will advertise its 802.11d (Country Information) and 802.11h (TPC) capabilities.
TPC Power	The transmit power advertised in the TPC IE of beacons and probe responses. Range: 0-51 dBm
Spectrum Load Balancing	The Spectrum Load Balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the managed device is responding to the wireless clients' probe requests. If enabled, the managed device compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.
Spectrum Load Balancing mode	Spectrum Load Balancing Mode allows control over how to balance clients. Select one of the following options: ■ **channel**: Channel-based load-balancing balances clients across channels. This is the default load-balancing mode ■ **radio**: Radio-based load-balancing balances clients across APs
Spectrum load balancing update interval	This value determines how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.
Advertised regulatory max EIRP	A cap for an radio's maximum EIRP. Even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons.
Spectrum load balancing domain	Define a spectrum load balancing domain to manually create RF neighborhoods. This option creates RF neighborhood information for networks that have disabled ARM scanning and channel assignment. ■ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is *not* defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain *isalso* defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.

Parameter	Description
`Rx sensitivity tuning based channel reuse`	The channel reuse feature can operate in either of the following three modes; static, dynamic or disable. (This feature is disabled by default.) ■ **Static mode**: This mode of operation is a coverage-based adaptation of the CCA thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ **Dynamic mode**: In this mode, the CCA thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ **Disable mode**: This mode does not support the tuning of the CCA Detect Threshold.
`Rx sensitivity threshold`	RX Sensitivity Tuning Based Channel Reuse Threshold, in -dBm. If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (in -dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. If the value is set to zero, the feature will automatically determine an appropriate threshold
`Non 802.11a interference Immunity`	The value for 802.11 Interference Immunity. This parameter sets the interference immunity on the 2.4 GHz band. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferes (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: ■ Level-0: no ANI adaptation. ■ Level-1: noise immunity only. ■ Level-2: noise and spur immunity. This is the default setting ■ Level-3: level 2 and weak OFDM immunity. ■ Level-4: level 3 and FIR immunity. ■ Level-5: disable PHY reporting.
`Enable CSA`	Displays whether or not the AP has enabled CSAs for 802.11h.
`CSA Count`	Number of channel switch announcements that must be sent before the AP will switch to a new channel.
`Management Frame Throttle interval`	Average interval that rate limiting management frames are sent from this radio, in seconds. If this column displays a zero rate limiting is disabled for this AP.
`Management Frame Throttle Limit`	Maximum number of management frames that can come from this radio in each throttle interval.
`ARM/WIDS Override`	Shows if ARM and Wireless IDS functions are enabled or disabled. If a radio is configured to operate in AM mode, then these functions are always enabled, regardless of this option.

Parameter	Description
`Protection for 802.11b Clients`	Displays whether or not protection for 802.11b clients is enabled or disabled.
`Maximum Distance`	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16 km. The upper limit for this parameter varies, depending on the 20/40 MHz mode for a 2.4 GHz frequency band radio: ■ 20 MHz mode: 54 km ■ 40 MHz mode: 24 km If you configure a value above the supported maximum, the maximum supported value will be used instead. Values below 600 m will use default settings.
`Spectrum Monitoring`	When this parameter is enabled, it turns an AP in ap-mode into a hybrid AP. An AP in hybrid AP mode will continue to serve clients as an access point while it scans and analyzes spectrum analysis data for a single radio channel.
`Assignment`	Displays whether or not ARM channel and power assignment has been enabled or disabled.
`Allowed bands for 40MHz channels`	Forty MHz channels may be used on the specified radio bands (802.11a or 802.11g).
`Client Aware`	Shows if the client aware feature has been enabled or disabled for this AP. If enabled, AP will not change channels when there are active clients.
`Max Tx Power`	Maximum transmission power for this AP, in dBm.
`Min Tx Power`	Minimum transmission power for this AP, in dBm.
`Multi Band Scan`	Shows if the multi-band scan feature has been enabled or disabled on this AP. If enabled, single-radio APs will try to scan across bands for Rogue AP detection.
`Rogue AP Aware`	Shows if the rogue AP awareness feature has been enabled or disabled on this AP. If enabled, the AP will try to contain off-channel Rogue APs.
`Scan Interval`	This parameter indicates, in seconds, how often the AP will leave its current channel to scan other channels in the band if scanning is enabled.
`Active Scan`	Displays whether or not the active scan feature is enabled. **NOTE:** This option elicits more information from nearby APs, but also creates additional management traffic on the network. **Active Scan** is disabled by default, and should *not be enabled* except under the direct supervision of Aruba Support.
`Scanning`	Shows if scanning is enabled or disabled for this AP. If this option is disabled, the following other options will also be disabled: ■ Multi Band Scan ■ Rogue AP Aware ■ Voip Aware Scan ■ Power Save Scan

Parameter	Description
Scan Time	The amount of time, in milliseconds, an AP will drift out of the current channel to scan another channel. The supported range for this setting is 0-2,147,483,647 seconds. Best practices are to configure a scan time between 50-200 msec.
VoIP Aware Scan	Shows if VoIP aware scanning is enabled or disabled. If you use voice handsets in the WLAN, **VoIP Aware Scan** should be enabled in the ARM profile so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that **Scanning** is also enabled.
Power Save Aware Scan	Shows if the power save aware scan is enabled or disabled. If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode. Default: enabled
Ideal Coverage Index	The Aruba coverage index metric is a weighted calculation based on the RF coverage for all Aruba APs and neighboring APs on a specified channel. The **Ideal Coverage Index** specifies the ideal coverage that an AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Acceptable Coverage Index	For multi-band implementations, the **Acceptable Coverage Index** specifies the minimal coverage an AP it should achieve on its channel. The denser the AP deployment, the lower this value should be.
Free Channel Index	The current free channel index value. The Aruba Interference index metric measures interference for a specified channel and its surrounding channels. This value is calculated and weighted for all APs on those channels (including 3rd-party APs). An AP will only move to a new channel if the new channel has a lower interference index value than the current channel. **Free Channel Index** specifies the required difference between the two interference index values before the AP moves to the new channel. The lower this value, the more likely it is that the AP will move to the new channel.
Backoff Time	After an AP changes channel or power settings, it waits for this backoff time interval before it asks for a new channel or power setting.
Error Rate Threshold	The minimum percentage of PHY errors and MAC errors in the channel that will trigger a channel change.
Error Rate Wait Time	Minimum time in seconds the error rate on the AP has to exceed its defined error rate threshold before it triggers a channel change.
Noise Threshold	Maximum level of noise in a channel that triggers a channel change.
Noise Wait Time	Minimum time in seconds the noise level has to exceed the Noise Threshold before it triggers a channel change on the AP.
Minimum Scan Time	Minimum number of times a channel must be scanned before it is considered for assignment. Best practices are to configure a **Minimum Scan Time** between 1-20 scans.
Load aware Scan Threshold	The **Load Aware Scan Threshold** is the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high.

Parameter	Description
Mode Aware Arm	Shows if the mode-aware ARM feature has been enabled or disabled for this AP. If enabled, ARM will turn the AP into an AMs if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).
Scan mode	Identifies the scan mode for the AP. ■ **all-reg-domain**: The AP scans channels within all regulatory domains. This is the default setting. ■ **reg-domain**:Limit the AP scans to just the regulatory domain for that AP.
40 MHz intolerance	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.
Honor 40 MHz intolerance	Shows if 40 MHz intolerance is enabled or disabled. If enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Legacy station workaround	Shows if interoperability for misbehaving legacy stations is enabled or disabled.
SSID enable	Shows if the SSID is enabled or disabled
ESSID	Name that uniquely identifies the Extended SSID.
Encryption	Encryption type used on this AP.
DTIM Interval	Shows the interval, in milliseconds, between the sending of DTIMs in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed.
Basic Rates	Lists supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses from this AP.
Transmit Rates	Lists 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error or loss rate of the client.
Station Ageout Time	Time, in seconds, that a client is allowed to remain idle before being aged out.
Max Transmit Attempts	Maximum number of retries allowed for the AP to send a frame
RTS Threshold	Wireless clients transmitting frames larger than this threshold must issue RTS and wait for the AP to respond with CTS. This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting.
Short Preamble	Shows if a short preamble for 802.11b/g radios is enabled or disabled for this AP. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.

Parameter	Description
Max Associations	Maximum number of wireless clients allowed to associate to the AP
Wireless Multimedia (WMM)	Shows if Wireless Multimedia (WMM) is enabled or disabled for this AP. WMM provides prioritization of specific traffic relative to other traffic in the network
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	Shows if Wireless Multimedia (WMM) UAPSD powersave is enabled or disabled.
WMM TSPEC Min Inactivity Interval	Displays the minimum inactivity time-out threshold of WMM traffic for this AP.
DSCP mapping for WMM voice AC	Displays the DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	Displays the DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	Displays the DSCP value used to map WMM best-effort traffic
DSCP mapping for WMM background AC	Displays the DSCP value used to map WMM background traffic.
902il Compatibility Mode	Shows if 902il compatibility mode is enabled or disabled. (This parameter only needs to be enabled for APs with associated clients using NTT DoCoMo 902iL phones.)
Hide SSID	Shows if the feature to hide a SSID name in beacon frames is enabled or disabled.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if local probe response is enabled or disabled on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the controller sends the 802.11 probe responses
Disable Probe Retry	If disabled, the AP will not resend probes if it does not get a response.
Battery Boost	Shows if the battery boost feature is enabled or disabled for the AP. If enabled, this feature converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life
Drop Broadcast and Multicast	If this feature is enabled on an AP, it drops all downstream broadcast or multicast traffic to increase battery life.
WEP Key 1	Displays the static WEP key (1 of 4).
WEP Key 2	Displays the static WEP key (2 of 4).
WEP Key 3	Displays the static WEP key (3 of 4).

Parameter	Description
WEP Key 4	Displays the static WEP key (4 of 4).
WEP Transmit Key Index	Displays the key index that specifies which static WEP key is to be used.
WPA Hexkey	Displays the WPA PSK.
WPA Passphrase	Displays the WPA passphrase with which the AP generates a PSK.
Maximum Transmit Failures	Display the maximum number of transmission failures allowed before the client gives up.
BC/MC Rate Optimization	Shows if the AP has enabled or disabled scanning of all active stations currently associated to that AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
Rate Optimization for delivering EAPOL frames	Shows if the AP has enabled or disabled rate optimization for delivering EAPOL frames.
Strict Spectralink Voice Protocol (SVP)	Shows if strict SVP is enabled or disabled.
802.11g Beacon Rate	Sets the beacon rate for 802.11g for APs use a DAS. Using this parameter in normal operation may cause connectivity problems.
802.11a Beacon Rate	Sets the beacon rate for 802.11a for APs use a DAS. Using this parameter in normal operation may cause connectivity problems.
Advertise QBSS Load IE	Shows if the AP has enabled or disabled the advertising of QBSS in the load IE.
High throughput enable (SSID)	Shows if the AP has enabled or disabled the use of its high-throughput SSID in 40 MHz mode.
40 MHz channel usage	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate.
MPDU Aggregation	Shows if the AP has enabled or disabled MDPU aggregation.
Max transmitted A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be sent on the AP's high-throughput SSID.
Max received A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be received on the AP's high-throughput SSID.
Min MPDU start spacing	Displays the minimum time between the start of adjacent MDPUs within an aggregate MDPU, in microseconds.
Supported MCS set	Comma-separated list of MCS values or ranges of values to be supported on this high-throughput SSID.
Short guard interval in 20 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 20 MHz mode of operation.
Short guard interval in 40 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 40 MHz mode of operation.

Parameter	Description
Maximum number of spatial stream usable for STBC transmission	Controls the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series and AP-105 only. The configured value will be adjusted based on AP capabilities.)
Minimum number of spatial stream usable for STBC transmission	Controls the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series, and AP-105 only. The configured value will be adjusted based on AP capabilities.)
Legacy stations	Shows if the AP has enabled or disabled the legacy stations option, which controls whether or not legacy (non-HT) stations are allowed to associate with the AP's SSID. By default, legacy stations are allowed to associate. **NOTE:** This setting has no effect on a BSS in which HT support is not available.
Allow weak encryption	Shows if the AP has enabled or disabled the weak encryption option. The use of TKIP or WEP for unicast traffic forces the use of legacy transmissions rates. Disabling this mode prevents the association of stations using TKIP or WEP for unicast traffic. This mode is disabled by default.
Virtual AP enable	WLAN profiles configure WLANs in the form of virtual AP profiles. This parameter shows if the AP has enabled or disabled virtual APs.
Allowed band	Shows the band(s) on which to use the virtual AP: ■ a—802.11a band only (5 GHz) ■ g—802.11b/g band only (2.4 GHz) ■ all—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)
VLAN	Shows the VLAN(s) into which users are placed in order to obtain an IP address.
Forward mode	Shows the current forward mode (tunnel, bridge, split-tunnel, or decrypt-tunnel) for the virtual AP. This parameter controls whether 802.11 frames are tunneled to the controller using GRE, bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the controller, and Internet access remains local). When an AP is configured to use the decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the controller, which then applies firewall policies to the user traffic. When the controller sends traffic to a client, the controller sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client. Only 802.1X authentication is supported when configuring bridge or split tunnel mode.
Deny time range	Shows the time range for which the AP will deny access for a virtual AP.
Mobile IP	Shows if IP mobility has been enabled or disabled for the virtual AP.

Parameter	Description
`HA Discovery on-association`	If enabled, home agent discovery is triggered on client association instead of home agent discovery based on traffic from client. Mobility on association can speed up roaming and improve connectivity for clients that do not send many uplink packets to trigger mobility (VoIP clients). Best practice is to keep this parameter disabled as it increases IP mobility control traffic between controllers in the same mobility domain. Enable this parameter only when voice issues are observed in VoIP clients. **NOTE:** `ha-disc-onassoc` parameter works only when IP mobility is enabled and configured on the controller.
`DoS Prevention`	Shows the status of the Dos Prevention option. If enabled, virtual APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.
`Station Blacklisting`	Shows if the virtual AP has enabled or disabled detection of DoS attacks, such as ping or SYN floods, that are not spoofed deauth attacks.
`Blacklist Time`	Shows the number of seconds that a client will be quarantined from the network after being blacklisted.
`Authentication Failure Blacklist Time`	Shows the time, in seconds, a client is blocked if it fails repeated authentication. If the virtual AP shows a value of 0, a blacklisted client is blocked indefinitely.
`Fast Roaming`	Shows if the AP has enabled or disabled fast roaming.
`Strict Compliance`	If enabled, the virtual AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.
`VLAN Mobility`	Shows if a virtual AP has enabled or disabled VLAN (Layer-2) mobility
`Remote-AP Operation`	Shows when the virtual AP operates on a remote AP: ■ **always**—Permanently enables the virtual AP (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ **backup**—Enables the virtual AP if the remote AP cannot connect to the controller (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ **persistent**—Permanently enables the virtual AP after the remote AP initially **connects** to the controller (Bridge Mode only). This option can be used for any (Open/PSK/802.1X) bridge VAPs. ■ **standard**—Enables the virtual AP when the remote AP connects to the controller. This option can be used for any (bridge/split-tunnel/tunnel/d-tunnel) VAPs.
`Convert Broadcast ARP requests to unicast`	If this option is enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the **show ap active** and the **show datapath** tunnel command. If enabled, the output will display the letter **a** in the flags column.

Parameter	Description
`Band Steering`	Shows if band-steering has been enabled or disabled for a virtual AP. ARM's band steering feature encourages dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40 MHz or 20 MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.

Related Commands

Command	Description
ap system-profile rf dot11g-radio-profile rf arm-profile rf ht-radio-profile wlan ht-ssid-profile wlan virtual-ap	The output of the show ap config command displays the content of the profile settings for an individual AP or AP group. Use the commands displayed in the column to the left to configure these parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap consolidated-provision info

```
show ap consolidated-provision info
   ap-name <ap-name>
   ip-addr <ip-address>
   ip6-addr <ipv6-address>
```

Description

This command shows the consolidated provision details of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows consolidated provision information based on the AP name.
`ip-addr <ip-address>`	Shows consolidated provision information based on the IP address of an AP.
`ip6-addr <ipv6-address>`	Shows consolidated provision information based on the IPv6 address of an AP.

Usage Guidelines

This command shows the consolidated provision details of an AP.

Examples

The following example shows the consolidated provision details of an AP with name xxxxx-ap-135.

```
(host) #show ap consolidated-provision info ap-name xxxxx-ap-135
ap name: xxxxx-ap-135
ipv4 address type: dynamic
ipv4 address: 10.17.160.247
ipv4 netmask: 255.255.255.0
ipv4 gateway: 10.17.160.2
ipv4 lease: 43200
ipv4 dhcp server: 10.17.160.2
ipv4 dns server: 10.13.6.110, 0.0.0.0
ipv6 address: none
master: 10.17.160.4
master discover type: Provisioned manually
previous lms: none
lms addrs [0]: 10.17.160.4
```

The output of this command includes the following parameters.

Parameter	Description
`ap name`	The name of the AP for which consolidated provisioned information is required.
`ipv4 address type`	The IPv4 address type of the AP.
`ipv4 address`	The IPv4 address of the AP.

Parameter	Description
`ipv4 netmask`	The IPv4 subnet mask of the AP.
`ipv4 gateway`	The IPv4 gateway information of the AP.
`ipv4 lease`	The IPv4 lease information pertaining to the AP.
`ipv4 dhcp server`	The IPv4 DHCP server of the AP.
`ipv4 dns server`	The IPv4 DNS server of the AP.
`ipv6 address`	The IPv6 address of the AP.
`master`	The IP address of the AP's Mobility Master.
`master discover type`	The Mobility Master discovery (provisioning) type information for the AP
`previous lms`	The previous LMS IP address of the AP.
`lms addrs`	The LMS IP address of the AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap-crash-transfer

```
show ap-crash-transfer
```

Description

This command displays info for the AP crash transfer feature, which transfers AP coredump files to the controller flash memory if no dumpserver is configured.

Syntax

No Parameters

Usage Guidelines

The command **ap system-profile <profile> dump-server <server>** specifies a server to receive a core dump generated when an AP process crashes. If no dump server is configured, issue the **ap-crash-transfer** command to save dump files to the controller flash memory.

If you define a dump server and issue the ap-crash-server command, the dump server configuration takes precedence, and coredump files are sent to the dump server.

Example

```
(host)) #show ap-crash-transfer
AP Crash Transfer:enabled
AP Crash folder limit:50 MB (non-editable)
```

Related Commands

Command	Description
ap-crash-transfer	This command allows AP coredump files to be transferred to the controller flash memory if no dumpserver is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Mode
All platforms	Base operating system	Enable or config mode on managed devices

show ap database

```
show ap database
   flags <flags>
   group {default|noauthapgroup|<group>}
   inactive {flags|group|indoor|local|long|outdoor|page|sort-by|sort-
   direction|start|status|switch|type|unprovisioned|usb}
   indoor {flags|group|inactive|local|long|outdoor|page|sort-by|sort-
   direction|start|status|switch|type|unprovisioned|usb}
   local {flags|group|inactive|indoor|long|outdoor|page|sort-by|sort-
   direction|start|status|switch|type|unprovisioned|usb}
   long {flags|group|inactive|indoor|local|outdoor|page|sort-by|sort-
   direction|start|status|switch|type|unprovisioned|usb}
   outdoor {flags|group|inactive|indoor|local|long|page|sort-by|sort-
   direction|start|status|switch|type|unprovisioned|usb}
   page <page> {flags|group|inactive|indoor|local|long|outdoor|sort-by|sort-
   direction|start|status|switch|type|unprovisioned|usb}
   sort-by {ap-flags|ap-group|ap-ip|ap-mac|ap-name|ap-serial|ap-
   type|fqln|provisioned|status|switch-ip|uptime}
   sort-direction {ascending|descending}
   start <start>
   status {up|down}
   switch <switch-ip-addr>
   type {cap|mesh|rap}
   unprovisioned {flags|group|inactive|indoor|local|long|outdoor|page|sort-by|sort-
   direction|start|status|switch|type|usb}
   usb {flags|group|inactive|indoor|local|long|outdoor|page|sort-by|sort-
   direction|start|status|switch|type|unprovisioned}
```

Description

This commands shows the list of access points in the database.

Syntax

Parameter	Description
`flags`	Shows only access points with specified flags [LUDINRCc12ME].
`group <group>`	Shows only access points in specified AP group.
`inactive`	Shows only local access points with no active BSSIDs or wired AP interfaces.
`indoor`	Shows only indoor access points.
`local`	Shows only access points connected to this managed device.
`long`	Shows following additional columns for access points: ■ Wired MAC Address, ■ Serial # ■ Port ■ FQLN
`outdoor`	Shows only outdoor access points.
`page <page>`	Shows only specified number of access points.

Parameter	Description
`sort-by`	Shows access points filtered by following columns: ■ ap-flags ■ ap-group ■ ap-ip ■ ap-mac ■ ap-name ■ ap-serial ■ ap-type ■ fqln ■ provisioned ■ status ■ switch-ip ■ uptime
`sort-direction`	Shows access points in sorted in following sequence: ■ ascending ■ descending
`start <start>`	Shows access points from the specified AP index number.
`status`	Shows access points sorted by following status: ■ down ■ up
`switch <switch-ip-addr>`	Shows access points registered with a specified managed device.
`unprovisioned`	Shows only unprovisioned access points.
`usb`	Shows USB related parameters.

Usage Guidelines

Many of the parameters in this command can be used together to filter a large database of information down to just the AP data you want to see. For example, you can issue the command **show ap database group <group> local status up** to view a list of local APs within a specific AP group that are reporting an **up** status. Include the **sort-by** and **sort-direction** keywords to specify how the data is sorted in the output of this command.

Examples

The following example shows shows the information of the access points in the group **default**. The output also includes a description of the flag types that may appear in the **Flags** column.

```
(host) [mynode] #show ap database group default

AP Database
-----------
Name    Group    AP Type  IP Address       Status             Flags  Switch IP      Standby IP
----    -----    -------  ----------       ------             -----  ---------      ----------
ap-205  default  205      191.191.191.252  Up 10d:8h:8m:6s           192.192.189.1  0.0.0.0
ap-215  default  215      191.191.191.253  Up 33d:14h:1m:37s         192.192.189.1  0.0.0.0

Flags:  U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed
        I = Inactive; D = Dirty or no config; E = Regulatory Domain Mismatch
        X = Maintenance Mode; P = PPPoE AP; B = Built-in AP; s = LACP striping
        R = Remote AP; R- = Remote AP requires Auth; C = Cellular RAP;
        c = CERT-based RAP; 1 = 802.1X authenticated AP; 2 = Using IKE version 2
        u = Custom-Cert RAP; S = Standby-mode AP; J = USB cert at AP
```

```
        i = Indoor; o = Outdoor
        M = Mesh node; Y = Mesh Recovery
        z = Datazone AP

Total APs:2
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap database-summary

```
show ap database-summary
```

Description

Show a general summary of access point information for this controller.

Usage Guidelines

Use this command to show the current number of active APs and Air Monitors. This command is also useful for determining how many unprovisioned APs or duplicate APs are on the network. For full details on each AP registered to a controller, use the command show ap database.

Examples

The output of this command shows that this controller can detect a total of five APs, four up, and one down.

```
AP Database Summary
-------------------
AP Mode               Total Up  Total Down  Total Upgrading*  Total Rebooting*  RAP Up  RAP
Down  RAP Upgrading*  RAP Rebooting*
-------               --------  ----------  ----------------  ----------------  ------  -------
-  --------------  --------------
Access Points         4         1           0                 0                 0       0
  0               0
Air Monitors          0         0           0                 0                 0       0
  0               0
Wired Access Points   0         0           0                 0                 0       0
  0               0
Mesh Portals          0         0           0                 0                 0       0
  0               0
Mesh Points           0         0           0                 0                 0       0
  0               0
Spectrum Monitors     1         1           0                 0                 0       0
  0               0

*Upgrading and Rebooting counts only reflect APs registered on this controller.
```

The output of this command includes the following information:

Column	Description
`Total Up`	Total number of APs with an *up* status.
`Total Down`	Total number of APs with a *down* status.
`IPSEC Up`	Total number of APs with an active (up) IPsec tunnel.
`IPSEC Down`	Total number of APs with an inactive (down) IPsec tunnel.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug acl-table

```
show ap debug acl-table {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
```

Description

This command shows ACL table in AP datapath.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows ACL table in AP datapath of an AP specified by AP name.
`ip-addr <ip-addr>`	Shows ACL table in AP datapath of an AP specified by IP address.
`ip6-addr <ip6-addr>`	Shows ACL table in AP datapath of an AP specified by IPv6 address.

Usage Guidelines

This command shows ACL table in AP datapath. For the remaining parameters, see the command syntax.

Example

The following example shows ACL table in AP datapath for an AP named ap-205:

```
(host) [mynode] #show ap debug acl-table ap-name ap-205

acl_2700: entries 21@7680, role, ACL 2700:, acl_flags:0000
0: any any    6  0-65535  80-80  f0000000000080001
1: any any    6  0-65535  135-135  f0000000000080001
2: any any    6  0-65535  445-445  f0000000000080001
3: any any  17  0-65535  67-68  f0000000000080001
4: any any  17  0-65535  53-53  f0000000000080001
5: any any  17  0-65535  123-123  f0000000000080001
6: any any    6  0-65535  23-23  f0000000000080001
7: any any  17  0-65535  69-69  f0000000000080001
8: any any    1  0-65535  2048-2048  f0000000000080001
9: any any    1  0-65535  0-65535  f0000000000080001
10: any any  17  8211-8211  8211-8211  f0000000000080001  hits 41037
11: any any  17  8209-8209  8209-8209  f0000000000080001
12: any any  17  0-65535  514-514  f0000000000080001
13: any any    0  0-65535  0-65535  f0000000000080001
14: user any  17  0-65535  500-500  f0000000000080001
15: any user  17  500-500  500-500  f0000000000080001
16: user any  17  0-65535  4500-4500  f0000000000080001
17: any user  17  4500-4500  4500-4532  f0000000000080001
18: user any  17  0-65535  53-53  f0000000000080001
19: user any  17  53-53  53-85  f0000000000080001
20: any any    0  0-0  0-0  f0000000000180000
acl_2701: entries 1@7700, role, ACL 2701:, acl_flags:0000
0: any any    0  0-0  0-0  f0000000000180000
acl_2702: entries 2@7701, role, ACL 2702:, acl_flags:0000
0: any 192.168.11.0 255.255.255.0    0  0-0  0-0  f0000000000180001
1: any any    0  0-65535  0-65535  f0000000000180050  po0
acl_2703: entries 1@7703, role, ACL 2703:, acl_flags:0000
0: any any    0  0-0  0-0  f0000000000180001
acl_2704: entries 5@7704, role, ACL 2704:, acl_flags:0000
0: any any    0  0-0  0-0  f0000000000000000
```

```
1: any any   0   0-0   0-0   f0000000000180011   po0
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug aid-table

```
show ap debug aid-table bssid <bssid> [advanced]
```

Description

This command shows the association ID table.

Syntax

Parameter	Description
`bssid <bssid> [advanced]`	Shows association ID table of the specified BSSID.

Usage Guidelines

This command shows the association ID table. For the remaining parameters, see the command syntax.

Example

The following example shows association ID table for the BSSID 00:1a:1e:aa:bb:cc:

```
(host) [mynode] #show ap debug aid-table bssid 00:1a:1e:aa:bb:cc [advanced]

AP Association-ID Table for BSSID: d8:c7:c8:38:fc:f5
---------------------------------------------------
AID  MAC
---  ---
1    80:86:f2:41:1f:1d
2    80:86:f2:41:1e:f0
3    80:86:f2:41:1e:be

Total AID count: 3
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap debug airmatch-reports

```
show ap debug airmatch-reports {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]
```

Description

This command displays information about AirMatch updates on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AirMatch data on an AP specified by AP name.
`ip-addr <ip-addr>`	Shows AirMatch data on an AP specified by IP address.
`ip6-addr <ip6-addr>`	Shows AirMatch data on an AP specified by IPv6 address.

Usage Guidelines

Issue this command to show AirMatch measurement settings applied to the selected AP, as well as information about the last update for different AirMatch reports.

Example

The following example shows the latest AirMatch statistics on the AP **Floor2-west.**

```
(Host) [node] #show ap debug airmatch-report ap-name Floor2-west

AirMatch measure info
---------------------
report period (mins)  measure duration (mins)  measure state  report enabled
--------------------  ------------------------  -------------  --------------
5                     5                         in progress    yes
AirMatch report info
--------------------
AirMatch Report Type  Count  Last Update Time
--------------------  -----  ----------------
reporting radio       2      2016-07-05 22:01:12
neighbors             8000   2016-07-06 22:46:09
feasibility           730    2016-07-06 22:47:44
event                 0      no update
```

The output of this command includes the following information:

Parameter	Description
`report period`	The AirMatch report period in the ap system profile
`measure duration`	The AirMatch measure duration in the ap system profile
`measure state`	The current AirMatch measurement state. Possible states are in **progress**, **stopped**, and **waiting**.
`Report enabled`	This value is expected to be the same as the **airmatch-report-enabled** setting in the ap system profile.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug anyspot-stats

```
show ap debug anyspot-stats {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
{radio <radio>}
```

Description

This command shows anyspot statistics of a radio on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows anyspot statistics of a radio on an AP specified by AP name.
`ip-addr <ip-addr>`	Shows anyspot statistics of a radio on an AP specified by IP address.
`ip6-addr <ip6-addr>`	Shows anyspot statistics of a radio on an AP specified by IPv6 address.
`radio <radio>`	Shows ACL table in AP datapath of AP specified by radio ID (either 0 or 1).

Usage Guidelines

This command shows anyspot statistics of a radio on an AP. For the remaining parameters, see the command syntax.

Example

The following example shows anyspot is disabled on radio 0 of an AP named ap-205:

```
(host) [mynode] #show ap debug anyspot-stats ap-name ap-205 radio 0

Anyspot is disabled on the specified radio!
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug backup-vap

```
show ap debug backup-vap {[ap-name <ap-name>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>]}
```

Description

This command shows backup VAP for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows backup VAP for an AP for specified AP name.
`ip-addr <ip-addr>`	Shows backup VAP for an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows backup VAP for an AP for specified IPv6 address.

Usage Guidelines

This command shows backup VAP for an AP. For the remaining parameters, see the command syntax.

Example

The following example shows backup VAP for an AP named ap-205:

```
(host) [mynode] #show ap debug backup-vap ap-name ap-205

AP backup ssid debug information
--------------------------------
Item    Value
----    -----
Host    192.192.189.1
Config  Mode:off  Band:all
Run:    Telnet[N] Enable[0] aruba015[N] aruba115[N]
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug bandwidth-management

```
show ap debug bandwidth-management [ap-name <ap-name>|ip-addr <ip-addr>
|ip6-addr <ip6-addr>]
```

Description

This command shows bandwidth management information for clients.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the access point.
`ip-addr <ip-addr>`	IP address of the access point.
`ip6-addr <ip6-addr>`	IPv6 address of the access point

Examples

The output of this command shows interface and shaping and interface policy for this AP.

```
(host) #show ap debug bandwidth-management ap-name amit-ap-105
Interface :wifi0
Shaping policy:Default-access (no stats)
Interface :wifi1
Shaping policy:Default-access (no stats)
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug ble-config

```
show ap debug ble-config {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the Bluetooth Low Energy (BLE) configuration of the AP. In addition, the command displays the update interval to the Beacon Management Console (BMC), BLE token, AP Beacon (APB) status, the last update time to BMC, and the beacon MAC for which the last update was sent.

This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Syntax

Parameter	Description
`ap-name`	Displays the BLE configuration of an AP for a specific AP based on the AP name.
`ip-addr`	Displays the BLE configuration of an AP for a specific AP based on the IPv4 address.
`ip6-addr`	Displays the BLE configuration of an AP for a specific AP based on the IPv6 address.

Example

The output of this command displays the update interval to the Beacon Management Console (BMC), BLE token, AP Beacon (APB) status, the last update time to BMC, and the beacon MAC for which the last update was sent.

```
(host) #show  ap debug ble-config ap-name ap325
BLE Configuration
-----------------
Item                            Value
----                            -----
LMS IP                          192.0.2.1
Authorization Token             YzJlNmEzOTMtYjE4MC00ZTc4LWJmNDEtMzMzNGEyY2NjY2RmOj
                                Y4YzBhOWI2LWYxMGQtNGZlMi05YmVkLTI5ZTY5MDNkYjhmYQ==
Endpoint URL                    https://edit.meridianapps.com/api/beacons/manage
BLE Ready                       Yes
Update Intvl (in sec)           300
BLE debug log                   Enabled
Operational Mode                Beaconing (APB: Beaconing)
Uplink Status                   Up (APB: -NA-)
APB Connection Status           0
Last BLE Device Update Attempt  c4:be:84:19:ef:99
Last Update Sent Time           2015-09-27 11:45:50
-----------------
Note: Uplink status is applicable only for Dynamic Console operational mode.
For APBs of type LS-BT1USB, applied operational mode is Beaconing if ap system profile setting
is either Persistent or Dynamic.
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug ble-counters

```
show ap debug ble-counters {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the packet counters for BLE devices seen by the AP. In addition, the command displays if any high power beacons are seen, the time at which configuration update was received for the beacons from the BMC and the updated response sent back.

This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Syntax

Parameter	Description
ap-name	Displays the packet counters for BLE devices seen by the AP for a specific AP based on the AP name.
ip-addr	Displays the packet counters for BLE devices seen by the AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the packet counters for BLE devices seen by the AP for a specific AP based on the IPv6 address.

Example

The output of this command displays the packet counters for BLE devices seen by the AP. In addition, it displays if any high power beacons are seen, the time at which configuration update was received for the beacons from the BMC and the updated response sent back.

```
(host) #show  ap debug ble-counters ap-name ap325

BLE Device Table
----------------
MAC                Major#  Minor#  iBeacon     ScanRspV0   ScanRspV1   HiPwr       RSSI
---                ------  ------  -------     ---------   ---------   -----       ----
d0:39:72:d5:43:75  1000    1215           453           0          62           4  -71
c4:be:84:19:8b:a3  0       0              617           0           6           4  -81
c4:be:84:19:ec:67  0       0              604           0           1           4  -83
d0:39:72:d4:fa:9c  6       1                1           0           0           0  -89
c4:be:84:19:ef:99  1000    1374           126           0           0           0  --
78:a5:04:15:23:35  1000    1222           445           0          47           1  -70
c4:be:84:19:ec:2f  0       0              575           0           1           5  -84

LastUpdate  CfgRx     CfgTx
----------  -----     -----
4s          NoUpdate  NoUpdate
4s          NoUpdate  NoUpdate
4s          NoUpdate  NoUpdate
1292s       NoUpdate  NoUpdate
4s          NoUpdate  NoUpdate
4s          NoUpdate  NoUpdate
4s          NoUpdate  NoUpdate

Total beacons:7
Total serial bytes read from APB:138761
Total msg bytes processed:138761
Total serial bytes dropped:0
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug ble-log

```
show ap debug ble-log {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the BLE debug logs of the AP.

This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Syntax

Parameter	Description
ap-name	Displays the BLE debug logs of an AP for a specific AP based on the AP name.
ip-addr	Displays the BLE debug logs of an AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the BLE debug logs of an AP for a specific AP based on the IPv6 address.

Example

The output of this command displays BLE process logs in the AP.

```
(Aruba7220) #show  ap debug ble-log ap-name ap325
[2127]2015-10-27 11:45:50 ble_ap_send_bmrequest:377 ble_
token:YzJlNmEzOTMtYjE4MC00ZTc4LWJmNDEtMzMzNGEyY2NjY2RmOjY4YzBhOWI2LWYxMGQtNGZlMi05YmVkLTI5ZTY5
MDNkYjhmYQ==. length:100
[2127]2015-10-27 11:45:50 ble_ap_send_bmrequest:378 ble_
url:https://edit.meridianapps.com/api/beacons/manage. length:48
[2127]2015-10-27 11:45:50 construct_bmrequest_payload:1265 mac:d0:39:72:d4:fa:9c retry bmreq
later... some attr pending (1/1/1/0/0).
[2127]2015-10-27 11:45:50 construct_bmrequest_payload:1337 6/7 beacons added to JSON. Total
beacons processed:7/7
[2127]2015-10-27 11:45:50 ble_ap_send_bmrequest: Sending BMRequest msg to ble_relay@192.0.2.2
[100/48] jsonlen:2145
[2127]2015-10-27 11:45:51 ble_ap_handle_bmresponse_msg:222 Result from 172.20.1.1:8505
strlen:30 footer:0xdeadbeef
[2127]2015-10-27 11:45:51 dwas_command:(nil) 1.
[2127]2015-10-27 11:45:51 process_json_response_from_ble_relay:2623 next_sync[0]:300 dwas_
command[0]:(null) updates array size is 0.
[2127]2015-10-27 11:45:56 msglen=90 :: 04 ff 57 f5 00 06 99 ef 19 84 be c4 0d 01 02 03 01 83
01 02 e8 03 02 02 5e 05 0f 10 09 45 8c 20 45 86 4e d3 8d 2f a0 84 2a cb d6 e6 06 01 02 07 01
08 08 01 01 09 01 01 0a 01 01 0b 01 26 0c 04 20 07 01 00 18 0b db 19 00 00 02 99 ef 19 84 be
c4 1a 01 03 19 01 00 04 01 00
[2127]2015-10-27 11:45:56 update_ble_data:2347 cmd status: seq_num: 6619 (19db) app_err (0):
Good  sys_err: 0  progress (2): Done  upg_progress[0]: 0.
[2127]2015-10-27 11:45:58 ageout_ble_device:694 numentries:7 sizeof(ble_mon_data_t):520.
[2127]2015-10-27 11:46:16 msglen=90 :: 04 ff 57 f5 00 06 99 ef 19 84 be c4 0d 01 02 03 01 83
01 02 e8 03 02 02 5e 05 0f 10 09 45 8c 20 45 86 4e d3 8d 2f a0 84 2a cb d6 e6 06 01 02 07 01
08 08 01 01 09 01 01 0a 01 01 0b 01 26 0c 04 34 07 01 00 18 0b db 19 00 00 02 99 ef 19 84 be
c4 1a 01 03 19 01 00 04 01 00
[2127]2015-10-27 11:46:16 update_ble_data:2347 cmd status: seq_num: 6619 (19db) app_err (0):
Good  sys_err: 0  progress (2): Done  upg_progress[0]: 0.
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug ble-table

```
show ap debug ble-table {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the statistics for BLE devices seen by the AP. In addition, the command displays beacons seen by the APB, each of the beacons' attributes such as the Major-Minor numbers, Batter Level, Firmware version, time since the beacon was last heard by the APB.

This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Syntax

Parameter	Description
ap-name	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the AP name.
ip-addr	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the IPv4 address.
ip6-addr	Displays the statistics for the BLE devices seen by the AP for a specific AP based on the IPv6 address.

Example

The output of this command displays the statistics for BLE devices seen by the AP.

```
(host) #show  ap debug ble-table ap-name ap325

BLE Device Table
----------------
MAC                HW_Type    FW_Ver         Flags   Status  Batt(%)  RSSI  Major#  Minor#
---                -------    ------         -----   ------  -------  ----  ------  ------
d0:39:72:d5:43:75  LS-BT1     OAD A 1.1-25   0x0001  IAH     100      -71   1000    1215
c4:be:84:19:8b:a3  LS-BT1USB  OAD B 1.1-25   0x0003  IAH     USB      -83   0       0
c4:be:84:19:ec:67  OCTOMORE   OAD B 1.1-26   0x0003  IAH     --       -74   0       0
c4:be:84:19:ef:99  OCTOMORE   OAD B 1.1-38   0x0083  LIA     --       --    1000    1374
78:a5:04:15:23:35  LS-BT1     OAD A 1.1-25   0x0001  IAH     100      -79   1000    1222
c4:be:84:19:ec:2f  OCTOMORE   OAD B 1.1-26   0x0003  IAH     --       -83   0       0

UUID                                  Tx_Power  Last Update  Uptime
----                                  --------  -----------  ------
5D3BCC63-BD6B-4FAF-906F-91C91519A69B  13        8s           11h:3m:0s
4152554E-F99B-4A3B-86D0-947070693A78  14        4s           23h:51m:30s
4152554E-F99B-4A3B-86D0-947070693A78  14        0s           19h:38m:30s
09458C20-4586-4ED3-8D2F-A0842ACBD6E6  2         4s           18h:45m:0s
09458C20-4586-4ED3-8D2F-A0842ACBD6E6  13        0s           22h:36m:0s
4152554E-F99B-4A3B-86D0-947070693A78  14        0s           19h:39m:0s

Total beacons:6
APB UI:[0/NO_UPGRADE_REQD]:65535(0xffff) blks:0/0 rep:0  total:0(0x0)
APB UI:upg_b_status-next:0x00/ooo:0x00/next2:0x00/upg_
b:0x00/allrx:0x00/oooBlk:0x00/oooBlk:0x00/oooBlk:0x00
APB UI:upg_b_status_errs-inv_upg:0x00/inv_cmd:0x00/inv_op:0x00/buf_tl:0x00/good:0x00
APB UI:acks/ka-From APB:0x00/0x00 From app:0x00,0x00/0x00
APB UI Clock:Start:1969-12-31 16:00:00  End:1969-12-31 16:00:00  Current:2015-10-27 11:48:20
Note: Battery level for LS-BT1USB devices is indicated as USB.
```

```
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Status Flags:L:AP's local beacon; I:iBeacon; A: Aruba Beacon; H: Aruba HiPower Beacon
                :U:Image Upgrade Pending
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug ble-tag-report

```
show ap debug ble-tag-report {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the Bluetooth Low Energy (BLE) asset tags that are reported to the Beacon Management Console (BMC).

This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Syntax

Parameter	Description
`ap-name <ap-name>`	Displays the BLE asset tags for a specific AP based on the AP name.
`ip-addr <ip-addr>`	Displays the BLE asset tags for a specific AP based on the IPv4 address.
`ip6-addr <ip6-addr>`	Displays the BLE asset tags for a specific AP based on the IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host) #show ap debug ble-tag-report ap-name ap325
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug ble-update-status

```
show ap debug ble-update-status {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command displays the configuration update status for BLE devices seen by the AP. In addition, the command displays the active versus desired configuration based on the configuration received from the BMC (if any).

This command is supported in 210 Series, 220 Series (with external BLE USB), and 320 Series.

Syntax

Parameter	Description
ap-name	Displays the configuration update status for BLE devices seen by the AP based on the AP name.
ip-addr	Displays the configuration update status for BLE devices seen by the AP based on the IPv4 address.
ip6-addr	Displays the configuration update status for BLE devices seen by the AP based on the IPv6 address.

Example

The output of this command displays the configuration update status for BLE devices seen by the AP. In addition, the command displays the active versus desired configuration based on the configuration received from the BMC (if any).

```
(host) #show  ap debug ble-update-status ap-name ap325

BLE Device Table
----------------
BLE Device MAC     Attribute  Actual/Observed                       Desired/Pending
--------------     ---------  ---------------                      ---------------
d0:39:72:d5:43:75  Tx Power   13                                   13
d0:39:72:d5:43:75  Major      1000                                 1000
d0:39:72:d5:43:75  Minor      1215                                 1215
d0:39:72:d5:43:75  UUID       5D3BCC63-BD6B-4FAF-906F-91C91519A69B  5D3BCC63-BD6B-4FAF-906F-
91C91519A69B
d0:39:72:d5:43:75  DWAS       0                                    0
c4:be:84:19:8b:a3  Tx Power   14                                   14
c4:be:84:19:8b:a3  Major      0                                    0
c4:be:84:19:8b:a3  Minor      0                                    0
c4:be:84:19:8b:a3  UUID       4152554E-F99B-4A3B-86D0-947070693A78  4152554E-F99B-4A3B-86D0-
947070693A78
c4:be:84:19:8b:a3  DWAS       0                                    0
c4:be:84:19:ec:67  Tx Power   14                                   14
c4:be:84:19:ec:67  Major      0                                    0
c4:be:84:19:ec:67  Minor      0                                    0
c4:be:84:19:ec:67  UUID       4152554E-F99B-4A3B-86D0-947070693A78  4152554E-F99B-4A3B-86D0-
947070693A78
c4:be:84:19:ec:67  DWAS       0                                    0
d0:39:72:d4:fa:9c  ---        Ineligible                           Reason:Missing data
c4:be:84:19:ef:99  Tx Power   2                                    2
c4:be:84:19:ef:99  Major      1000                                 1000
c4:be:84:19:ef:99  Minor      1374                                 1374
```

```
c4:be:84:19:ef:99  UUID       09458C20-4586-4ED3-8D2F-A0842ACBD6E6  09458C20-4586-4ED3-8D2F-
A0842ACBD6E6
c4:be:84:19:ef:99  Firmware   1.1-38                                1.1-38 (Status:65535/0 -
NotRequired)
c4:be:84:19:ef:99  DWAS       0                                     0
78:a5:04:15:23:35  Tx Power   13                                    13
78:a5:04:15:23:35  Major      1000                                  1000
78:a5:04:15:23:35  Minor      1222                                  1222
78:a5:04:15:23:35  UUID       09458C20-4586-4ED3-8D2F-A0842ACBD6E6  09458C20-4586-4ED3-8D2F-
A0842ACBD6E6
78:a5:04:15:23:35  DWAS       0                                     0
c4:be:84:19:ec:2f  Tx Power   14                                    14
c4:be:84:19:ec:2f  Major      0                                     0
c4:be:84:19:ec:2f  Minor      0                                     0
c4:be:84:19:ec:2f  UUID       4152554E-F99B-4A3B-86D0-947070693A78  4152554E-F99B-4A3B-86D0-
947070693A78
c4:be:84:19:ec:2f  DWAS       0                                     0

Total beacons:7
Devices marked "Ineligible" are currently not capable of being upgraded.
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug bss-config

```
show ap debug bss-config [ap-name <ap-name>|bssid <bssid>||essid <essid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>|port <port>/<slot>]
```

Description

Show the configuration for each BSSID of an AP. This information can be used to troubleshoot problems on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Filter the AP Config table by AP name.
`bssid <bssid>`	Filter the AP Config table by BSSID. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`essid <essid>`	Filter the AP Config table by ESSID. An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	Filter the AP Config table by IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Filter the AP Config table by IP address by entering an IPv6 IP address in dotted-decimal format.
`port <port>/<slot>`	Filter the AP Config table by port and slot numbers. The slot and port numbers should be separated by a forward slash (/).

Examples

The output of this command shows the AP configuration table for a specific BSSID.

```
(host) #show ap debug bss-config
Aruba AP Config Table
---------------------
bss                ess   vlan ip          phy type fw-mode max-cl rates tx-rates preamble  mtu
---                ----  ---- --          --- ---- ------- -----  ----- -------- --------  ---
status wmm
------ ---
00:1a:1e:11:24:c2  cera2 66   10.6.1.203  g-HT ap  tunnel  64      0x3   0xfff   enable    0
enable enable
00:1a:1e:8d:5b:11  wpa2  65   10.6.1.198  a-HT ap  tunnel  20      0x150 0xff0   -         0
enable  enable
00:0b:86:9b:e5:60  guest 63   10.6.14.79  g    ap  tunnel  20      0x2   0x3fe   enable    0
enable  enable
00:1a:1e:97:e5:41  voip  66   10.6.1.199  g-HT ap  tunnel  20      0xc   0x14c   enable    0
enable enable
00:1a:1e:11:74:a1  voip  66   10.6.1.197  g-HT ap  tunnel  20      0xc   0x14c   enable    0
enable enable
00:1a:1e:11:5f:11  wpa2  65   10.6.1.200  a-HT ap  tunnel  20      0x150 0xff0   -         0
enable enable
```

The output of this command includes the following information:

Column	Description
bss	Basic Service Set (BSS) identifier, which is usually the AP's MAC address.
ess	Extended Service Set (ESS) identifier; a user-defined name for a wireless network.
vlan	The BSSID's VLAN number.
IP	The AP's IP address.
phy	One of the following 802.11 types ■ a ■ a-HT (high-throughput) ■ g ■ g-HT (high-throughput)
type	This column shows if the BSSID is for an access point (**ap**) or an air monitor (**am**).
fw-mode	The configured forward mode for the AP's virtual AP profile. ■ **bridge**: Bridge locally ■ **split-tunnel**: Tunnel to controller or NAT locally ■ **tunnel**: Tunnel to controller
max-cl	The maximum number of clients allowed for this BSSID.
preamble	Shows if short preambles are enabled for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using a short preamble.
MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
status	Shows if this BSSID is enabled or disabled.
wmm	Shows if the BSSID has enabled or disabled WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF) WMM provides prioritization of specific traffic relative to other traffic in the network.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug bss-stats

```
show ap debug bss-stats [bssid <bssid>]
```

Description

Show debug and troubleshooting statistics from a specific BSSID of an AP.

Syntax

Parameter	Description
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The example below shows part of the output of the command **show ap debug bss-stats bssid <bssid>**.

```
(host) #show ap debug bss-stats bssid 00:1a:1e:11:5f:11
BSSID Stats
-----------
BSSID Stats
-----------
Parameter                       Value
---------                       -----
--------------------            General
--------------------            Transmit
Tx Frames Rcvd                  972118
Tx Bcast Frames Rcvd            4139
Tx Frames Dropped               375241
Tx Bcast Frames Dropped         0
Tx Frames Transmitted           596088
Tx Bytes Rcvd                   633849487
Tx Bytes Transmitted            593931482
Tx Time Frames Rcvd             705492586
Tx Time Frames Dropped          397125178
Tx Time Frames Transmitted      308367408
Tx Success With Retry           91875
Tx Multiple Retries             467116
Tx Mgmt Frames                  502661
Tx Beacons Transmitted          3528036
Tx Probe Responses              502612
Tx Data Transmitted Retried     91867
Tx Data Transmitted             467744
Tx Data Frames                  469457
Tx Broadcast Data Frames In     4139
Tx Data Bytes Transmitted       580843154
Tx Data Bytes                   582581297
Tx Time Data Transmitted        173621140
Tx Time BC/MC Data              0
Tx Time Data dropped            4070686
Tx Time Data                    177691826
Tx Time Data (Ideal)            0
Tx Broadcast Data Frames Sent   4136
Tx Multicast Data Frames        4011
Tx DMO Multicast                0
Tx DMO Invalid                  0
Tx Data Frames  12 Mbps  (Mon)       0
```

```
Tx Data Frames  24 Mbps  (Mon)      0
Tx Data Frames  36 Mbps  (Mon)      0
Tx Data Frames  54 Mbps  (Mon)      0
Tx Data Frames  72 Mbps  (Mon)      0
Tx Data Frames 108 Mbps  (Mon)      0
Tx Data Frames 300 Mbps  (Mon)      22651
Tx Data Frames 450 Mbps  (Mon)      0
Tx Data Frames 1300 Mbps  (Mon)     0
Tx Data Frames 1300 Mbps+ (Mon)     0
Tx Data Bytes   12 Mbps  (Mon)      0
Tx Data Bytes   24 Mbps  (Mon)      0
Tx Data Bytes   36 Mbps  (Mon)      0
Tx Data Bytes   54 Mbps  (Mon)      0
Tx Data Bytes   72 Mbps  (Mon)      0
Tx Data Bytes  108 Mbps  (Mon)      0
Tx Data Bytes  300 Mbps  (Mon)      34300555
Tx Data Bytes  450 Mbps  (Mon)      0
Tx Data Bytes  1300 Mbps  (Mon)     0
Tx Data Bytes  1300 Mbps+ (Mon)     0
Tx 6 Mbps                           11
Tx HT 130 Mbps                      22651
Tx WMM [BE]                         22651
Tx UAPSD OverflowDrop               0
Tx Mgmt Bytes                       547
...
```

The output of this command includes the following information:

Parameter	Description
`Tx Frames Rcvd`	Number of transmitted frames that were received.
`Tx Bcast Frames Rcvd`	Number of transmitted broadcast frames that were received.
`Tx Frames Dropped`	Number of transmitted frames that were dropped.
`Tx Bcast Frames Dropped`	Number of transmitted broadcast frames that were dropped.
`Tx Frames Transmitted`	Number of frames successfully transmitted.
`Tx Bytes Rcvd`	Number of transmitted bytes received.
`Tx Bytes Transmitted`	Number of transmitted bytes.
`Tx Time Frames Rcvd`	Number of times transmitted frames were received.
`Tx Time Frames Dropped`	Number of times transmitted frames were dropped.
`Tx Time Frames Transmitted`	Number of times frames were transmitted.
`Tx Success With Retry`	Number of frames that were successfully transmitted after being retried.
`Tx Multiple retries`	Number of frames that were successfully transmitted after being retried multiple times.
`Tx Mgmt Frames`	Number of management frames transmitted.
`Tx Beacons Transmitted`	Number of beacons transmitted.

Parameter	Description
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Transmitted Retried	Number of retried data frames.
Tx Data Transmitted	Number of transmitted data frames.
Tx Data Frames	Number of transmitted data frames.
Tx Broadcast Data Frames In	Number of broadcast data frames received by the AP from wired interface to be transmitted in the air.
Tx Data Bytes Transmitted	Total data bytes received by an AP from its wired interface to be transmitted over the air.
Tx Data Bytes	Total data bytes transmitted by the AP over the air.
Tx Time BC/MC Data	Total time spent transmitting broadcast/multicast frames.
Tx Time Data dropped	Total time spent transmitting dropped frames.
Tx Time Data	Total time spent sending frames received for transmission, including the frames that were dropped after retrying.
Tx Broadcast Data Frames Sent	Broadcast data frames transmitted by the AP.
Tx Multicast Data Frames	Multicast data frames transmitted by the AP.
Tx DMO Multicast	**NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx DMO Invalid	**NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx DMO Converted	**NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APsin bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx DMO Replicated	**NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APsin bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx DMO Dropped	**NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APsin bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx DMO No Client	Number of times no client was found for an association-ID indicated by the frame. (This value is typically normally 0.) **NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APs in bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.

Parameter	Description
Tx DMO No BSSID	Number of times the BSSID indicated by the frame was not found. (This value is typically normally 0.) **NOTE:** This counter applies to APs in decrypt-tunnel or split forwarding modes only. They may also increment for Instant APsin bridge forwarding mode if the Instant AP performs bridge-mode multicast conversion.
Tx Unicast Data Frames	Number of transmitted unicast data frames.
Tx RTS Success	Number of Ready To Send (RTS) frames successfully transmitted.
Tx RTS Failed	Number of Ready To Send (RTS) frames that were not successfully transmitted
Tx CTS Frames	Number of Clear-to-Send (CTS) frames transmitted.
Tx Dropped After Retry	Number of frames dropped after an attempted retry.
Tx Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Tx Missed ACKs	Number of retries triggered because an acknowledgement was not received.
Tx EAPOL Frames	Number of EAPOL frames transmitted
TX STBC Frames	Number of transmitted frames with Space-time block coding (STBC) enabled.
TX LDPC Frames	Number of transmitted frames with Low Density Parity Check (LDPC) enabled.
Tx WMM	Number of Wi-fi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. ■ Tx WMM [BE]: Best Effort ■ Tx WMM [BK]: Background ■ Tx WMM [VO]: VoIP ■ Tx WMM [VI]: Video
Tx Data <value> Mbps	Number of frames transmitted at the specified rate, (Mbps).
Tx Data Bytes <value> Mbps	Number of bytes of data transmitted at the specified rate, (Mbps).
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
Tx Mgmt Bytes	Total management frame bytes transmitted.
Tx Beacons Bytes	Total number of Beacon frame bytes transmitted.
Tx AMSDU pkt count	Total number of AMSDU bytes transmitted.

Parameter	Description
Tx Data Frames/Bytes 24 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (12-24)
Tx Data Frames/Bytes 36 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (24-36)
Tx Data Frames/Bytes 54 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (36-54)
Tx Data Frames/Bytes 72 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (54-72)
Tx Data Frames/Bytes 108 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (72-108)
Tx Data Frames MCS 0	Total number of data frames transmitted at rate of MCS 0
Tx Data Frames MCS 1	Total number of data frames transmitted at rate of MCS 1
Tx Data Frames MCS 2	Total number of data frames transmitted at rate of MCS 2
Tx Data Frames MCS 3	Total number of data frames transmitted at rate of MCS 3
Tx Data Frames MCS 4	Total number of data frames transmitted at rate of MCS 4
Tx Data Frames MCS 5	Total number of data frames transmitted at rate of MCS 5
Tx Data Frames MCS 6	Total number of data frames transmitted at rate of MCS 6
Tx Data Frames MCS 7	Total number of data frames transmitted at rate of MCS 7
Tx Data Frames MCS 8	Total number of data frames transmitted at rate of MCS 8
Tx Data Frames MCS 9	Total number of data frames transmitted at rate of MCS 9
Tx Data Frames Legacy	Total number of data frames transmitted at legacy rate
Tx Data Frames MCS	Total number of data frames transmitted at MCS rate
Tx Data Frames NSS1	Total number of data frames transmitted 1 spacial stream
Tx Data Frames NSS2	Total number of data frames transmitted with 2 spacial stream
Tx Data Frames NSS3	Total number of data frames transmitted with 3 spacial stream
Tx Data Frames Short-GI(HALF)	Total number of data frames transmitted with short GI
Tx Data Frames Long-GI(FULL	Total number of data frames transmitted with long GI
Tx Data Frames BW20	Total number of data frames transmitted at 20 Mhz
Tx Data Frames BW40	Total number of data frames transmitted at 40 Mhz
Tx Data Frames BW80	Total number of data frames transmitted at 80 Mhz

Parameter	Description
Tx Data Frames BW160	Total number of data frames transmitted at 160 Mhz
Rx Last SNR	The last recorded signal-to-noise ratio.
Rx Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR	Signal-to-noise ratio for the last received ACK packet.
Rx Last ACK SNR CTL0	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR CTL1	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR CTL2	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Frames Received	Number of frames received.
Rx retry frames	Number of retried frames received.
Rx data frames retried	Number of retried data frames received.
Rx Data Frames	Number of data frames received.
Rx Data Bytes	Number of data bytes received.
Rx Time Data	Total time spent on frames successfully received.
Rx Duplicate Frames	Number of duplicate frames received.
Rx Broadcast Data Frames	Number of broadcast frames received.
Rx Multicast Data Frames	Number of multicast frames received.
Rx Unicast Data Frames	Number of unicast frames received.
Rx Null Data Frames	Number of null data frames received.
Rx Mgmt Frames	Number of management frames received.
Control Frames	Number of control frames received.

Parameter	Description
`Frames To Me`	Number of frames received that are addressed to the specified BSSID.
`Bytes To Me`	Number of bytes received that are addressed to the specified BSSID.
`Time To Me`	Total time spent receiving frames sent to a specified BSSID.
`Rx Probe Requests`	Number of probe requests received.
`RX PS Poll Frames`	Power-Save Poll (PS-Poll) frames received. When a client exits a power-saving mode, it transmits a PS-Poll frame to the AP to retrieve any frames buffered while it was in power-saving mode.
`RX STBC Frames`	Number of received frames with STBC enabled.
`RX LDPC Frames`	Number of received frames with LDPC enabled.
`Rx Data <value> Mbps`	Number of frames received at the specified rate, (Mbps).
`Rx Data Bytes <value> Mbps`	Number of bytes of data received at the specified rate, (Mbps).

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.3.0.0	The output of this command now includes MCS bucket mapping information channel width, number of spatial streams, and guard interval information of 802.11ac APs.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug bucketmap-state

```
show ap debug bucketmap-state {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> |
ip-addr <ip-addr> | ip6-addr <ip6-addr>} | uac {bucket <bucket> | dormant {essid <essid> |
filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} |
verbose {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> |
ip6-addr <ip6-addr>}} | uac-ip <uac-ip> | uac-ip6 <uac-ip6>}} | verbose {essid <essid> |
filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} | uac
{bucket <bucket> | dormant {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-
addr <ip-addr> | ip6-addr <ip6-addr>}}}}}
```

Description

This command shows clients in different buckets.

Syntax

Parameter	Description
`essid <essid>`	Shows clients filtered by ESSID.
`filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}`	Shows clients filtered by name of AP, BSSID, IP address or IPv6 address.
`uac {bucket <bucket> | dormant {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} | verbose {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}} | uac-ip <uac-ip> | uac-ip6 <uac-ip6>}}`	Shows clients filtered by bucket index, dormancy, IP address, or IPv6 address.
`verbose {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} | uac {bucket <bucket> | dormant {essid <essid> | filter-by {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}}}}`	Shows clients filtered by bucket index, dormancy, IP address, or IPv6 address

Usage Guidelines

This command shows clients in different buckets. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to show clients filtered by the ESSID **test**:

```
(host) [mynode] #show ap debug bucketmap-state essid test

Essid "test"
Number of updates 1; Time since last update 1h:19m:24s
```

```
Activations: New Bmap=0, Node Down=0
Bucketmap State
---------------
Index  UAC                 status
-----  ---                 ------
0      10.15.146.3 (self)  Up
1      10.15.146.4         Up
2      10.15.146.5         Up
3      10.15.146.6         Up
Stations in buckets for Essid SriniZone1TestEssid
-------------------------------------------------
BucketIndex  MAC  BSSID  AID  AP Name  UAC IP
-----------  ---  -----  ---  -------  ------
Total Stations=0 Total Active=0 Total Dormant=0
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug client-deauth-reason-counters

```
show ap debug client-deauth-reason-counters
```

Description

Shows the aggregate client deauth reason counters

Examples

The output of the command below shows client deauth reason counters.

```
(host) #show ap debug client-deauth-reason-counters
Deauth Reason Counters
----------------------
Name             Value
----             -----
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug client-mgmt-counters

```
show ap debug client-mgmt-counters
```

Description

This command shows the message counters.

Syntax

No parameters.

Usage Guidelines

This command shows the numbers of each type of message sent from a client to an AP. Use this information to troubleshoot problems on an AP.

Examples

The following example shows the client management counters.

```
(host) [mynode] #show ap debug client-mgmt-counters

Counters
--------
Name                                                                Value
----                                                                -----
41228                                                               3
Tunnel DACL                                                         7
STM Restart Notification to Auth                                    1
Associations Dropped Due to Auth Throttling                         0
PubSub Messages Rcvd                                                992
User Mon Messages                                                   0
Auth .1x Queue: High, Pending                                       450, 0
Reg timer calls                                                     141274
BSS publish Failures                                                0
Tunnel Timeouts                                                     0
Unreg/Wipeout Requests                                              0 0
Auth Resp for unknown sap                                           0
Auth enet Resp Tout                                                 0
SOS Rx Msg Count: tunop ctrl dtun_data tun_data misc                0 0 0 0 0 0 0 0 0 0 0 0
Received Client Ageout Messages from APs                            0
Received stale Entries                                              0
Received stale Entries in Deauth (Deauths from clients)             0
Processed stale Entries in Deauth                                   0
Stale entry error - BSS not found                                   0
Stale entry error - STA not found in Deauth                         0
Stale entry error - failed to clear STA in Deauth                   0
Stale entry error - Deauth bad length                               0
Stale entry error - special handling                                0
Sta down: total flag_unmatch not_assoc papi_send papi_ok papi_fail  0 0 0 0 0 0
Sta up: total flag_unmatch not_assoc papi_send papi_ok papi_fail    0 0 0 0 0 0
AMSDU Updates sent to SOS from STM                                  0
Invalid tunnel-id (0)                                               0
HBT tunnel not found on timeout                                     0
AID-MAC mismatch                                                    0
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug client-stats

```
show ap debug client-stats
   client-mac <client_mac> [advanced]
```

Description

This command shows the detailed statistics about a client from an AP.

Syntax

Parameter	Description	Range	Default
`client-mac <client_mac> [advanced]`	Shows detailed statistics about a specified client MAC.	—	—
`[advanced]`	Shows additional statistics.	—	—

Usage Guidelines

This command shows the detailed statistics about a client from an AP. For the remaining parameters, see the command syntax.

Example

The following command shows additional statistics for packets received from and transmitted to a specified client.

```
(host) [mynode] #show ap debug client-stats client-mac 00:19:7e:89:fa:e7 advanced

Station Stats
-------------
Parameter            Value
---------            -----
----------------     General Per-radio Statistics
----------------     Transmit specific Statistics
Frames Rcvd For TX   22
Tx Frames Dropped    0
Frames Transmitted   22
Success With Retry   1
Tx Mgmt Frames       2
Tx Probe Responses   0
Tx Data Frames       20
Tx CTS Frames        0
Dropped After Retry  0
Dropped No Buffer    0
Missed ACKs          1
Long Preamble        22
Short Preamble       0
Tx EAPOL Frames      13
Tx 6 Mbps            15
Tx 48 Mbps           5
Tx 54 Mbps           2
Tx WMM [VO]          15
UAPSD OverflowDrop   0
TX LDPC Frames                  0
Tx Data Priority [BE]           6283
Tx Data Frames  12 Mbps  (Mon)  0
```

```
Tx Data Frames  24 Mbps  (Mon)   0
Tx Data Frames  36 Mbps  (Mon)   0
Tx Data Frames  54 Mbps  (Mon)   0
Tx Data Frames  72 Mbps  (Mon)   0
Tx Data Frames 108 Mbps  (Mon)   0
Tx Data Frames 300 Mbps  (Mon)   6283
Tx Data Frames 450 Mbps  (Mon)   0
Tx Data Frames 1300 Mbps  (Mon)  0
Tx Data Frames 1300 Mbps+ (Mon)  0
Tx Data Bytes  12 Mbps  (Mon)    0
Tx Data Bytes  24 Mbps  (Mon)    0
Tx Data Bytes  36 Mbps  (Mon)    0
Tx Data Bytes  54 Mbps  (Mon)    0
Tx Data Bytes  72 Mbps  (Mon)    0
Tx Data Bytes  108 Mbps  (Mon)   0
Tx Data Bytes  300 Mbps  (Mon)   9510308
Tx Data Bytes  450 Mbps  (Mon)   0
Tx Data Bytes  1300 Mbps  (Mon)  0
Tx Data Bytes  1300 Mbps+ (Mon)  0
Tx 6 Mbps                        5
Tx HT 130 Mbps                   6283
Tx WMM [BE]                      6283
Tx UAPSD OverflowDrop            0
Tx AMSDU pkt count               0
Tx EAPOL Frames Rcvd             0
Tx EAPOL Frames Dropped          0
Tx Data Frames MCS 7 :           6283
Tx Data Frames MCS :             6283
Tx Data Frames NSS2 :            6283
Tx Data Frames Long-GI(FULL) :   6283
Tx Data Frames BW 20 :           6283
----------------     Receive specific Statistics
Last SNR             31
Last SNR CTL0        28
Last SNR CTL1        25
Last SNR CTL2        22
Last ACK SNR         32
Last ACK SNR CTL0    30
Last ACK SNR CTL1    28
Last ACK SNR CTL2    21
Last ACK SNR EXT0    5
Last ACK SNR EXT1    4
Frames Received      2932
Rx Data Frames       2930
Null Data Frames     2879
Rx Mgmt Frames       1
PS Poll Frames       0
Rx 6 Mbps            14
Rx 12 Mbps           6
Rx 18 Mbps           5
Rx 24 Mbps           2
Rx 36 Mbps           13
Rx 48 Mbps           1162
Rx 54 Mbps           1730
Rx WMM [BE]          39
```

The output of this command includes the following information:

Parameter	Description
Frames Rcvd For TX	Number of frames received for transmission.
Tx Frames Dropped	Number of transmission frames that were dropped.
Frames Transmitted	Number of frames successfully transmitted.
Success With Retry	Number of frames that were transmitted after being retried.
Tx Mgmt Frames	Number of management frames transmitted.
Tx Probe Responses	Number of transmitted probe responses.
Tx Data Frames	Number of transmitted data frames.
Tx CTS Frames	Number of clear-to-sent (CTS) frames transmitted.
Dropped After Retry	Number of frames dropped after an attempted retry.
Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Missed ACKs	Number of missed acknowledgements (ACKs)
Long Preamble	Number of frames sent with a long preamble.
Short Preamble	Number of frames sent with a short preamble.
Tx EAPOL Frames	Number of Extensible Authentication Protocol over LAN (EAPOL) frames transmitted.
Tx <n> Mbps	Number of frames transmitted at <n> Mbps, where <n> is a value between 6 and 300.
Tx WMM	Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. **Tx WMM [BE]:** Best Effort **Tx WMM [BK]:** Background **Tx WMM [VO]:** VoIP **Tx WMM [VI]:** Video
UAPSD OverflowDrop	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
Tx Data Frames/Bytes 24 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (12-24)
Tx Data Frames/Bytes 36 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (24-36)
Tx Data Frames/Bytes 54 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (36-54)
Tx Data Frames/Bytes 72 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (54-72)

Parameter	Description
Tx Data Frames/Bytes 108 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (72-108)
Tx Data Frames MCS 0	Total number of data frames transmitted at rate of MCS 0
Tx Data Frames MCS 1	Total number of data frames transmitted at rate of MCS 1
Tx Data Frames MCS 2	Total number of data frames transmitted at rate of MCS 2
Tx Data Frames MCS 3	Total number of data frames transmitted at rate of MCS 3
Tx Data Frames MCS 4	Total number of data frames transmitted at rate of MCS 4
Tx Data Frames MCS 5	Total number of data frames transmitted at rate of MCS 5
Tx Data Frames MCS 6	Total number of data frames transmitted at rate of MCS 6
Tx Data Frames MCS 7	Total number of data frames transmitted at rate of MCS 7
Tx Data Frames MCS 8	Total number of data frames transmitted at rate of MCS 8
Tx Data Frames MCS 9	Total number of data frames transmitted at rate of MCS 9
Tx Data Frames Legacy	Total number of data frames transmitted at legacy rate
Tx Data Frames MCS	Total number of data frames transmitted at MCS rate
Tx Data Frames NSS1	Total number of data frames transmitted 1 spacial stream
Tx Data Frames NSS2	Total number of data frames transmitted with 2 spacial stream
Tx Data Frames NSS3	Total number of data frames transmitted with 3 spacial stream
Tx Data Frames Short-GI(HALF)	Total number of data frames transmitted with short GI
Tx Data Frames Long-GI(FULL	Total number of data frames transmitted with long GI
Tx Data Frames BW20	Total number of data frames transmitted at 20 Mhz
Tx Data Frames BW40	Total number of data frames transmitted at 40 Mhz
Tx Data Frames BW80	Total number of data frames transmitted at 80 Mhz
Tx Data Frames BW160	Total number of data frames transmitted at 160 Mhz
Last SNR	The last recorded signal-to-noise ratio.
Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.

Parameter	Description
`Last SNR CTL2`	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
`Last ACK SNR`	Signal-to-noise ratio for the last received ACK packet.
`Last ACK SNR CTL0`	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
`Last ACK SNR CTL1`	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
`Last ACK SNR CTL2`	Signal-to-noise ratio for the last received ACK packet on the primary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
`Last ACK SNR EXT0`	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
`Last ACK SNR EXT1`	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
`Frames Received`	Number of frames received.
`Rx Data Frames`	Number of data frames received.
`Null Data Frames`	Number of null data frames received.
`Rx Mgmt Frames`	Number of management frames received.
`PS Poll Frames`	Number of power save poll frames received.
`Rx <n> Mbps`	Number of frames received at <n> Mbps, where <n> is a value between 6 and 300.
`Tx WMM`	Number of Wifi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. **`Tx WMM [BE]:`** Best Effort **`Tx WMM [BK]:`** Background **`Tx WMM [VO]:`** VoIP **`Tx WMM [VI]:`** Video

Command History

Command	Description
ArubaOS 8.3.0.0	The output of this command now includes MCS bucket mapping information channel width, number of spatial streams, and guard interval information of 802.11ac APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug client-table

```
show ap debug client-table [ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>]
```

Description

Show clients associated to an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Filter the client table by AP name.
`bssid <bssid>`	Filter the client table by BSSID. This will print clients on top from given BSSID.
`ip-addr <ip-addr>`	Filter the client table by AP IP address.
`ip6-addr <ip-addr>`	Filter the client table by AP IPv6 address.

Usage Guidelines

The **Tx_Rate**, **Rx_Rate**, **Last_ACK_SNR**, and **Last_Rx_SNR** columns shown in the output of this command display valuable troubleshooting information for clients trying to connect to a specific AP. Use this command to verify that the transmit (Tx_Rate) and receive (Rx_Rate) rates are not too low, and that the signal-to-noise (SNR) ratio is acceptable.

Examples

The example below the AP configuration table for a specific BSSID. In this example, the output is divided into multiple sections to better fit on the pages of this document. In the actual CLI, it appears in a single, long table.

```
(host) #show ap debug client-table ap-name apname1
Client Table
------------
MAC                ESSID            BSSID              Assoc_State  HT_State  AID
---                -----            -----              -----------  --------  ---
00:10:18:a9:7c:48  essidname1       6c:f3:7f:e7:5c:90  Associated   cAWvSseM  0x1

PS_State  UAPSD            Tx_Pkts  Rx_Pkts  PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate
--------  -----            -------  -------  -------  ----------  -------  -------
Awake     (0,0,0,0,N/A,0)  799      1377     0        48          1300     1053

Last_ACK_SNR  Last_Rx_SNR  TX_Chains Tx_Timestamp
------------  -----------  --------- ------------
32            47           3[0x7]    Sun Jul 21 11:05:50 2013

Rx_Timestamp              MFP Status (C,R)  Idle time  Client health (C/R)
------------              ----------------  ---------  -------------------
Sun Jul 21 11:05:50 2013  (0,0)             119        90/90

UAPSD:(VO,VI,BK,BE,Max SP,Q Len)
HT  Flags: A - LDPC Coding; W - 40MHz; S - Short GI 40; s - Short GI 20
D - Delayed BA; G - Greenfield; R - Dynamic SM PS
Q - Static SM PS; N - A-MPDU disabled; B - TX STBC
b - RX STBC; M - Max A-MSDU; I - HT40 Intolerant
VHT Flags: C - 160MHz; c - 80MHz;  V - Short GI 160; v - Short GI 80
```

```
E - Beamformee; e - Beamformer
HT_State shows client's original capabilities (not operational capabilities)
```

The output of this command includes the following information:

Parameter	Description
MAC	MAC address of a client.
ESSID	Extended Service Set identifier (ESSID) used by the client. An ESSID is a user-defined name for a wireless network.
BSSID	Basic Service Set identifier for the client.
Assoc_State	The associated state column shows whether or not the client is currently authorized and/or associated with the AP.
HT_State	Shows information about the client's high-throughput or very-high throughput transmission type. The description for each of the flags that can appear in this column follows the output of the command. ■ A - LDPC Coding ■ W - 40MHz ■ S - Short GI 40 ■ s - Short GI 20 ■ D - Delayed BA ■ G - Greenfield ■ R - Dynamic SM PS ■ Q - Static SM PS ■ N - A-MPDU disabled ■ B - TX STBC ■ b - RX STBC ■ M - Max A-MSDU ■ I - HT40 Intolerant ■ C - 160MHz ■ c - 80MHz ■ V - Short GI 16 ■ v - Short GI 80 ■ E - Beamformee ■ e - Beamformer
AID	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
PS_State	Powersave state, showing if the AP is in the awake or power-save state.
UAPSD	This parameter shows the Unscheduled Automatic Power Save Delivery (UAPSD) queue statuses in the following comma-separated format: (<VO>,< VI>,< BK>, <BE>,< Max SP>,<Q Len>). ■ VO: If **1**, UAPSD is enabled for the VoIP access category. If UAPSD is disabled for this access category, this value is **0**. ■ VI: If **1**, UAPSD is enabled for the Video access category. If UAPSD is disabled for this access category, this value is **0**. ■ BK: If **1**, UAPSD is enabled for the Background access category. If UAPSD is disabled for this access category, this value is **0**. ■ BE: If **1**, UAPSD is enabled for the Best Effort access category. If UAPSD is disabled for this access category, this value is **0**. ■ Max SP: The maximum service period is the number of frame sent per trigger packet. This value is value can be 0, 2, 4 or 8. ■ Q Len: The number of frames currently queued for the client, from 0 to 16 frames.

Parameter	Description
Tx_Pkts	Number of packets transmitted from the AP to the client.
Rx_Pkts	Number of packets the AP received from the client.
PS_Qlen	Number of packets in the power save queue length.
Tx_Retries	Number of packets that the AP had to resend to the client due to an initial transmission failure.
Tx_rate	Rate at which last packet was sent to client (in Mbps)
Rx_rate	Rate at which last packet was received from client (in Mbps)
Last_ACK_SNR	Signal-to-Noise ratio of the last acknowledge packet sent by client.
Last_Rx_SNR	Signal-to-Noise ratio of the last data packet received from the client.
TX_Chains	The first digit in this value indicates the number of transmission chains on the radio currently in use, and the number in brackets shows which of the chains are active. The current status of each chain is indicated by a single-digit binary number; **1** if the chain is active, and **0** if it is inactive. In the example output above (**2 [0x5]**), two chain are active; chain one and chain three. ■ chain one: **1** (active) ■ chain two: **0** (inactive) ■ chain three: **1** (active In the example above, the chain would generate the value **101**, which translates to the hexadecimal number **5**. If all three chain were active, it would generate the value **111**, (the hexadecimal number **7**), and would appear in the CLI output as **3 [0x7]**.
Tx_timestamp	Date and time the last packet was sent to the client.
Rx_timestamp	Date and time the last packet was received from the client.
MFP status	Client is 802.11W capable/802.11W is enabled on Radio
Idle Time	Number of seconds elapsed since a packet was received from the client.
Client Health	This column shows the client health of the client and the AP radio, in the format <client_ health>/<AP-health>. These values report the quality of link between the client and radio, An AP's client health is the efficiency at which that AP transmits downstream traffic to a particular client. This value is determined by comparing the amount of time the AP spends transmitting data to a client to the amount of time that would be required under ideal conditions, that is, at the maximum Rx rate supported by client, with no data retries. A client health metric of 100% means the actual airtime the AP spends transmitting data is equal to the ideal amount of time required to send data to the client. A client health metric of 50% means the AP is taking twice as long as is ideal, or is sending one extra transmission to that client for every packet. A metric of 25% means the AP is taking four times longer than the ideal transmission time, or sending 3 extra transmissions to that client for every packet.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug client-trace

```
show ap client-trace
   {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>} mac <client-mac>
```

Description

Use this command to show counts of different types of management data frames traced from a client MAC address.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IPv4 address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.
mac <client-mac>	MAC address of the client.

Usage Guidelines

This command should only be used under the guidance of Aruba technical support.

Related Commands

Command	Description
ap debug client-trace start	Use this command to trace management packets from a client MAC address.
ap debug client-trace stop	Use this command to stop tracing management packets from a client MAC address.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug client-trace clients

```
show ap debug client-trace clients {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows debug client trace for all registered clients in an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows debug client trace for all registered clients in an AP for specified AP name.
`ip-addr <ip-addr>`	Shows debug client trace for all registered clients in an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows debug client trace for all registered clients in an AP for specified IPv6 address.

Usage Guidelines

This command shows debug client trace for all registered clients in an AP. For the remaining parameters, see the command syntax.

Example

The following example shows an AP named ap-205 does not support the show ap debug client-trace clients command:

```
(host) [mynode] #show ap debug client-trace clients ap-name ap-205

The AP platform do not support the command
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug cluster-counters

```
show ap debug cluster-counters
```

Description

Displays the controller cluster statistics.

Examples

The output of the command below shows cluster statistics.

```
(host) (config) #show ap debug cluster-counters

STM Cluster Debug Counters
--------------------------
Name                                                          Value
----                                                          -----
UAC BSS Adds, Add Failures                                    0 0
UAC BSS: Role Cleared, Deletes, Delete Failures               0 0 0
Standby UAC BSS Adds, Add Failures                            0 0
Dormant STA: Success, No Bmap on add, Fails, Defer Add        6, 0, 0 0
STAs emptied : UAC, Standby UAC, STA_negve SBY_negve          0, 6, 0 0
Down Node: not found, update bmap, not in bmap, self not in bmap  6, 2, 0 0
Standby Activations, Activation Errors, Not dormant           0 0 0
Active De-activations: No STA, No SAP, No SAP_STA             0 0 0 0 0
SOS punted frames ignored at UAC                              0
Cluster Disable Events                                        2
Bucketmap Events when Cluster Disabled                        0
Bucketmap Create Events, SAPM bmap errors                     12 3
AAC SAP Stby to Active: Requests, moves, empty                5 1 4
AAC Enet Stby to Active: Requests, moves, empty               5 0 5
Dormant STA: Skip Clear, Ageout                               0 6
AUTH restart Clear AP events                                  0
CBSS DEL Ignored: AAC, SBY-AAC                                5 38
CBSS Not found count                                          0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices

show ap cluster-node-state

```
show ap cluster-node-state
```

Description

Displays the nodes state of a cluster.

Syntax

No syntax.

Example

The output of this command shows the state of the nodes in a cluster:

```
(host) (config) #show ap debug cluster-node-state

Cluster Name "multiZone1"; Redundancy=Yes; Cluster AP Limit=0
Cluster Nodes
-------------
Index  Node IP             Status  Duration since Last Update
-----  -------             ------  --------------------------
0      10.15.146.3 (self)  Up      3d:18h:44m:26s
1      10.15.146.4         Up      3d:18h:40m:2s
2      10.15.146.6         Up      3d:18h:40m:2s
3      10.15.146.5         Up      3d:18h:40m:2s
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices.

show ap debug config-msg-history

```
show ap debug config-msg-history {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows recent configuration messages sent and received by an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows recent configuration messages sent and received by an AP for specified AP name.
`ip-addr <ip-addr>`	Shows recent configuration messages sent and received by an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows recent configuration messages sent and received by an AP for specified IPv6 address.

Examples

The following example shows the configuration message history for the AP named ap-205:

```
(host) [mynode] #show ap debug config-msg-history ap-name ap-205

Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=LOG_CONFIG len=151
peer=192.192.189.1 seq_num=3 resps_sent=1
040000009204000000001405C0C0BD0104575BE5D4040000000307020107020104000000060400000208040000000404
000000000400000188040000000404040000
Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=MONITORING_MSG_CONFIG len=59
peer=192.192.189.1 seq_num=4 resps_sent=1
040000003604000000001D05C0C0BD0104575BE5D4040000000404020102C7027F025502FC02FF02E4023F020002F9021F
020002000200020002000200
Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=ESSID_LIST len=94 peer=192.192.189.1
seq_num=5 resps_sent=1
040000005904000000002705C0C0BD0104575BE5D4040000000504000000050000086172756261 2D617000000A617275
62612D6D657368000008656D706C6F7965
Sat Jun 11 02:20:13 2016(1779212 secs ago): RCVD REQ type=MCELL len=28 peer=192.192.189.1 seq_
num=6 resps_sent=1 040000001704000000 3905C0C0BD0104575BE5D40400000006070201
Wed Dec 31 16:00:00 1969(1467419625 secs ago): RCVD RESP type=HELLO len=0 peer=0.0.0.0 seq_
num=0
Wed Dec 31 16:00:00 1969(1467419625 secs ago): RCVD RESP type=HELLO len=0 peer=0.0.0.0 seq_
num=0
Wed Dec 31 16:00:00 1969(1467419625 secs ago): RCVD RESP type=HELLO len=0 peer=0.0.0.0 seq_
num=0
Sat Jun 11 02:20:05 2016(1779220 secs ago): RCVD REQ type=REG_DOM_INFO len=1787
peer=192.192.189.1 seq_num=0 resps_sent=1
04000006F6040000003505C0C0BD0104575BE5D4040000000007020102160224022802 2C023002340238023C024002
640268026C027002740284028802 8C0290
Sat Jun 11 02:20:05 2016(1779220 secs ago): RCVD REQ type=CONFIG len=3508 peer=192.192.189.1
seq_num=1 resps_sent=1
0400000DAF040000000F05C0C0BD0104575BE5D4040000000104000000000400000005070201020004000000050400
0001A804000000000400000001040000003
Sat Jun 11 02:20:12 2016(1779213 secs ago): RCVD REQ type=CONFIG len=2291 peer=192.192.189.1
seq_num=2 resps_sent=1
04000008EE040000000F05C0C0BD0104575BE5D4040000000204000000030400000034040000000040000000004000
000000040000000107020104575BE5D400
Fri Jul  1 15:00:18 2016(5607 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2958 num_attempts=1 rtt=0 secs
040000002804000000020 5BFBFBFFC040000000004000 00B8E045776F60205FFFFFF0005BFBFBFFE0000000000
```

```
Fri Jul  1 15:10:18 2016(5007 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2959 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B8F045776F85A05FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 15:20:18 2016(4407 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2960 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B90045776FAB205FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 15:30:18 2016(3807 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2961 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B91045776FD0A05FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 15:40:18 2016(3207 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2962 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B92045776FF6205FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 15:50:18 2016(2607 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2963 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B9304577701BA05FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 16:00:18 2016(2007 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2964 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B94045777041205FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 16:10:18 2016(1407 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1
seq_num=2965 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B95045777066A05FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 16:20:18 2016(807 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1 seq_
num=2966 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B9604577708C205FFFFFF0005BFBFBFFE0000000000
Fri Jul  1 16:30:18 2016(207 secs ago): SENT REQ type=KEEPALIVE len=45 peer=192.192.189.1 seq_
num=2967 num_attempts=1 rtt=0 secs
040000002804000000205BFBFBFFC04000000000400000B970457770B1A05FFFFFF0005BFBFBFFE0000000000
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug counters

```
show ap debug counters {ap-name <ap-name>|bssid <bssid>|group <group>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show AP reboot/bootstrap counters, and crash information for an individual AP or AP group, or all APs referenced on the controller.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show debug counters for an AP with a specified name.
`bssid <bssid>`	Show debug counters for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`group <group>`	Show debug counters for an AP group.
`ip-addr <ip-addr>`	Show debug counters for an AP with a specified IP address by entering an IP address in dotted-decimal format.
ip6-addr <ip6-addr>	Show debug counters for an AP with a specified IPv6 address by entering an IP address in dotted-decimal format.

Example

The output of this command shows how many times each AP has rebooted (a hard boot) or bootstrapped (a soft boot), the number of configuration changes sent and acknowledged by that AP, and whether or not the AP rebooted due to a kernel crash.

In this example, the output has been divided into multiple sections to better fit on the pages of this document. In the actual CLI, it will appear in a single, long table.

```
(host) #show ap debug counters group corp1
AP Counters
-----------
Name  Group  IP Address  Configs Sent  Configs Acked  AP Boots Sent
----  -----  ----------  ------------  -------------  -------------
AL1   corp1  10.6.1.209  1597             1597           0
AL10  corp1  10.6.1.198  165              165            0
AL12  corp1  10.6.1.200  195              195            0
AL15  corp1  10.6.1.197  1580             1580           0
AL16  corp1  10.6.1.199  73               73             0
AL19  corp1  10.6.1.212  8                8              0

AP Boots Acked  Bootstraps (Total)  Reboots  Crash
--------------  ------------------  -------  -----
0               1           (1)       0       N
0               2           (2)       1       Y
0               1           (1)       0       N
0               1           (1)       0       N
0               1           (1)       0       N
0               1           (1)       0       N
Total APs :6
```

The output of this command includes the following information:

Column	Description
Name	Name of the AP.
Group	Name of the AP's group.
IP Address	IP address of the AP.
Configs sent	Number of times configuration changes have been sent to the AP.
Configs Acked	Number of times that the AP has acknowledged receiving a configuration change.
AP Boots Sent	Number of times reboot requests have been sent to the AP.
AP Boots Acked	Number of times that the AP has acknowledged receiving a reboot request.
Bootstraps	Number of times the AP bootstrapped since AP reboot. Bootstraps are also known as "soft" restarts.
Total Bootstraps	Total number of times the AP bootstrapped since AP image upgrade.
Reboots	Number of times power to the AP cycled off and then on again since image upgrade. Reboots also known as "hard" restarts.
Crash	Indicates whether or not the AP was rebooted due to a kernel crash. Use show ap debug crash-info to view the crash signature.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug crash-info

```
show ap debug crash-info {ap-name <ap-name>|ip-addr <ip-addr>

ip6-addr <ip6-addr>}
```

Description

Show crash log information (if it exists) for an individual AP. The stored information is cleared from the flash after the AP reboots.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show crash information for an AP with a specified name.
`ip-addr <ip-addr>`	Show crash information for an AP with a specified IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show crash information for an AP with a specified IPv6 address by entering an IP address in dotted-decimal format.

Example

The output of this command shows a partial sample crash log information for an AP named **MyAP**

```
(host) #show ap debug crash-info ap-name MyAP

<4>ArubaOS Version x.x.x.x (build xxxx / label #xxxx)
<4>Built by p4build@cartman on 2012-07-29 at 14:44:06 PST (gcc version x.x.x
Cavium Networks Version: 1.4.0, build 58)
<4>CVMSEG size: 2 cache lines (256 bytes)
<4>Setting flash physical map for 16MB flash at 0x1ec00000
<4>Determined physical RAM map:
<7>On node 0 totalpages: 16384
<7>  DMA zone: 16384 pages, LIFO batch:3
<7>  DMA32 zone: 0 pages, LIFO batch:0
<7>  Normal zone: 0 pages, LIFO batch:0
<7>  HighMem zone: 0 pages, LIFO batch:0
<4>Primary instruction cache 32kB, virtually tagged, 4 way, 64 sets, linesize 128 bytes.
<4>Primary data cache 16kB, 64-way, 2 sets, linesize 128 bytes.
<4>Using 500.000 MHz high precision timer. cycles_per_jiffy=1000000
<6>Memory: 56636k/65536k available (1925k kernel code, 8840k reserved, 575k data, 2716k init,
0k highmem)
<4>Calibrating delay using timer specific routine.. 1000.32 BogoMIPS (lpj=1000322)
<4> available.
<4>Checking for the multiply/shift bug... no.
<4>Checking for the daddi bug... no.
<4>Checking for the daddiu bug... no.
<5>detected lzma initramfs
<5>initramfs: LZMA lc=3,lp=0,pb=2,dictSize=8388608,origSize=15217664
<5>LZMA initramfs
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show ap debug crypto

```
show ap debug crypto
   ap-name <ap-name>
   detail {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
   history {[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]}
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
```

Description

This command shows the debug crypto logs for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows debug crypto logs for the specified AP name.
`detail`	Shows detailed debug crypto logs for: ■ ap-name ■ ip-addr ■ ip6-addr
`history`	Shows historical debug crypto logs for: ■ ap-name ■ ip-addr ■ ip6-addr
`ip-addr <ip-addr>`	Shows debug crypto logs for specified IP address of an AP.
`ip6-addr <ip6-addr>`	Shows debug crypto logs for specified IPv6 address of an AP.

Usage Guidelines

The **show ap debug crypto** command shows the debug crypto logs for an AP.

Example

The example shows the AP debug crypto logs of an AP named **MyAP**

```
(host) [mynode] #show ap debug crypto ap-name MyAP

2014-01-07 14:48:43 ESP: spi[93477900] 10:15:64:104 << 10:15:66:151
2014-01-07 14:48:43 ESP: spi[ca0db300] 10:15:66:151 << 10:15:64:104
2014-01-07 15:19:34 SEND: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG: CREATE_CHILD_SA
2014-01-07 15:19:34 RECV: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG: CREATE_CHILD_SA
2014-01-07 15:19:39 SEND: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG: INFORMATIONAL
2014-01-07 15:19:39 RECV: a793342e9b6f8bec : 25baf55ae40e91c3 , np=46, EXHG: INFORMATIONAL
2014-01-07 18:00:49 RECV: 090cbf2a1ff1c433 : a496e13623118522 , np=46, EXHG: CREATE_CHILD_SA
2014-01-07 21:33:02 RECV: 090cbf2a1ff1c433 : a496e13623118522 , np=46, EXHG: INFORMATIONAL
2014-01-07 22:49:00 SEND: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG: CREATE_CHILD_SA
2014-01-07 22:49:00 RECV: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG: CREATE_CHILD_SA
2014-01-07 22:49:00 ESP: spi[d774af00] 10:15:64:104 << 10:15:66:151
2014-01-07 22:49:00 ESP: spi[49799700] 10:15:66:151 << 10:15:64:104
2014-01-08 00:25:05 SEND: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG: CREATE_CHILD_SA
2014-01-08 00:25:05 RECV: d6e361df5a012297 : f5ffdd8f2be2f073 , np=46, EXHG: CREATE_CHILD_SA
2014-01-08 00:25:05 ESP: spi[83c32c00] 10:15:64:104 << 10:15:66:151
2014-01-08 00:25:05 ESP: spi[072a9200] 10:15:66:151 << 10:15:64:104
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug datapath

```
show ap debug datapath {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show datapath tunnel parameters of an AP or AP group.

Syntax

Parameter	Description
`ap-group <ap-group>`	Show data path information for a specific AP group.
`ap-name <ap-name>`	Show data path information for an AP with a specific name.
`bssid <bssid>`	Show data path information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data path information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show data path information for an AP with a specific IPv6 address by entering an IP address in dotted-decimal format.

Example

The output of the following command shows datapath tunnel parameters for an AP with the IP address 192.0.2.32.

```
(host) #show ap debug datapath ip-addr 192.0.2.32

Datapath Parameters Table
-------------------------
essid   encr-alg        client-vlan-id  tunnel-id  gre-type  deny-bcast  num-clients
-----   --------        --------------  ---------  --------  ----------  -----------
guest   Open            63              0x10f6     0x8300    disable     0
voip    WPA2 8021X AES  66              0x1103     0x8310    disable     7
corp    WPA2 PSK AES    66              0x10f1     0x8320    disable     0
guest   Open            63              0x10f7     0x8200    disable     1
wpa2    WPA2 8021X AES  65              0x10be     0x8210    enable      15
```

The output of this command includes the following information:

Column	Description
`ESSID`	The Extended Service Set Identifier is a unique name that identifies a wireless network
`encr-alg`	Encryption algorithm used by the network
`client-vlan-id`	ID of the network VLAN
`tunnel-id`	Identification number of the AP's tunnel.

Column	Description
gre-type	GRE tunnel type.
deny-bcast	If **enabled**, the AP will respond to broadcast probe requests. If **disabled**, the AP will not respond to these requests.
num-clients	Number of clients currently using the network.

The output of the following command shows datapath tunnel parameters for an AP with the IPv6 address 11:12:11:11::2.

```
(host) #show ap debug datapath ip6-addr 11:12:11:11::2
Datapath Parameters Table
-------------------------
essid                    encr-alg      client-vlan-id  tunnel-id  gre-type  deny-bcast  num-
clients
-----                    --------      --------------  ---------  --------  ----------  ------
-----
i-platform-mobility  WPA2 PSK AES  10              0x1000b    0x8300    disable     0
i-platform-mobility  WPA2 PSK AES  10              0x1000a    0x8200    disable     1
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug dot11r

```
show ap  debug dot11r
   efficiency <client-mac>
   state [ap-name <ap-name> | ip-addr <ip-addr>] ip6-addr <ip6-addr>
```

Description

This command displays all the r1 keys that are stored in an AP and the hit/miss rate of r1 keys cached on an AP before a Fast BSS Transition roaming.

Syntax

Parameter	Description
`efficiency <client-mac>`	Show the hit/miss rate of r1 keys cached on an AP before a Fast BSS Transition roaming for the specified client MAC address.
`state`	Show all the r1 keys that are stored in an AP based on the filter specified.
`ap-name <ap-name>`	Show debugging information for a specific AP.
`ip-addr <ip-addr>`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Examples

Use this command to view all the r1 keys that are stored in an AP. You can filter the output based on the AP name or IP address.

```
(host) #show ap  debug dot11r state ap-name MAcage-105-GL

Stored R1 Keys
--------------
Station MAC        Mobility Domain ID  Validity Duration  R1 Key
-----------        ------------------  -----------------  ------
00:50:43:21:01:b8  1                   3568               (32): 94 ff 18 0a 5f 47 8b 3e 95 2b
93 31 bd 44 58 fe fe 6a ad aa 1d d7 29 94 fb 5b 7c 15 76 66 d2 1f
```

Use this command to view the hit/miss rate of r1 keys cached on an AP before a Fast BSS Transition roaming. This counter helps to verify if enough r1 keys are pushed to the neighboring APs.

```
(host) #show ap  debug dot11r efficiency
Fast Roaming R1 Key Efficiency
------------------------------
Client MAC         Hit (%)  Miss (%)
----------         -------  --------
00:50:43:21:01:b8  0 (0%)   0 (0%)
```

Command History

Command	Description
ArubaOS 8.2.0.0	The **ip6-addr** parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug dot11r state

```
show ap debug dot11r state [ap-name <ap-name> | ip-addr <ip-addr>]
```

Description

This command displays all the r1 keys that are stored in an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show debugging information for a specific AP.
`ip-addr <ip-addr>`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Examples

Use this command to view all the r1 keys that are stored in an AP. You can filter the output based on the AP name or IP address.

```
(host) #show ap  debug dot11r state ap-name MAcage-105-GL

Stored R1 Keys
--------------
Station MAC        Mobility Domain ID  Validity Duration  R1 Key
-----------        ------------------  -----------------  ------
00:50:43:21:01:b8  1                   3568               (32): 94 ff 18 0a 5f 47 8b 3e 95 2b
93 31 bd 44 58 fe fe 6a ad aa 1d d7 29 94 fb 5b 7c 15 76 66 d2 1f
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on managed devices

show ap debug driver-log

```
show ap debug driver-log {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip-addr>}
```

Description

Show an AP's driver logs.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip-addr>`	Show log information for an AP with a specific IPv6 address.

Usage Guidelines

Use this command to review configuration changes made since the AP was last reset.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug gre-tun-stats

```
show ap debug gre-tun-stats {ap-name <ap-name>| bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Shows GRE tunnel packet statistics of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows GRE tunnel packets information for an AP.
`bssid <bssid>`	Shows GRE tunnel packets information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Shows GRE tunnel packets information for an AP with a specified IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip-addr>`	Shows GRE tunnel packets information for an AP with a specific IPv6 address.

Example

The output of this command shows GRE tunnel packets information for an AP named AP325.

```
(host) #show ap debug gre-tun-stats ap-name AP325
GRE HBT Tunnel Stats
--------------------
AP IP     Controller IP  Sent Count  HBT Tx Seqnum  Idle (secs)  Rcvd Count  HBT Rx Seqnum
-----     -------------  ----------  -------------  -----------  ----------  -------------
1.1.1.11  10.15.91.8     864681      12697          0            864636      12697

Idle (secs)
-----------
0

GRE Tunnel Packet Stats
-----------------------
MAC                BSSID     Tun Input  In IP Frags  To WLAN  Idle (secs)  Rate pps  From WLAN

---                -----     ---------  -----------  -------  -----------  --------  ---------
C4:85:08:A2:15:2F  4F:4E:B0  54048      0            54048    60           5/        143339
00:26:C6:52:6B:7C  4F:4E:B0  31712      0            31712    120          2/        69115
00:21:6A:B9:5F:34  4F:4E:B0  29628      3            29628    60           0/        64985
FF:FF:FF:FF:FF:FF  4F:4E:B0  259841     0            259841   60           2/        0
01:00:5E:00:01:74  4F:4E:B0  221714     6            221714   0            1/        0
01:00:0C:CC:CC:CD  4F:4E:B0  443906     0            443906   0            0/        0
01:00:5E:00:00:FC  4F:4E:B0  191310     0            191310   60           1/        0

Tun Output  Out IP Frags  Idle (secs)  Rate pps
----------  ------------  -----------  --------
 143339      143339        0            0/
 69115       69115         60           1/
 64985       64985         60           1/
 0           0             0            0/
 0           0             0            0/
```

```
 0           0             0            0/
 0           0             0            0/


NSS state
---------
*** GRE offload feature is disabled (RAP) ***
NSS GRE Tunnel Stats
--------------------
NSS IPv4 Node stats
-------------------
ipv4 stats start:
common node stats:
rx_packets = 7119875
rx_bytes = 1547705849
rx_dropped = 0
tx_packets = 0
tx_bytes = 0
ipv4 node stats:
rx_pkts = 0
rx_bytes = 0
tx_pkts = 0
tx_bytes = 0
create_requests = 0
create_collisions = 0
create_invalid_interface = 0
destroy_requests = 0
destroy_misses = 0
hash_hits = 0
hash_reorders = 0
flushes = 0
evictions = 0
fragmentations = 0
mc_create_requests = 0
mc_update_requests = 0
mc_create_invalid_interface = 0
mc_destroy_requests = 0
mc_destroy_misses = 0
mc_flushes = 0
ipv4 exception stats:
IPV4_ICMP_HEADER_INCOMPLETE = 0
IPV4_ICMP_UNHANDLED_TYPE = 1743
.
.
.
```

The command output shows only information applicable for the specified AP. The output of the previous command is only a representative information of the likely output.

The output parameters in the command output (NSS State) are explained in the following table:

Column	Description
NSS LAG	Corresponds to the AP lag. This means that link aggregation is enabled on the Ethernet ports in NSS. This is only for the IP acceleration rule, so that NSS can expect packets coming in on both ports to match an acceleration rule. It is not necessarily for LACP. It is applicable for active-standby as well.

Column	Description
`NSS Jumbo`	Meant for the AP ports. This corresponds to the NSS phy layer setting to receive jumbo (9 KB) frames.
`LMS GRE redi`	Indicates GRE tunnel in NSS. In the output, the if_num value (for example, if_ num 24) is the NSS interface number for a specific GRE tunnel.
`LMS GRE rule`	Refers to the IP-GRE acceleration rule for client traffic from and to the controller.
`Standby GRE redir`	Same as the LMS GRE redir, but corresponds to that of the standby controller.
`Standby GRE rule`	Same as the LMS GRE rule, but corresponds to that for the standby controller.
NOTE: NSS refers to the network subsystem. It is a flow acceleration chipset from Qualcomm used in AP-315, and AP-325 access points. The hardware has Ethernet, IP, and GRE flow acceleration modules, IP fragmentation/reassembly, IPsec encap/decap. NSS also has the corresponding driver software. Most of these functions were performed by the software in previous AP models.	

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap debug gsm-counters

```
show ap debug gsm-counters
  verbose
```

Description

Displays the GSM counters of an AP or AP group.

Syntax

Parameter	Description
`verbose`	Displays the event statistics in a tabular format.

Example

The output of the following command shows gsm counters of an AP:

```
(host) (config) #show ap debug gsm-counters verbose
STM GSM Counters
----------------
Name                                                    Value
----                                                    -----
AP Publish Events                                       15
AP Delete Events                                        3
Radio Publish Events                                    9548
Radio Delete Events                                     0
BSS Publish Events                                      6
Responses to BSS Rcvd                                   6
BSS Delete Events                                       0
STA Publish Events                                      0
STA Delete Events                                       0
WIRED_AP Publish Events                                 0
Responses to WIRED_AP Rcvd                              0
WIRED_AP Delete Events                                  0
MAC-User Publish Notifications                          0
MAC-User Notify Events                                  0
MAC-User Responses Sent                                 0
BSS Response time histogram [1...128] seconds in powers of 2  4 2 0 0 0 0 0 0
STA Response time histogram [1...128] seconds in powers of 2  0 0 0 0 0 0 0 0
STA Delete Reason                                       Count
-----------------                                       -----
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug hotspot statistics

```
show ap debug hotspot statistics bssid <bssid_string>
```

Description

This command shows the statistics of ANQP/H2QP information.

Syntax

Parameter	Description	Range	Default
`bssid <bssid_string>`	Shows statistics of ANQP/H2QP information for the specified BSSID.	–	–

Usage Guidelines

This command shows the statistics of ANQP/H2QP information. For the remaining parameters, see the command syntax.

Example

The following example shows the statistics of ANQP/H2QP information for the BSSID 00:1a:1e:aa:bb:cc:

```
(host) [mynode] #show ap debug hotspot statistics bssid 00:1a:1e:aa:bb:cc
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap debug ipc forwarding-statistics

```
show ap debug ipc forwarding-statistics {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip-addr>}
```

Description

Show an AP's ipc forwarding statistics.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip-addr>`	Show log information for an AP with a specific IPv6 address.

Usage Guidelines

Use this command to review configuration changes made since the AP was last reset.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug lacp

```
show ap debug lacp {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addre<ipv6-addr>}
```

Description

Displays the number of GRE packets sent and received on the two Ethernet ports.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show LACP information for an AP with a specific name.
`bssid <bssid>`	Show LACP information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show LACP information for an AP with a specific IPv4 address.
`ip6-addr <ipv6-addr>`	Show LACP information for an AP with a specific IPv6 address.

Usage Guidelines

Use this command to know if LACP is active on an AP from the number of GRE packets sent and received on the two Ethernet ports. If a GRE striping IP address is configured in the **ap-lacp-striping-ap** profile, the output of this command displays the GRE striping IP address.

Example 1

The following example displays that the wireless GRE packets are being sent and received on different wired ports of the AP for the 5GHz and 2.4GHz bands, and is only applicable to 220 Series and 270 Series. It also shows that the interfaces eth0 and eth1 are part of the link aggregation group (LAG):

```
AP LACP GRE Striping IP: 10.65.30.50
AP LACP Status
--------------
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC
-----------  ---------  ---------  ---------  -----------  -----------
Up           slow       2          17         2            00:0b:86:61:7a:58
Slave Interface Status
----------------------
Slave I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link Fail Count
--------------  -----------------  -----------  -------------  ---------------
eth0            6c:f3:7f:c6:72:82   Up           Yes            0
eth1            6c:f3:7f:c6:72:83   Up           Yes            1
GRE Radio Traffic Received on Enet Ports
----------------------------------------
Radio Num  Enet 0 Rx Count  Enet 1 Rx Count
---------  ---------------  ---------------
0          5048             0
1          0                23
Traffic Sent on Enet Ports
--------------------------
Radio Num  Enet 0 Tx Count  Enet 1 Tx Count
---------  ---------------  ---------------
0          65               3466
1          64               0
non-wifi   2                50
```

The following example is only applicable to 320 Series:

```
#show ap debug lacp ap-name ap325 verbose
AP LACP GRE Striping IP: 10.3.44.34
AP LACP Status
--------------
Link Status  LACP Rate  Num Ports  Actor Key  Partner Key  Partner MAC
-----------  ---------  ---------  ---------  -----------  -----------
Up           slow       2          17         4            00:1a:1e:0f:b4:80
Slave Interface Status
----------------------
Slave I/f Name  Permanent MAC Addr  Link Status  Member of LAG  Link Fail Count
--------------  ------------------  -----------  -------------  ---------------
eth0            ac:a3:1e:cd:35:ce   Up           Yes            1
eth1            ac:a3:1e:cd:35:cf   Up           Yes            1
GRE Traffic Received on Enet Ports
----------------------------------
Radio Num  Enet 0 Rx Count  Enet 1 Rx Count
---------  ---------------  ---------------
0          23785            22083
1          0                0
non-wifi   15684            3
Traffic Sent on Enet Ports
--------------------------
Radio Num  Enet 0 Tx Count  Enet 1 Tx Count
---------  ---------------  ---------------
0          8166             307
1          0                0
non-wifi   32326            7
Link Aggregation destination list
---------------------------------
[ 0] 00:1A:1E:01:4F:28  Tx: 6008
[ 1] 24:77:03:F4:82:B4  Tx: 28
[ 2] 78:31:C1:BC:D6:12  Tx: 26
[ 3] F0:1F:AF:69:51:9E  Tx: 229
Total: 4
Odd numbered entries use striping GRE tunnel.
Total tunnel mode AMSDU Tx: 99
Link Aggregation station packet re-ordering statistics
------------------------------------------------------
3C:A9:F4:24:B2:54: exp-seq 21; eap 0 zero 0; rx 20 tx 20 drop 0 max_hold 0 skip 0 old-seq 0
(last-seq# 0); window: resets 0 pkts 0; Timer: start 0 stop 0 run 0 more 0
78:31:C1:BC:D6:12: exp-seq 223; eap 0 zero 0; rx 222 tx 222 drop 0 max_hold 0 skip 0 old-seq 0
(last-seq# 0); window: resets 0 pkts 0; Timer: start 0 stop 0 run 0 more 0
```

Command HistoryCommand History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug lldp

```
show ap debug lldp
```

Description

Show an AP's debug log.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.

Usage Guidelines

An AP's log files show configuration changes since the AP was last reset.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug lldp counters

```
show ap debug lldp counters {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
[interface <port-string>]
```

Description

This command shows LLDP statistics of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows LLDP statistics of an AP for specified AP name.
`ip-addr <ip-addr>`	Shows LLDP statistics of an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows LLDP statistics of an AP for specified IPv6 address.
`interface <port-string>`	Shows LLDP statistics for specified interface of an AP.

Usage Guidelines

This command shows LLDP statistics of an AP. For the remaining parameters, see the command syntax.

Example

The following example shows radio scanning of an AP named ap-205:

```
(host) [mynode] #show ap debug lldp counters ap-name ap-205

LLDP Counters
-------------
Interface  Received  Unknown TLVs  Malformed  Overflow  Transmitted
---------  --------  ------------  ---------  --------  -----------
bond0      49937     0             0          0         49914
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug lldp neighbors

```
show ap debug lldp neighbors {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
[interface <port-string> [detail]]}
```

Description

This command shows LLDP peer information of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows LLDP peer information of an AP for specified AP name.
`ip-addr <ip-addr>`	Shows LLDP peer information of an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows LLDP peer information of an AP for specified IPv6 address.
`interface <port-string> [detail]`	Shows LLDP peer information for specified interface of an AP. Detail parameter shows additional LLDP peer information.

Usage Guidelines

This command shows LLDP peer information of an AP. For the remaining parameters, see the command syntax.

Example

The following example shows LLDP peer information of an AP named ap-205:

```
(host) [mynode] #show ap debug lldp neighbors ap-name ap-205

Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
LLDP Neighbor Information
-------------------------
Interface  Neighbor ID        Capabilities  Remote Interface  Expiry-Time (Secs)
---------  -----------        ------------  ----------------  ------------------
bond0      00:0b:86:96:fe:f7  B:R           GE0/0/2           91

Number of neighbors: 1
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug lldp state

```
show ap debug lldp state {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
[interface <port-string>]
```

Description

This command shows LLDP state of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows LLDP state of an AP for specified AP name.
`ip-addr <ip-addr>`	Shows LLDP state of an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows LLDP state of an AP for specified IPv6 address.
`interface <port-string>`	Shows LLDP state for specified interface of an AP.

Usage Guidelines

This command shows LLDP state of an AP. For the remaining parameters, see the command syntax.

Example

The following example shows LLDP state of an AP named ap-205:

```
(host) [mynode] #show ap debug lldp state ap-name ap-205

LLDP Interface Information
--------------------------
Interface  LLDP TX  LLDP RX  LLDP-MED  TX interval  Hold Timer
---------  -------  -------  --------  -----------  ----------
bond0      Enabled  Enabled  Disabled  30           120
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug log

```
show ap debug log {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show an AP's debug log.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show log information for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Usage Guidelines

An AP's log files show configuration changes since the AP was last reset.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug log-config

```
show ap debug log-config {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows AP log configuration.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AP log configuration for specified AP name.
`ip-addr <ip-addr>`	Shows AP log configuration for specified IP address.
`ip6-addr <ip6-addr>`	Shows AP log configuration for specified IPv6 address.

Usage Guidelines

This command shows AP log configuration. For the remaining parameters, see the command syntax.

Example

The following example shows an AP named ap-205 is not registered with managed device:

```
(host) [mynode] #show ap debug log-config ap-name ap-205
AP is not registered with this switch
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug dot11r state

```
show ap debug dot11r state [ap-name <ap-name> | ip-addr <ip-addr>]
```

Description

This command displays all the r1 keys that are stored in an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show debugging information for a specific AP.
`ip-addr <ip-addr>`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Examples

Use this command to view all the r1 keys that are stored in an AP. You can filter the output based on the AP name or IP address.

```
(host) #show ap  debug dot11r state ap-name MAcage-105-GL

Stored R1 Keys
--------------
Station MAC        Mobility Domain ID  Validity Duration  R1 Key
-----------        ------------------  -----------------  ------
00:50:43:21:01:b8  1                   3568               (32): 94 ff 18 0a 5f 47 8b 3e 95 2b
93 31 bd 44 58 fe fe 6a ad aa 1d d7 29 94 fb 5b 7c 15 76 66 d2 1f
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on managed devices

show ap debug multizone

```
show ap debug multizone
   ap-name                  Name of AP
   ip-addr                  IP Address of AP
   ip6-addr                 IPv6 address of AP
```

Description

Displays the multizone configured for an AP.

Syntax

Parameter	Description
ap-name	Name of AP
ip-addr	IP Address of AP
ip6-addr	IPv6 address of AP

Example

The following example shows the multizone configured for a particular AP:

```
(host) #show ap debug multizone ap-name RFCage05_AP214_2_C_6_7031

Multizone Table
---------------
Zone  Configured IP  Serving IP   Max Vaps Allowed  Nodes  Flags
----  -------------  ----------   ----------------  -----  -----
0     10.16.84.10    10.16.84.10  13 (0~12)         1      2
1     10.15.146.3    10.15.146.3  3 (13~15)         4      C2
Flags: C = Cluster; L = Limited nodes; N = Nodes in other zones; 2 = Using IKE version 2;
Number of datazones:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode in managed devices

show ap debug openflow

```
show ap debug openflow
  flows {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
  state {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} detail
```

Description

This command shows the OpenFlow protocol.

Syntax

Parameter	Description	Range	Default
`flows {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}`	Shows OpenFlow protocol flows filtered by specified AP name, IP address of an AP, or IPv6 address of an IP.	–	–
`state {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} detail`	Shows basic or detailed OpenFlow protocol state filtered by specified AP name, IP address of an AP, or IPv6 address of an AP.	–	–

Usage Guidelines

This command shows the OpenFlow protocol. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to show basic OpenFlow protocol state of AP **test**:

```
(host) [mynode] #show ap debug openflow state ap-name test

Controller IP: 0.0.0.0, port:0, State: Init, Last Up:Thu Jan  1 05:30:00 1970, Last down:Thu
Jan  1 05:30:00 1970
Openflow Interface List
   IF MAC:9c:1c:12:c0:95:c8, port_no:8453, name:bond0, oflow_index:0
OpenFlow MAC Bridge List
OpenFlow Dynamic Tunnel List
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug port status

```
show ap debug port status {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Shows the status of the AP's wired ports.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP.
`bssid <bssid>`	BSSID of the AP.
`ip-addr <ip-addr>`	IP address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.

Examples

The output of the command displays the wired port status of an AP named **LocalAP1**. In this example, the output is divided into multiple sections to fit better on the pages of this document. In the actual CLI, it appears in a single long table.

```
(host) [mynode] #show ap debug port status ap-name LocalAP1

AP "LocalAP1" Port Status
-------------------------
Port  MAC                Type  Forward Mode  Admin     Oper  Speed     Duplex  802.3az
802.3bz  PoE
----  ---                ----  ------------  -----     ----  -----     ------  -------  ------
-  ----
0     00:1a:1e:10:05:1a  GE    N/A           enabled   up    1 Gb/s    full    N/A      N/A
  N/A
1     00:1a:1e:10:05:1b  FE    tunnel        enabled   up    100 Mb/s  full    N/A      N/A
  N/A
2     00:1a:1e:10:05:1c  FE    tunnel        enabled   down  N/A       N/A     N/A      N/A
  N/A
3     00:1a:1e:10:05:1d  FE    N/A           disabled  down  N/A       N/A     N/A      N/A
  N/A

STP          TX-Packets  TX-Bytes  RX-Packets  RX-Bytes
---          ----------  --------  ----------  --------
N/A          23697       3338307   27449       8471871
Forwarding   12185       6593226   18436       1758272
Disabled     0           0         0           0
Off          0           0         0           0
```

Command History

Version	Modification
ArubaOS 8.3.0.0	A new column **802.3bz** displays the 802.3bz state of the wired port.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug radar-logs

```
show ap debug radar-logs
   ap-name <ap-name>
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
```

Description

Displays the latest four RADAR event logs from the AP. This command is useful for debugging false radar detection related issues.

This command is applicable for APs running the Broadcom chip-set.

Syntax

Parameter	Description
`ap-name <ap-name>`	Displays RADAR logs for an AP with a specific name.
`ip-addr <ip-addr>`	Displays RADAR logs for an AP with a specific IP address.
`ip6-addr <ip6-addr>`	Displays RADAR logs for an AP with a specific IPv6 address.

Example

The output of this command displays RADAR logs from an AP-225.

```
(host) #show ap debug radar-logs ap-name AP-225

The latest 4 radar event logs
Radar logs:

Pruned Intv:
3220-0
3220-1
3220-2
3220-3
3220-4
3220-5
3220-6
3220-7
3220-8
3220-9
3220-10

Pruned PW:
50-0
50-1
50-2
50-3
50-4
50-5
50-6
50-7
50-8
50-9
50-10
```

```
Nepochs=1 len=27 epoch_#=1; det_idx=0 pw_delta=0 min_pw=50 max_pw=50
Type 7 Radar Detection. Detected pulse index=0 fm_min=0 fm_max=0 nconsecq_pulses=5. Time from
last detection = 19, = 0min 19sec, Time 244
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Radar logs:

Pruned Intv:
4140-0
4140-1
4140-2
4140-3
4140-4
4140-5
4140-6
4140-7
4140-8
4140-9
4140-10

Pruned PW:
19-0
18-1
18-2
19-3
19-4
18-5
19-6
18-7
18-8
18-9
18-10

Nepochs=1 len=30 epoch_#=1; det_idx=0 pw_delta=1 min_pw=18 max_pw=19
Type 7 Radar Detection. Detected pulse index=0 fm_min=0 fm_max=0 nconsecq_pulses=9. Time from
last detection = 3, = 0min 3sec, Time 247
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Radar logs:

Pruned Intv:
4200-0
4200-1
4200-2
4200-3
4200-4
4200-5
4200-6
4200-7
4200-8
4200-9
4200-10

Pruned PW:
17-0
18-1
17-2
16-3
17-4
17-5
17-6
17-7
17-8
17-9
```

```
17-10

Nepochs=1 len=30 epoch_#=1; det_idx=0 pw_delta=2 min_pw=16 max_pw=18
Type 7 Radar Detection. Detected pulse index=0 fm_min=0 fm_max=0 nconsecq_pulses=9. Time from
last detection = 3, = 0min 3sec, Time 250
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Radar logs:
Valid LP: KIntv=151077 Ksalintv=27820 PW=1557 FM=255 pulse#=0 pw2=0 pw_dif=0 pw_tol=8 fm2=0
fm_dif=0 fm_tol=0
nLP=1 nSKIP=0 skipped_salvate=0 pw_fm_matched=0 #non-single=0 skip_tot=0 csect_single=1
Valid LP: KIntv=23 Ksalintv=23 PW=1558 FM=255 pulse#=1 pw2=1557 pw_dif=1 pw_tol=8 fm2=255 fm_
dif=0 fm_tol=127
nLP=2 nSKIP=0 skipped_salvate=0 pw_fm_matched=1 #non-single=1 skip_tot=0 csect_single=0
Valid LP: KIntv=36 Ksalintv=36 PW=1557 FM=255 pulse#=2 pw2=1558 pw_dif=1 pw_tol=8 fm2=255 fm_
dif=0 fm_tol=127
nLP=3 nSKIP=0 skipped_salvate=0 pw_fm_matched=2 #non-single=2 skip_tot=0 csect_single=0
Skipped LP: nLP=3 nSKIP=1 KIntv=59 Ksalintv=59 PW=1557 FM=255 Type=4 pulse#=3 skip_tot=1
csect_single=0
Valid LP: KIntv=35680 Ksalintv=35740 PW=1904 FM=255 pulse#=0 pw2=0 pw_dif=0 pw_tol=8 fm2=0 fm_
dif=0 fm_tol=0
nLP=4 nSKIP=0 skipped_salvate=0 pw_fm_matched=2 #non-single=2 skip_tot=1 csect_single=1
Valid LP: KIntv=25 Ksalintv=25 PW=1904 FM=255 pulse#=1 pw2=1904 pw_dif=0 pw_tol=8 fm2=255 fm_
dif=0 fm_tol=127
nLP=5 nSKIP=0 skipped_salvate=0 pw_fm_matched=3 #non-single=3 skip_tot=1 csect_single=0
Valid LP: KIntv=28 Ksalintv=28 PW=1904 FM=255 pulse#=2 pw2=1904 pw_dif=0 pw_tol=8 fm2=255 fm_
dif=0 fm_tol=127
nLP=6 nSKIP=0 skipped_salvate=0 pw_fm_matched=4 #non-single=4 skip_tot=1 csect_single=0
FCC-5 Radar Detection. Time from last detection = 17, = 0min 17sec, Time 454
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Parameter	Description
`Pruned Intv`	Displays the filtered and pre-processed RADAR pulse interval.
`Pruned PW`	Displays the filtered and pre-processed RADAR pulse width.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug radio-event-log status

```
show ap debug radio-event-log status {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show information about the radio event information captured in packet log files.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IPv4 address by entering its IPv4 address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show log information for an AP with a specific IPv6 address by entering its IPv6 address.

Example

```
Radio Event Logs
----------------
Radio Index  Radio's Bssid      Radio's Band  Event Type  Log File Size  Status
-----------  -------------      ------------  ----------  -------------  ------
0            00:24:6c:bd:65:b0  80211a        N/A         N/A            start
1            00:24:6c:bd:65:a0  80211g        N/A         N/A            stop
```

The output of this command includes the following information:

Parameter	Description
`radio Index`	Index number of the AP radio (0 or 1)
`Radio's BSSID`	BSSID of the AP radio. This is typically the AP radio's MAC address.
`Radio's Band`	Band used by the AP radio.
`Event Type`	Type of events recorded. By default, all supported event types are recorded. ■ N/A: The default event type setting, which captures all supported types of radio events. ■ ani Adaptive Noise Immunity control events ■ rcfind: Transmission (Tx) control event ■ rcupdate: Transmission (Tx) rate update event ■ rx: Received (Rx) status register event ■ text: Text record event ■ tx: Transmission (Tx) control and Tx status register event
`Log File Size`	Size of the log file. A value of N/A indicates that the packet log feature uses the default log file size of 3145728 bytes (3MB)
`Status`	Shows if packet log capture was started or stopped on the AP radio.

Related Commands

ap debug radio-event-log

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap debug radio-info

```
show ap debug radio-info
   ap-name <ap-name> radio <radio>
   ip-addr <ip-addr> radio <radio>
   ip6-addr <ip6-addr> radio <radio>
```

Description

Displays the Wi-Fi radio debug logs from the AP driver.

This command is applicable for 200 Series, 210 Series, 220 Series, and 270 Series access points.

Syntax

Parameter	Description
`ap-name <ap-name>`	Displays Wi-Fi radio debug logs for an AP with a specific name.
`ip-addr <ip-addr>`	Displays Wi-Fi radio debug logs for an AP with a specific IP address.
`ip6-addr <ip6-addr>`	Displays Wi-Fi radio debug logs for an AP with a specific IPv6 address.

Example

The output of this command displays the log information about Wi-Fi radio 0 for an AP-225:

```
(host) #show ap debug radio-info ap-name AP-225 radio 0

Radio Info Script
-----------------
aruba_dbg_radio_info_0 Start time: Fri Mar 27 14:33:21 IST 2015
----------------------------------------------------------------
wifi0-drop-list:
_dma_rxreclaim(1633): 2520/2520 0/0
wlc_recvctl(44993): 3130421/3130421 0/0
wlc_dotxstatus(41101): 2502/2502 2502/2502
...
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug radio-registers

```
show ap debug radio-registers  {ap-name <name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>} {radio 0|1}
```

Description

This command allows you to view radio register changes.

Syntax

Parameter	Description
`ap-name`	Name of the AP for which you want to view register changes.
`ip-addr`	IPv4 address of the AP for which you want to view register changes.
`ip6-addr`	IPv6 address of the AP for which you want to view register changes.
`radio 0|1`	Show information for the specified radio on the AP.

Usage Guidelines

This command displays radio register changes made under the supervision of Aruba technical support.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug radio-stats

```
show ap debug radio-stats {ap-name <ap-name>|ip-addr <ip-addr>} radio {0|1} [advanced]
```

Description

Show aggregate radio debug statistics of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	IPv6 address of the Access Point.
`radio {0|1}`	Specify the ID number of the radio for which you want to view statistics.
`advanced`	Include this parameter to display additional radio statistics.

Example

The output of this command displays general statistics for the radio, as well as statistics for transmitted and received frames.

```
(host) #show ap debug radio-stats ap-name AP12 radio 1
RADIO Stats
-----------
Parameter            Value
---------            -----
-------------------  General Per-radio Statistics
Total Radio Resets   0
Resets Beacon Fail   0
TX Power Changes     5
Channel Changes      2
Radio Band Changes   0
Current Noise Floor  95
11g Protection       0
-------------------  Transmit specific Statistics
Frames Rcvd For TX   2452151
Tx Frames Dropped    1736429
Frames Transmitted   4247212
Tx EAPOL Frames                    0
TX STBC Frames                     0
TX LDPC Frames                     0
Tx AGGR Good                       0
Tx AGGR Unaggr                     20
Tx Data Priority [BE]              20
Tx Data Frames  12 Mbps  (Mon)     0
Tx Data Frames  24 Mbps  (Mon)     0
Tx Data Frames  36 Mbps  (Mon)     0
Tx Data Frames  54 Mbps  (Mon)     0
Tx Data Frames  72 Mbps  (Mon)     0
Tx Data Frames 108 Mbps  (Mon)     0
Tx Data Frames 300 Mbps  (Mon)     20
Tx Data Frames 450 Mbps  (Mon)     0
```

```
Tx Data Frames 1300 Mbps  (Mon)      0
Tx Data Frames 1300 Mbps+ (Mon)      0
Tx Data Bytes   12 Mbps   (Mon)      0
Tx Data Bytes   24 Mbps   (Mon)      0
Tx Data Bytes   36 Mbps   (Mon)      0
Tx Data Bytes   54 Mbps   (Mon)      0
Tx Data Bytes   72 Mbps   (Mon)      0
Tx Data Bytes  108 Mbps   (Mon)      0
Tx Data Bytes  300 Mbps   (Mon)      4371
Tx Data Bytes  450 Mbps   (Mon)      0
Tx Data Bytes  1300 Mbps  (Mon)      0
Tx Data Bytes  1300 Mbps+ (Mon)      0
Tx 6 Mbps                            7
Tx HT 130 Mbps                       20
Tx WMM [BE]                          20
Tx UAPSD OverflowDrop                0
TX Timeouts                          0
Lost Carrier Events                  0
Tx HT40 Hang Detected                0
Tx HT40 Hang Stuck                   0
Tx HT40 Hang Possible                0
Tx HT40 Dfs IMM WAR                  0
Tx HT40 Dfs HT20 WAR                 0
Tx MAC/BB Hang Stuck                 0
Tx Mgmt Bytes                        415
Tx Beacons Bytes                     0
Tx Managment Frames Dropped          1
Tx AMSDU pkt count                   0
Tx EAPOL Frames Rcvd                 0
Tx EAPOL Frames Dropped              0
Tx Data Frames MCS 7                 20
Tx Data Frames MCS                   20
Tx Data Frames NSS2                  20
Tx Data Frames Long-GI(FULL)         20
Tx Data Frames BW 20                 20
-------------------                  Received Statistics
Rx Last SNR                          15
Rx Last SNR CTL0                     15
```

If you include the **advanced** option at the end of the **show ap debug radio-stats** command, the output of this command will include all the following parameters, as well as additional information for the SNR, frame counts, channel busy times, and data bytes for transmitted and received packets. If you omit the **advanced** option, the output will include less information, and the data will be displayed in a different order. The following table describes the output of this command when the **advanced** option is included.

Parameter	Description
`Total Radio Resets`	Total number of times the radio reset.
`Resets Beacon Fail`	Number of times the radio reset due to beacon failure.
`BB check positives`	Number of times the radio checked for a base-band hang condition

Parameter	Description
Resets BeacQ Stuck	An AP's radio typically sends a beacon every 100 milliseconds. If beacons are not sent at a regular interval or the radio experiences excessive noise, the beacon queue will reset. This parameter indicates the number of queue resets.
Resets Fatal Intr	Number of time the radio was reset because the AP hardware was unresponsive.
Resets RX Overrun	The number of radio resets due to Receive FIFO overruns.
Resets RF Gain	Number of radio resets due to gain changes.
Resets MTU Change	Number of times the radio reset due to a change in the Maximum Transmission Unit (MTU) value.
Resets TX Timeouts	Number of radio resets due to transmission timeouts (the radio doesn't transmit a signal within the required time frame.)
POE-Related Resets	If the radio power profile drops, an AP may not be able to support three transmit chains, and may drop to two chains only. This parameter displays the number of resets due to this type of power change.
External Reset	Number of times the AP has been reset because it was unplugged or its reset button was pressed.
PCI Fatal Intr Reset	Radio reset due to PCI fatal interrupt received from radio chip.
Chaimask Reset	Radio reset when new chain mask is configured.
TX stat Reset	Radio reset caused by inconsistent state of hardware transmit queue.
TX Power Changes	Number of times the radio's transmission power changed.
Channel Changes	Number of times the radio's channel changed.
Radio Band Changes	Number of time the radio's band changed.
Current Noise Floor	The residual background noise detected by an AP. Noise seen by an AP is reported as -dBm. Therefore, a noise floor of -100 dBm is smaller (lower) than a noise floor of -50 dBm. For most environments, the noise floor should be no greater than -80 dBm. Anything larger may indicate an interference problem which is drowning out good signals (data) in background noise.
Dummy NF pkts on home channel	Number of noise floor readings on the home channel.
Dummy NF pkts on scan channel	Number of noise floor readings on the scan channel.
Avail TX Buffers	An AP has a set number of buffers which it can use to buffer frames for non-responsive power save clients. The total number of buffer frames depends upon the AP model type.

Parameter	Description
11g Protection	This parameter shows whether 802.11g protection has been enabled or disabled.
Last TX Antenna	This parameter indicates whether the last frame transmitted was sent on antenna 1 or antenna 0. This parameter can be useful for troubleshooting external antennas.
Last RX Antenna	This parameter indicates whether the last frame received was via antenna 1 or antenna 0. This parameter can be useful for troubleshooting external antennas.
Scan Requests	Total number of scan requests received by the AP.
Scan Rejects	Total number of scan rejected by the AP.
Scan Rejects (Misc 1)	Number of scan rejects due to pending transmissions.
Load aware Scan Rejects	Load aware ARM preserves network resources during periods of high traffic by temporarily halting scanning if the load for the AP gets too high. The **load aware Scan Rejects** parameter shows the number of times the AP has rejected a scan because of the load aware scan feature.
PS aware Scan Rejects	If the ARM power-save aware scan feature is enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode. The **ps aware Scan Rejects** parameter shows the number of times the AP has rejected a scan because of the power-save aware scan feature.
EAP Scan Rejects	If you enable the EAP-aware scanning feature in the AP's ARM profile, the AP will not attempt to scan a different channel if the Extensible Authentication Protocol over LAN (EAPOL) exchange is in progress with a client. This parameter shows the number of times the AP has rejected a scan because of the EAP aware scanning feature.
Voice aware Scan Rejects	If you enable the VoIP Aware Scan feature in the AP's ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This **Voice aware scan Rejects** parameter shows the number of times the AP has rejected a scan because of the Voip aware scan feature.
Video aware Scan Rejects	If you enable the Video Aware Scan feature in the AP's ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active video session. This **Video aware scan Rejects** parameter shows the number of times the AP has rejected a scan because of the Video aware scan feature.
UAPSD Scan Rejects	Number of times the scan was rejected due to UAPSD-related transmissions.
Post radar related scan Rejects	Number of times the scan was rejected due to recent radar detection.

Parameter	Description
CABQ traffic Scan Rejects	Number of times the scan was rejected due to pending multicast transmissions.
Radio Reset Scan Rejects	Number of times the scan was rejected due to a recent radio reset.
Queue Drain Scan Rejects	This legacy statistic has been deprecated, and will not increment.
Scan Success	Number of successful scans. To view scan details, use the command **show ap arm scan-times**.
Scan Deferred	Number of times the scan was deferred due to pending beacon transmissions on the home channel.
EIRP	The value of this parameter is the transmission power level (in dBm) + the antenna gain value.
MAX EIRP	The max EIRP depends on AP capability and the regulatory domain constraint for the channel of operation. For example, in the US, Channels 36-48 have max EIRP of 23dBm
Dummy<number>	For internal use only.
UAPSD Flush STA Wake	Number of times a client wakes from power-save mode and flushes the UAPSD queue.
UAPSD SP Set	The number of unique UAPSD Scheduled Period is started in response to UAPSD trigger frames.
UASPD Dup Trig	The number of times duplicate UAPSD trigger frames are received (i.e., retried UAPSD triggers that were received by the AP more than once).
UAPSD Recv frame for TX	The number of frames received for transmission over the air interface using UAPSD
UAPSD Ageout Drain	The number of time UAPSD queue is drained (i.e. frames are dropped) due to ageout.
UAPSD TX proc comp	The number of UAPSD frames that were successfully transmitted
UAPSD SP In prog	The number of times a trigger frame was received while a Scheduled Period (SP) was already in progress based on an earlier trigger frame.
UAPSD QOS NULL TX	The number of times the AP had to respond with a QoS Null Data frame in response to a UAPSD trigger because AP did not have Data frame queued for that client
UAPSD TX HW Queued	The number of frames (Data and Null Data) that were transferred to the radio HW for transmission, in response to UAPSD triggers.
UAPSD SP Reset	The number of times the UAPSD Scheduled Period (SP) in progress is reset or canceled.

Parameter	Description
Tx Time perct @ beacon intvl	Percentage of time spent transmitting Wi-Fi frames since the last beacon.
Tx Frames Rcvd	Number of transmitted frames that were received.
Tx Bcast Frames Rcvd	Number of transmitted broadcast frames that were received.
Tx Frames Dropped	Number of transmitted frames that were dropped.
Tx Bcast Frames Dropped	Number of transmitted broadcast frames that were dropped.
Tx Frames Transmitted	Number of frames successfully transmitted.
Tx Bytes Rcvd	Number of transmitted bytes received.
Tx Bytes Transmitted	Number of transmitted bytes
Tx Time Frames Rcvd	Number of times transmitted frames were received.
Tx Time Frames Dropped	Number of times transmitted frames were dropped.
Tx Time Frames Transmitted	Number of times frames were transmitted.
Tx PS Unicast	Number of power save unicast frames
Tx DTIM Broadcast	Number of broadcast frames with DTIM values.
Tx Success With Retry	Number of frames that were successfully transmitted after being retried.
Tx Multiple retries	Number of frames that were successfully transmitted after being retried multiple times.
Tx Mgmt Frames	Number of management frames transmitted.
Tx Mgmt Frames (PPS)	Rate of retransmitted frames, in packets per second.
Tx Beacons Transmitted	Number of beacons transmitted.
Tx Beacons Transmitted (PPS)	Rate of transmitted beacons, in packets per second.
Tx Probe Responses	Number of transmitted probe responses.
Tx Probe Responses (PPS)	Rate of transmitted probe responses, in packets per second.
Tx Data Transmitted Retried	Number of retried data frames.
Tx Data Transmitted	Number of transmitted data frames.
Tx Data Frames	Number of transmitted data frames.
Tx Broadcast Data Frames In	Number of broadcast data frames received by the AP from wired interface to be transmitted in the air.

Parameter	Description
Tx Data Bytes Transmitted	Total data bytes received by an AP from its wired interface to be transmitted over the air.
Tx Data Bytes	Total data bytes transmitted by the AP over the air.
Tx Time Data Transmitted	Total time on spent successfully transmitting frames (including the retried frames).
Tx Time BC/MC Data	Total time spent transmitting broadcast/multicast frames.
Tx Time Data dropped	Total time spent transmitting dropped frames.
Tx Time Data	Total time spent sending frames received for transmission, including the frames that were dropped after retrying.
Tx Broadcast Data Frames Sent	Broadcast data frames transmitted by the AP.
Tx Broadcast Data Frames Sent(PPS)	Rate of broadcast data frames transmitted by the AP, in packets per second.
Tx Multicast Data Frames	Multicast data frames transmitted by the AP.
Tx Multicast Data Frames(PPS)	Rate of multicast data frames transmitted by the AP, in packets per second.
Tx DMO Multicast	The number of multicast frames transmitted as multicast without converting to unicast.
Tx DMO Invalid	The number of multicast frames which should have been converted but were not as due to invalid format. (This value is typically normally 0.)
Tx DMO Converted	The number of multicast frames received as multicast which were then converted to unicast one or more times. This counter increments once per multicast frame.
Tx DMO Replicated	The number of frames transmitted as unicast frames. For each multicast frame the counter is incremented by the number of replications for that frame. (The number of replications is the number of clients associated to the BSSID, VLANor group receiving these frames).
Tx DMO Dropped	The number of frames dropped as conversion was not consistent with state on the AP. (This value is typically normally 0.)
Tx DMO No Client	Number of times no client was found for an association-ID indicated by the frame. (This value is typically normally 0.)
Tx DMO No BSSID	Number of times the BSSID indicated by the frame was not found. (This value is typically normally 0.)
Tx Unicast Data Frames	Number of transmitted unicast data frames
Tx RTS Success	Number of Ready To Send (RTS) frames successfully transmitted.

Parameter	Description
Tx RTS Failed	Number of Ready To Send (RTS) frames that were not successfully transmitted
Tx CTS Frames	Number of Clear-to-Send (CTS) frames transmitted.
Tx CTS Frames (PPS)	Rate of CTS frames sent, in packets per second. (This parameter does not include CTS frames send in response to RTS).
Tx Powersave Queue Timeouts	Number of transmit frames discarded from the power save queue because the frames aged out
Tx Dropped After Retry	Number of frames dropped after an attempted retry.
Tx Dropped No Buffer	Number of frames dropped because the AP's buffer was full.
Tx Missed ACKs	Number of retries triggered because an acknowledgment was not received.
Tx Failed Beacons	Number of times a radio failed to transmit a beacon at the scheduled interval (100ms).
Tx Multi-Beacon Fail	Number of times multiple consecutive beacons failed to transmit.
Tx Long Preamble	Number of frames sent with a long preamble.
Tx Short Preamble	Number of frames sent with a short preamble.
Tx Beacon Interrupts	Number of broadcast beacons that were interrupted.
TX Interrupts	Number of transmission interrupts.
Tx FIFO Underrun	The number of transmitted FIFO overruns.
Tx Allocated Desc	Number of allocated transmit descriptors.
Tx Freed Desc	Number of freed transmit descriptors.
Tx EAPOL Frames	Number of EAPOL frames transmitted
TX STBC Frames	Number of transmitted frames with Space-time block coding (STBC) enabled.
TX LDPC Frames	Number of transmitted frames with Low Density Parity Check (LDPC) enabled.
Tx AGGR Good	Number of aggregated frames successfully transmitted.
Tx AGGR Unaggr	Number of non-aggregate frames transmitted due to unavailability of additional frames for aggregation at the time of transmission.
Tx data <number> Mbps	Number of frames transmitted at the specified rate (in Mbps).

Parameter	Description
`Tx <number> Mbps [Long]`	Number of frames with a long preamble transmitted at the specified rate.
`Tx <number> Mbps [Short]`	Number of frames with a short preamble transmitted at the specified rate.
`Tx HT <number> Mbps`	Number of high-throughput frames transmitted at the specified rate.
`Tx WMM [category]`	Number of Wi-Fi Multimedia (WMM) packets transmitted for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. Tx WMM [BE]: Best Effort Tx WMM [BK]: Background Tx WMM [VO]: VoIP Tx WMM [VI]: Video
`Tx WMM [category] dropped`	Number of dropped Wi-Fi Multimedia (WMM) packets in the following access categories . If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. Tx WMM [BE]: Best Effort Tx WMM [BK]: Background Tx WMM [VO]: VoIP Tx WMM [VI]: Video
`Tx UAPSD OverflowDrop`	Number of packets dropped due to Unscheduled Automatic Power Save Delivery (U-APSD) overflow.
`TX Timeouts`	Number of transmission timeouts
`Lost Carrier Events`	Number of carrier sense timeouts.
`Tx HT40 Hang Detected`	Parameter deprecated.
`Tx HT40 Hang Stuck`	Parameter deprecated.
`Tx HT40 Hang Possible`	Parameter deprecated.
`Tx HT40 Dfs IMM WAR`	Number of times the HT 40 RX Clear Hang immunity workaround was employed.
`Tx HT40 Dfs HT20 WAR`	Number of times the HT 20 RX Clear Hang immunity workaround was employed.
`Tx MAC/BB Hang Stuck`	Number of times a workaround was employed for potential beacons stuck due to MAC or base-band stuck conditions.
`Tx Mgmt Bytes`	Total management frame bytes transmitted.
`Tx Beacons Bytes`	Total number of Beacon frame bytes transmitted.
`Tx Data Frames/Bytes 24 Mbps (Mon)`	Total number of data frames and corresponding bytes transmitted at rate (12-24)
`Tx Data Frames/Bytes 36 Mbps (Mon)`	Total number of data frames and corresponding bytes transmitted at rate (24-36)

Parameter	Description
Tx Data Frames/Bytes 54 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (36-54)
Tx Data Frames/Bytes 72 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (54-72)
Tx Data Frames/Bytes 108 Mbps (Mon)	Total number of data frames and corresponding bytes transmitted at rate (72-108)
Tx Data Frames MCS 0	Total number of data frames transmitted at rate of MCS 0
Tx Data Frames MCS 1	Total number of data frames transmitted at rate of MCS 1
Tx Data Frames MCS 2	Total number of data frames transmitted at rate of MCS 2
Tx Data Frames MCS 3	Total number of data frames transmitted at rate of MCS 3
Tx Data Frames MCS 4	Total number of data frames transmitted at rate of MCS 4
Tx Data Frames MCS 5	Total number of data frames transmitted at rate of MCS 5
Tx Data Frames MCS 6	Total number of data frames transmitted at rate of MCS 6
Tx Data Frames MCS 7	Total number of data frames transmitted at rate of MCS 7
Tx Data Frames MCS 8	Total number of data frames transmitted at rate of MCS 8
Tx Data Frames MCS 9	Total number of data frames transmitted at rate of MCS 9
Tx Data Frames Legacy	Total number of data frames transmitted at legacy rate
Tx Data Frames MCS	Total number of data frames transmitted at MCS rate
Tx Data Frames NSS1	Total number of data frames transmitted 1 spacial stream
Tx Data Frames NSS2	Total number of data frames transmitted with 2 spacial stream
Tx Data Frames NSS3	Total number of data frames transmitted with 3 spacial stream
Tx Data Frames Short-GI(HALF)	Total number of data frames transmitted with short GI
Tx Data Frames Long-GI(FULL	Total number of data frames transmitted with long GI
Tx Data Frames BW20	Total number of data frames transmitted at 20 Mhz
Tx Data Frames BW40	Total number of data frames transmitted at 40 Mhz
Tx Data Frames BW80	Total number of data frames transmitted at 80 Mhz
Tx Data Frames BW160	Total number of data frames transmitted at 160 Mhz
Tx Data Frames Dropped	Number of transmitted data frames that were dropped.
Tx AMSDU pkt count	Total number of AMSDU bytes transmitted.

Parameter	Description
Rx Last SNR	The last recorded signal-to-noise ratio.
Rx Last SNR CTL0	The signal-to-noise ratio for the last received data packet on the primary (control) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL1	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR CTL2	The signal-to-noise ratio for the last received data packet on the secondary (control) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR EXT0	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 0. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR EXT1	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 1. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Last ACK SNR EXT2	Signal-to-noise ratio for the last received ACK packet on the secondary (extension) channel 2. This parameter is only displayed for APs operating in 40 Mhz mode.
Rx Frames Received	Number of frames received.
Rx Good Frames	Number of frames received with no errors.
Rx Bad Frames	Number of bad or error frames received.
Rx Total Data Frames Recvd	Total number of data frames received.
Rx Total Mgmt Frames Recvd	Total number of management frames received.
Rx Total Control Frames Recvd	Total number of control frames received.
Rx Total Bytes Recvd	Total number of bytes received.
Rx Total Data Bytes Recvd	Total number of data bytes received.
Rx Total RTS Frames Recvd	Total number of Ready-To-Send (RTS) frames received.
Zx Total CTS Frames Recvd	Number of Clear-to-Send (CTS) frames received.

Parameter	Description
Rx Total ACK Frames	Number of acknowledgment frames received.
Rx Total Beacons Received	Number of beacons received.
Rx Total Probe Requests	Number of probe requests received.
Rx Total Probe Responses	Number of probe responses received.
Rx retry frames	Number of retried frames received.
Channel busy 1s	The percentage of time the radio channel was busy in the last 1 second.
Channel busy 4s	The percentage of time the radio channel was busy in the last 4 seconds.
Channel busy 64s	The percentage of time the radio channel was busy in the last 64 seconds.
Ch Busy perct @ beacon intvl	Percentage of time the channel was busy over the last 30 beacon intervals.
Rx Time perct @ beacon intvl	Percentage of time the AP was receiving data over the last 30 beacon intervals.
Rx Discarded Events	Number of non-802.11 events that were detected and discarded during normal operation.
Rx ARM Scan Frames	Number of scan frames sent for the adaptive radio management (ARM) feature.
Rx Data Frames	Number of data frames received.
Rx Data Frames (PPS)	Rate at which data frames were received, in packets per second.
Rx Data Bytes	Number of data bytes received.
Rx Time Data	Total time spent on frames successfully received.
Rx Duplicate Frames	Number of duplicate frames received.
Rx Broadcast Data Frames	Number of broadcast frames received.
Rx Multicast Data Frames	Number of multicast frames received.
Rx Unicast Data Frames	Number of unicast frames received.
Rx Null Data Frames	Number of null data frames received.
Rx Mgmt Frames	Number of management frames received.
Rx Mgmt Frames (PPS)	Rate at which management frames were received, in packets per second.
Rx Control Frames	Number of control frames received.

Parameter	Description
Rx Control Frames (PPS)	Rate at which control frames were received, in packets per second.
Rx Frames To Me	Number of frames received that are addressed to the specified BSSID.
Rx Bytes To Me	Number of bytes received that are addressed to the specified BSSID.
Rx Time To Me	Total time spent receiving frames sent to a specified BSSID.
Rx Broadcast Frames	Number of broadcast frames received.
Rx Probe Requests	Number of Probe requests received.
Rx Probe Requests (PPS)	Rate at which probe requests were received, in packets per second.
Rx RTS Frames	Ready To Send (RTS) frames received. These frames are sent when a computer has data to transmit.
Rx RTS Frames (PPS)	Rate at which RTS frames were received, in packets per second.
Rx CTS Frames	Clear To Send (CTS) frames received. This type of frame are used to verify that a client is ready to receive information.
Rx CTS Frames (PPS)	Rate at which CTS frames were received, in packets per second.
RX PS Poll Frames	Power-Save Poll (PS-Poll) frames received. When a client exits a power-saving mode, it transmits a PS-Poll frame to the AP to retrieve any frames buffered while it was in power-saving mode.
RX CRC Errors	Cyclic Redundancy Check (CRC) is a data sequence that is sent with a frame to help verify if all the data received correctly. Possible CRC error causes include: ■ Hardware malfunction ■ Loose or unconnected cables ■ RF interference, such as overlapping access point coverage on a channel or interfering 2.4-GHz signals from devices like microwave ovens ■ and wireless handset phones
RX PLCP Errors	Physical Layer Convergence Protocol (PLCP) errors.
Rx Frames Dropped	Number of received frames that were dropped.
Rx PHY Events	The number of Physical Layer Events, that are not 802.11 packets, detected by radio as part of its normal receive operation.
Rx RADAR Events	Number of times an AP detects a radar signature. Aruba APs are DFS-compliant detects a radar signature, it will change its channel.

Parameter	Description
RX Interrupts	The number of receive interrupts received by the CPU from the radio.
RX Overrun	The number of Receive FIFO overruns.
Rx undecryptable	Number of non-decryptable frames received.
RX STBC Frames	Number of received frames with STBC enabled.
RX LDPC Frames	Number of received frames with LDPC enabled.
Rx data <number> Mbps	Data packets received at the specified rate (in Mbps).
Rx <number> Mbps	Packets received at the specified rate (in Mbps).
Rx data <number> Mbps	Packets received at the specified rate (in Mbps).
Rx HT <number> Mbps	Number of high-throughput packets received at the specified rate.
Rx WMM [BE]	Number of Wifi Multimedia (WMM) packets received for the following access categories. If the AP has not transmitted packets in a category type, this data row will not appear in the output of the command. Rx WMM [BE]: Best Effort Rx WMM [BK]: Background Rx WMM [VO]: VoIP Rx WMM [VI]: Video
RX bad length	Number of frames received with incorrect length.
Rx Null Src MAC	Number of received frames with source MAC address as NULL.
Rx Managment Frames Dropped	Number of received management frames that were dropped.
Rx Data Frames Dropped	Number of received data frames that were dropped.
SNR from CTL0	Signal-to-noise ratio (SNR) on chain 0.
Throttle drops	Number of received frames dropped by AP due to throttling when AP is under high load.
Stop all but Mgmt	Number of data frames dropped because radar was detected on a channel. An AP is allowed to send management frames only and must drop all other frames when radar is detected on a channel.

Command History

Command	Description
ArubaOS 8.3.0.0	The output of this command now includes MCS bucket mapping information channel width, number of spatial streams, and guard interval information of 802.11ac APs.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug received-config

```
show ap debug received-config
   ap-name <ap-name> [essid <essid>]
   bssid <bssid> [essid <essid>]
   ip-addr <ip-addr> [essid <essid>]
   ip6-addr <ip6-addr> [essid <essid>]
```

Description

Show the configuration the AP downloaded from the managed device.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show log information for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Example

The output of this command displays configuration information for each interface. The example below shows only part of the output for this command. Additional parameters not shown in this example are described in the table below.

```
(host) #show ap debug received-config ap-name AP12

Downloaded Config for WIFI 0
----------------------------
Item                                Value
----                                -----
BSSID
LMS IP                              10.6.2.250
Master IP                           10.100.103.2
Mode                                AP Mode
QBSS Probe Response                 Allow Access
Native VLAN ID                      1
SAP MTU                             1500 bytes
Heartbeat DSCP                      0
High throughput enable (radio)      Enabled
Channel                             40-
Beacon Period                       100 msec
Transmit Power                      15 dBm
Advertise TPC Capability            Disabled
Enable CSA                          Disabled
CSA Count                           4
Management Frame Throttle interval  1 sec
Management Frame Throttle Limit     20
Active Scan                         Disabled
VoIP Aware Scan                     Enabled
Power Save Aware Scan               Enabled
```

```
Load aware Scan Threshold           1250000 Bps
40 MHz intolerance                  Disabled
Honor 40 MHz intolerance            Enabled
Legacy station workaround           Disabled
Country Code                        US
ESSID                               guest
...
```

The output of this command includes the following information:

Parameter	Description
BSSID	The BSSID of the AP.
LMS IP	The LMS IP is the IP address of the managed device used by the AP for client data processing.
Master IP	IP address of Mobility Master, the central configuration and management point for all managed devices.
Mode	Shows the operating modes for the AP. ap-mode: Device provides transparent, secure, high-speed data communications between wireless network devices and the wired LAN. am-mode: Device behaves as an air monitor to collect statistics, monitor traffic, detect intrusions, enforce security policies, balance traffic load, self-heal coverage gaps, etc.
QBSS Probe Response	Quality-of-service BSS (QBSS).
Native VLAN ID	The ID number of the Native VLAN.
SAP MTU	The Maximum Transmission Unit (MTU) for the GRE tunnel.
Heartbeat DSCP	DSCP value for the heartbeat traffic between the AP and the managed device.
High throughput enable (radio)	Shows if high-throughput (802.11n) features on tare enabled or disabled on the radio.
Channel	Shows the channel number for the AP's 802.11a/802.11n physical layer.
Beacon Period	Shows the time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Transmit Power	Shows the current transmission power level.
Advertise TPC Capability	If enabled, the AP will advertise its Transmit Power Control (TPC) capability.
Enable CSA	Displays whether or not the AP has enabled channel switch announcements (CSAs) for 802.11h.
CSA Count	Number of channel switch announcements that must be sent before the AP will switch to a new channel.

Parameter	Description
Management Frame Throttle interval	Average interval that rate limiting management frames are sent from this radio, in seconds. If this column displays a zero (**0**), rate limiting is disabled for this AP.
Management Frame Throttle Limit	Maximum number of management frames that can come from this radio in each throttle interval.
Active Scan	Displays whether or not the active scan feature is enabled. This option elicits more information from nearby APs, but also creates additional management traffic on the network. **Active Scan** is disabled by default, and should *not be enabled* except under the direct supervision of Aruba Support.
VoIP Aware Scan	Shows if VoIP aware scanning is enabled or disabled. If you use voice handsets in the WLAN, **VoIP Aware Scan** should be enabled in the ARM profile so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call. This option requires that **Scanning** is also enabled.
Power Save Aware Scan	Shows if the power save aware scan is enabled or disabled. If enabled, the AP will not scan a different channel if it has one or more clients and is in power save mode.
Load aware Scan Threshold	The **Load Aware Scan Threshold** is the traffic throughput level an AP must reach before it stops scanning. Load aware ARM preserves network resources during periods of high traffic by temporarily halting ARM scanning if the load for the AP gets too high.
40 MHz intolerance	The specified setting allows ARM to determine if 40 MHz mode of operation is allowed on the 5 GHz or 2.4 GHz frequency band only, on both frequency bands, or on neither frequency band.
Honor 40 MHz intolerance	Shows if 40 MHz intolerance is enabled or disabled. If enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Legacy station workaround	Shows if interoperability for misbehaving legacy stations is enabled or disabled.
Country Code	Display the country code for the AP. The country code specifies allowed channels for that country.
ESSID	An Extended Service Set Identifier (ESSID), for the AP.
Encryption	Encryption type used on this AP.
WPA2 Pre-Auth	802.11x settings are **enabled** or **disabled**.
DTIM Interval	Number of beacons that should elapse before an AP sends beacon broadcasts for power save clients.
802.11a Basic Rates	Minimum data rate required for a client to associate with the AP. For an 802.11a radio, this value can be 6, 12 and 24 802.11 data rates. 802.11b/g radios will report a value of 1 and 2 802.11 data rates.

Parameter	Description
802.11a Transmit Rates	802.11 data rate at which the AP will transmit data to its clients. This value can be 6-54 for 802.11a radios, and 1-54 for 802.11b/g radios.
Station Ageout Time	Number of seconds a station may be idle before it is deauthorized from an AP.
Max Transmit Attempts	maximum number of times the AP will attempt to retransmit data.
RTS Threshold	The minimum packet size at which the AP will issue a request-to-send (RTS) before sending the packet.
Max Associations	The maximum number of clients allowed to associated with the AP
Wireless Multimedia (WMM)	Shows if Wireless Multimedia (WMM) is enabled or disabled for this AP. WMM provides prioritization of specific traffic relative to other traffic in the network.
WMM TSPEC Min Inactivity Interval	Displays the minimum inactivity time-out threshold of WMM traffic for this AP.
DSCP mapping for WMM voice AC	Displays the DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	Displays the DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	Displays the DSCP value used to map WMM best-effort traffic
DSCP mapping for WMM background AC	Displays the DSCP value used to map WMM background traffic.
Hide SSID	Shows if the feature to hide a SSID name in beacon frames is **enabled** or **disabled**.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if local probe response is enabled or disabled on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the managed device sends the 802.11 probe responses
Disable Probe Retry	Shows if the AP has enabled or disabled MAC-level retries for probe response frames. By default this parameter is enabled, which mean that MAC level retries for probe response frames is disabled.
Maximum Transmit Failures	Display the maximum number of transmission failures allowed before the client gives up.

Parameter	Description
BC/MC Rate Optimization	Shows if the AP has enabled or disabled scanning of all active stations currently associated to that AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
High throughput enable (SSID)	Shows if the AP has enabled or disabled the use of its high-throughput SSID in 40 MHz mode.
40 MHz channel usage	Determines if this high-throughput SSID allows high-throughput (802.11n) stations to associate.
MPDU Aggregation	Shows if the AP has enabled or disabled MAC protocol data unit (MDPU) aggregation.
Max transmitted A-MPDU size	Shows the maximum size, in bytes, of an A-MPDU that can be sent on the AP's high-throughput SSID.
Max received A-MPDU size	Shows the maximum size, in bytes, of an Aggregated-MAC Packet Data Unit (A-MPDU) that can be received on the AP's high-throughput SSID.
Min MPDU start spacing	Displays the minimum time between the start of adjacent MDPUs within an aggregate MDPU, in microseconds.
Supported MCS set	Comma-separated list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this high-throughput SSID.
Short guard interval in 40 MHz mode	Shows if the AP has enabled or disabled use of short guard interval in 40 MHz mode of operation.
VLAN	VLAN ID used by the SSID.
Forward mode	Shows the current forward mode (bridge, split-tunnel, or tunnel) for the virtual AP. This parameter controls whether 802.11 frames are tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). Only 802.1X authentication is supported when configuring bridge or split tunnel mode.
Band Steering	Shows if band-steering has been enabled or disabled for a virtual AP. ARM's band steering feature encourages dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40 MHz or 20 MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug received-log-config

```
show ap debug received-log-config {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows log of configuration received by an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows log of configuration received by specified AP name.
`ip-addr <ip-addr>`	Shows log of configuration received by an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows log of configuration received by an AP for specified IPv6 address.

Usage Guidelines

This command shows log of configuration received by an AP. For the remaining parameters, see the command syntax.

Example

The following example shows log of configuration received by an AP named ap-205:

```
(host) [mynode] #show ap debug received-log-config ap-name ap-205

AP log level config
-------------------
Facility  Level     Sub Category  Level
--------  -----     ------------  -----
arm       warnings
network   warnings
security  warnings  ids           warnings
security  warnings  ids-ap        warnings
system    warnings
user      warnings
wireless  warnings
Log level config version :1

AP debug level config
---------------------
Facility  Level  Debug value  Sub Category
--------  -----  -----------  ------------
Debug log config version :1
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug received-reg-table

```
show ap debug received-reg-table {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows downloaded regulatory table for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows downloaded regulatory table for a specified AP name.
`bssid <bssid>`	Shows downloaded regulatory table for a specified BSSID.
`ip-addr <ip-addr>`	Shows downloaded regulatory table for a specified IP address.
`ip6-addr <ip6-addr>`	Shows downloaded regulatory table for a specified IPv6 address.

Usage Guidelines

This command shows downloaded regulatory table for an AP. For the remaining parameters, see the command syntax.

Example

The following example shows downloaded regulatory table for an AP named ap-205:

```
(host) [mynode] #show ap debug received-reg-table ap-name ap-205

Country reg-info for Country Code "US"
--------------------------------------
PHY Type                  Allowed Channels
--------                  ----------------
802.11g (indoor)          1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)          36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 144 149 153
157 161 165
802.11g (outdoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)         52 56 60 64 100 104 108 112 116 132 136 140 144 149 153 157 161 165
802.11g 40MHz (indoor)    1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)    36-40 44-48 52-56 60-64 100-104 108-112 132-136 140-144 149-153 157-
161
802.11g 40MHz (outdoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)   52-56 60-64 100-104 108-112 132-136 140-144 149-153 157-161
802.11a 80MHz (indoor)    36-48 52-64 100-112 132-144 149-161
802.11a 80MHz (outdoor)   52-64 100-112 132-144 149-161
802.11a (DFS)             52 56 60 64 100 104 108 112 116 132 136 140 144

Certificate reg-info for AP-205 Country Code "US"
-------------------------------------------------
PHY Type                  Allowed Channels
--------                  ----------------
802.11g (indoor)          1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)          36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 144 149 153
157 161 165
802.11g (outdoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)         52 56 60 64 100 104 108 112 116 132 136 140 144 149 153 157 161 165
802.11g 40MHz (indoor)    1-5 2-6 3-7 4-8 5-9 6-10 7-11
```

```
802.11a 40MHz (indoor)   36-40 44-48 52-56 60-64 100-104 108-112 132-136 140-144 149-153 157-
161
802.11g 40MHz (outdoor)  1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)  52-56 60-64 100-104 108-112 132-136 140-144 149-153 157-161
802.11a 80MHz (indoor)   36-48 52-64 100-112 132-144 149-161
802.11a 80MHz (outdoor)  52-64 100-112 132-144 149-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140 144

Max EIRP settings for AP-205 Country Code "US"
-----------------------------------------------
Channel  1   2   3   4   5   6   7   8   9   10  11  12  13  14  36  40  44  48  52  56  60
 64   100  104  108  112  116  120  124  128  132  136  140  144  149  153  157  161  165
-------  -   -   -   -   -   -   -   -   -   --  --  --  --  --  --  --  --  --  --  --  --
 --   ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---
b        29  29  29  29  29  29  29  29  29  29  29  *   *   *   *   *   *   *   *   *   *
 *    *    *   *   *   *   *   *   *   *   *   *   *   *   *   *   *   *   *
g/a      32  32  32  32  32  32  32  32  32  32  32  *   *   *   21  21  21  21  28  28  28
 28   28   28  28  28  28   *   *   *   27  27  27  27  33  33  33  33  33
HT 20    32  32  32  32  32  32  32  32  32  32  32  *   *   *   21  21  21  21  27  28  28
 28   28   28  28  28  28   *   *   *   27  27  27  27  33  33  33  33  33
HT 40    32  32  32  32  32  32  32  32  32  32  32  *   *   *   20  20  20  20  24  24  24
 24   24   24  24  24   *   *   *   *   24  24  24  23  32  32  32  32  32
VHT 80   *   *   *   *   *   *   *   *   *   *   *   *   *   *   21  21  21  21  21  21  21
 21   21   21  21  21   *   *   *   *   21  21  21  20  33  33  33  33  33
country  36  36  36  36  36  36  36  36  36  36  36  *   *   *   23  23  23  23  30  30  30
 30   36   36  36  36  36   *   *   *   36  36  36  36  36  36  36  36  36
DFS      *   *   *   *   *   *   *   *   *   *   *   *   *   *   *   *   *   *   FCC FCC FCC
 FCC  FCC  FCC  FCC  FCC  FCC  *   *   *   FCC FCC FCC FCC *   *   *   *   *
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug scan-settings

```
show ap debug scan-settings {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows radio scanning of an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows radio scanning of an AP for specified AP name.
`ip-addr <ip-addr>`	Shows radio scanning of an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows radio scanning of an AP for specified IPv6 address.

Usage Guidelines

This command shows radio scanning of an AP. For the remaining parameters, see the command syntax.

Example

The following example shows radio scanning of an AP named ap-205:

```
(host) [mynode] #show ap debug scan-settings ap-name ap-205

Radios Scan-setting
-------------------
Radio Index  Status
-----------  ------
0            Enable
1            Enable
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug shaping-table

```
show ap debug shaping-table {ap-name <ap-name>|ip-addr <ip-addr>}
```

Description

Show shaping information for clients associated to an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show shaping table information for a specific AP.
`ip-addr <ip-addr>`	Show shaping table information for a specific AP IP address by entering its IP address in dotted-decimal format.

Example

The following command shows the shaping table of an AP named ap22.

```
(host) #show ap debug shaping-table ap-name ap22

VAP station000
pktin   pktout  pktdrop pktqd   cmn[C:O:H]      drop    Numcl   TotCl   BWmgmt
0       0       0       0      0-0-0   0-0     0-0-0   0       0

d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0      0       0       0       0       0

idx     tokens  last-t  in      out     drop    q       tx-t    rx-t    al-t    rate

idx     d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0      0       0       0       0       0       0

VAP station001
pktin   pktout  pktdrop pktqd   cmn[C:O:H]      drop    Numcl   TotCl   BWmgmt
0       8144    0       0      0-0-0   0-0     0-2-0   2       0

d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0      0       0       0       0       0

idx     tokens  last-t  in      out     drop    q       tx-t    rx-t    al-t    rate
1       0       0       0      2966    0       0       716     0       0       0
3       0       0       0      31      0       0       8       0       0       0

idx     d1      d2      d3      d4      d5      d6      d7      d8      d9
0       0       0       0      0       0       0       0       0       0
1       0       0       0      0       0       0       0       0       0
3       0       0       0      0       0       0       0       0       0
```

The output of this command includes the following information:

Column	Description
`pktin`	Number of packets received by the AP.

Column	Description
pktout	Number of packets sent by the AP.
pktdrop	Number of packets dropped by the AP.
pktqd	Number of packets queued.
cmn [C:O:H]	(For internal use only.)
drop	Number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
Numcl	Number of CCK (802.11b) and OFDM (802.11a/g) packets dropped.
TotCl	Total number of clients associated with the AP
Bwmgmt	This data column displays a 1 if the bandwidth management feature has been enabled. Otherwise, it displays a 0.
d<n>	(For internal use only.)
idx	Association ID.
tokens	This value represents the credits the station has to transmit tokens.
last-t	Number of tokens that were allocated to the station last time token allocation algorithm ran.
in	Number of packets received.
out	Number of packets sent.
drop	Number of dropped packets.
q	Number of queued packets
tx-t	Total time spent transmitting data.
rx-t	Total time spent receiving data.
al-t	Total time allocated for transmitting data to this station.
rate	(For internal use only.)

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug spanning-tree

```
show ap debug spanning-tree {ap-group <ap-group>|ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show an AP's spanning tree statistics.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show log information for an AP with a specific name.
`bssid <bssid>`	Show log information for a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show log information for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show log information for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Example

The following command shows the AP debug spanning tree state.

```
(host) [mynode] #show ap debug spanning-tree
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug sta-msg-stats

```
show ap debug sta-msg-stats {[ap-name <ap-name>] [bssid <bssid>]}
```

Description

This command shows AP-STM to STM message statistics.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AP-STM to STM message statistics for specified AP name.
`bssid <bssid>`	Shows AP-STM to STM message statistics for specified BSSID.

Usage Guidelines

This command shows AP-STM to STM message statistics. For the remaining parameters, see the command syntax.

Example

The following example shows AP-STM to STM message statistics for BSSID d8:c7:c8:38:fc:f5:

```
(host) [mynode] #show ap debug sta-msg-stats bssid d8:c7:c8:38:fc:f5

STA Up/Down Message Counters for BSSID d8:c7:c8:38:fc:f5
-------------------------------------------------------
Name                                                Value
----                                                -----
STA Messages: Up Down                               0 0
Dup Seqnum                                          0
Success: Assoc Re-Assoc                             0 0
STA Not found Errors                                UP: 0 DN 0
Assoc Rejections: Total BLIST CAC VLAN AID ALLOC FT  0 0 0 0 0 0 0
Dormant Clear Skipped                               0

STA Up/Down Message Counters
----------------------------
Num Messages Received                                                    0
---------------------                                                    -
Messages Received per slot                                               0 0 0
STA Messages: Up Down Total                                              0 0 0
Success: Assoc Re-Assoc AcksSent                                         0 0 0
Unpack Errors                                                            0
Not found Errors: sta sap; sta_alloc                                     UP: 0 0 DN: 0 0;
alloc_err=0
Duplicate Sequence Num, Auth Busy Drops                                  0, 0
Assoc Rejections: Total UAC BLIST CAC VLAN AID ALLOC FT TIME CTRMSR SCTRMSR  0 0 0 0 0 0 0 0 0 0
0 0
```

Command History:

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap debug stm-trace

```
show ap debug stm-trace
```

Description

This command shows the debug trace settings for STM.

Syntax

No parameters.

Usage Guidelines

This command shows the debug trace settings for STM.

Example

The following example shows the debug trace settings for STM:

```
(host) [mynode] #show ap debug stm-trace

STM Debug tracing: Categories=All; loglevel=INFO; mac_filter=not set; ip_filter=not set
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap debug switching

```
show ap debug switching {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show an AP's switching statistics.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the Access Point.
`ip-addr <ip-addr>`	IP address of the Access Point.
`ip6-addr <ip6-addr>`	IPv6 address of the Access Point.

Example

The following command shows the .....

```
(host) #show ap debug switching
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug system-status

```
show ap debug system-status
   ap-name <ap-name>
   bssid <bssid>
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
```

Description

Show detailed system status information for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show system status data for an AP with a specific name.
`bssid <bssid>`	Show system status data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show system status data for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Usage Guidelines

Issue this command under the guidance of Aruba technical support to troubleshoot network issues. The output of this command displays the following types of information (if it exists) for the selected AP:

■ Bootstrap information	■ Per-radio statistics	■ Ethernet duplex/speed settings
■ Descriptor Usage	■ Encryption statistics	■ Tunnel heartbeat stats
■ Interface counters	■ AP uptime	■ Boot version
■ MTU discovery	■ Memory usage	■ LMS information
■ ARP cache	■ Kernel slab statistics	■ Power status
■ Route table	■ Interrupts	■ CPU type
■ Interface Information	■ Crash Information	■ CPU usage statistics
■ System Status Script	■ Radio profile name	■ Dual 5 GHz mode

Power Status

The following lines under power status indicate the power status of the AP:

- **Operational State** indicates the current state of the AP, that is, as seen with the power light on the AP. **Operational State** may be different from **Current HW State** as a result of LLDP negotiation.
- **Current HW State** indicates the result from POE negotiation in hardware.
- **LLDP Negotiated POE Power** indicates the LLDP negotiated power.

The following parameters are included in the output of this command, and can help troubleshoot problems on an AP or wireless network.

Parameter	Description
The **Failed** column in the **Descriptor Usage** section	This parameter can tell you if the AP is dropping packets.
Interface Information table	This parameter can tell you if the Ethernet network is working properly. This table should not show an excessive number of errors.
AP Uptime table	Low values in this table can indicate problems with the wired network, or with the AP itself.
Tunnel Heartbeat table	This table can indicate the health of the underlying wired network.
Rebootstrap Information table /**Reboot Information** table	A large number of reboots can mean that the AP has hardware problems.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug trace-addr

```
show ap debug trace-addr
```

Description

Show MAC addresses in the trace buffer.

Usage Guidelines

Use this command to troubleshoot wireless clients that are being traced for 802.11 communication

Examples

The output of the command shows the **Trace List** table. If no wireless clients are being traced, this table will be empty.

```
(host) #show ap debug trace-addr

Trace List
----------
MAC Address
-----------
00:1a:1e:c5:ca:b4
00:1a:1e:c5:d6:46
00:1a:1e:c5:d7:40
00:1a:1e:c5:d7:64
00:1a:1e:c5:d9:56
```

00:1a:1e:c5:d9:b0

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap debug tunnel-id

```
show ap debug tunnel-id
```

Description

This command shows all tunnel IDs stored in STM.

Syntax

No parameters.

Usage Guidelines

This command shows all tunnel IDs stored in STM.

Example

The following example shows all tunnel IDs stored in STM:

```
(host) [mynode] #show ap debug tunnel-id

List of Tunnel id
-----------------
Hash Table  Tunnel id  IP Address
----------  ---------  ----------
SAP Hash    65548      10.15.147.180
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap debug usb

```
show ap debug usb
   ap-name <ap-name>
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
```

Description

This command displays the USB information provisioned on the RAP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show system status data for an AP with a specific name.
`ip-addr <ip-addr>`	Show system status data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show system status data for an AP with a specific IPv6 address by entering an IPv6 address in dotted-decimal format.

Usage Guidelines

Use this command to view the USB information provisioned on the RAP.

Examples

The output of the command shows the USB information provisioned on the RAP.

```
(host) #show ap debug usb ap-name RAP2
USB Information
---------------
Parameter                   Value
---------                   -----
Manufacturer                 Pantech,
Product                      PANTECH
Serial Number
Driver                       ptuml_cdc_ether
Vendor ID                    106c
Product ID                   3718
USB Modem State              Active
USB Uplink RSSI(in dBm)      -73
Supported Network Services   CDMA GSM LTE
Firmware Version             L0290VWB522F.242
ESN Number                   990000472325325
Current Network Service      4G-LTE
```

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap deploy-profile

```
show ap deploy-profile
```

Description

This command displays if the AP deploy profile is enabled or not. It also displays if the policy is applied on default AP group, status of the blacklist policy and the complete list of IPv4 and IPv6 address ranges to which the AP deployment policy is applied.

Syntax

None.

Example

The following command displays the status of the AP deploy profile and various configurations applied on the profile:

```
(host) [mynode] #show ap deploy-profile

Profile enabled: no
Apply to default ap group: no
Blacklist enabled: yes

AP deploy policy IP range Table
-------------------------------
Starting IP  Ending IP
-----------  ---------
1.1.1.1      1.1.1.10

AP deploy policy IPv6 range Table
---------------------------------
Starting IP  Ending IP
-----------  ---------
::3          ::5
2016::1      2016::10
2016::15     2016::15
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap details

```
show ap details [advanced] {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>|wired-mac
<wired-mac>}
```

Description

This command shows the detailed provisioning parameters, hardware, and operating information for a specific AP.

Syntax

Parameter	Description
`advanced`	Shows additional information of specified AP. Include the following additional data in the output of this command: ■ Switch message counts ■ AP group information ■ Virtual AP operating information
`ap-name <ap-name>`	Show data for a specific AP by entering the name of the AP for which you want to display information.
`ip-addr <ip-addr>`	Show data for an AP with the specified IP address.
`ip6-addr <ip6-addr>`	Show data for an AP with the specified IPv6 address.
`wired-mac <wired-mac>`	Show mac address of an AP.

Usage Guidelines

This command shows the detailed provisioning parameters, hardware, and operating information for a specific AP. For the remaining parameters, see the command syntax.

Examples

The following example shows part of the output for the command **show ap details ap-name <ap-name>**.

```
(host) [mynode] #show ap details ap-name ap-205

AP "ap-205" Basic Information
-----------------------------
Item            Value
----            -----
AP IP Address   191.191.191.252
LMS IP Address  192.192.189.1
Group           default
Location Name   N/A
Status          Up
Up time         19d:13h:30m:19s

AP "ap-205" Hardware Information
--------------------------------
Item                Value
----                -----
AP Type             205
Serial #            CM0487514
Wired MAC Address   40:e3:d6:cf:61:96
Radio 0 BSSID       40:e3:d6:76:19:70
Radio 1 BSSID       40:e3:d6:76:19:60
Enet 1 MAC Address  N/A
Enet 2 MAC Address  N/A
Enet 3 MAC Address  N/A
Enet 4 MAC Address  N/A
```

```
Enet 5 MAC Address  N/A
Enet 6 MAC Address  N/A
Enet 7 MAC Address  N/A
```

Starting from ArubaOS 8.3.0.0, this command displays the new statistics on AP recovery mode:

```
(host)[node] #show ap details ap-name <ap-name>
AP "<ap-name>" Radio 0 Operating Information
----------------------------------------
Item                  Value    Source
----                  -----    ------
Very High throughput  Enabled  Configuration
High throughput       Enabled  Configuration
Mode                  AP       Configuration
Band                  802.11a
Primary Channel       36       Configuration
80MHz Channel Group   36-48    Configuration
EIRP                  10.0     Configuration
Fast recovery start  2017-03-09 11:57:56
Fast recovery end    2017-03-09 11:58:00
Fast recovery         1
```

The output of this command includes the following information:

Column	Description
AP IP Address	IP address of the AP
LMS IP Address	The IP address of the local management switch (LMS)—the Aruba controller which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network.
Group	Name of the AP's AP group.
Location Name	Location of the AP.
Status	Current status of the AP, either **Up** or **Down**.
Up time	Number of hours, minutes and seconds since the last controller reboot or bootstrap, in the format *hours:minutes:seconds*.
AP Type	AP model
Serial #	Serial number for the AP
Wired MAC address	MAC address of the wired interface.
Radio 0 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 0. This is usually the radio's MAC address.
Radio 1 BSSID	Basic Service Set Identifier (BSSID) of the AP's radio 1. This is usually the radio's MAC address.
Enet 1 MAC address	MAC address of the Ethernet1 port of AP.
Enet 3 MAC address	MAC address of the Ethernet3 port of AP.
Enet 4 MAC address	MAC address of the Ethernet4 port of AP.
Enet 5 MAC address	MAC address of the Ethernet5 port of AP.

Column	Description
`Enet 6 MAC address`	MAC address of the Ethernet6 port of AP.
`Enet 7 MAC address`	MAC address of the Ethernet7 port of AP.
`Fast recovery start`	Start date and time of the AP Fast Recovery process.
`Fast recovery end`	End date and time of the AP Fast Recovery process.
`Fast Recovery`	Number of Fast Recoveries that happened in the AP.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.3.0.0	Additional statistics on AP Fast Recovery was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap enet-link-profile

```
show ap enet-link-profile [<profile>]
```

Description

Show a list of all Ethernet Link profiles.

Usage Guidelines

Include a profile name to display details for the specified Ethernet Link Profile, or omit the <profile> parameter to display a list of all Ethernet Link profiles.

Example

This command shows the speed of the Ethernet interface and the current duplex mode for the Ethernet Link profile “default”:

```
(host) [mynode] #show ap enet-link-profile default

AP Ethernet Link profile "default"
----------------------------------
Parameter  Value
---------  -----
Speed                auto
Duplex               auto
802.3az (EEE)        Disabled
802.3bz              Yes
Power over Ethernet  Disabled
```

The output of this command includes the following parameters:

Parameter	Description
Speed	The speed of the Ethernet interface. This value can be either **10 Mbps**, **100 Mbps**, **1000Mbps** (1 Gbps), or **auto** (auto-negotiated).
Duplex	The duplex mode of the AP’s Ethernet interface. This value can be either **full**, **half**, or **auto** (auto-negotiated).
802.3az	This displays if the support for the 802.3az Energy Efficient Ethernet (EEE) standard is enabled.
802.3bz	This displays if the support for IEEE 802.3bz standard is enabled.
Power Over Ethernet	This displays if the physical port is Power over Ethernet (PoE) enabled.

Related Commands

Command	Description	Mode
ap enet-link-profile	This command configures an AP Ethernet link profile.	Config mode

Command History

Version	Modification
ArubaOS 8.3.0.0	A new row 802.3bz displays if the standard is enabled or disabled for an AP.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap essid

```
show ap essid
```

Description

Show a Extended Service Set Identifier (ESSID) summary for the controller, including the numbers of APs and clients associated with each ESSID.

Examples

The output of the command in the example below shows statistics for four configured ESSIDs.

```
(host) [mynode] #show ap essid
ESSID Summary
-------------
ESSID             APs  Clients  VLAN(s)  Encryption
-----             ---  -------  -------  ----------
vocera  21   0         66       WPA2 PSK AES
voip    23   52        66,64    WPA2 8021X AES
guest             49   6        63       Open
wpa2    26   88        65,64    WPA2 8021X AES
Num ESSID:4
```

The output of this command includes the following information:

Column	Description
ESSID	An Extended Service Set Identifier (ESSID) is the identifying name of an 802.11 wireless network.
APs	Number of APs associated with the ESSID.
VLAN(s)	VLAN IDs of the VLANs for the ESSID.
Encryption	The layer-2 authentication and encryption used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap general-profile

```
show ap general-profile
```

Description

This command shows the general profile of an AP.

Syntax

No parameters.

Usage Guidelines

This command shows the general profile of an AP.

Example

The following example shows the general profile of an AP:

```
(host) [mynode] #show ap general-profile

ap general-profile
------------------
Parameter                                                 Value      Set
---------                                                 -----      ---
Enable AP State Periodic Sync                             Enabled
AP State sync interval in minutes (5 - 1440 mins(24 hours))  5 minutes
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap global acl-table

```
show ap global acl-table
```

Description

This command shows the ACL table of STM.

Syntax

No parameters.

Usage Guidelines

This command shows the ACL table of STM.

Example

The following example shows the ACL table of STM:

```
(host) [mynode] #show ap global acl-table

STM ACL Table
-------------
ACL  Type     ACE Index  Ace Count  Name
---  ----     ---------  ---------  ----
1    session  7680       1          global-sacl
2    role     8132       33         logon
3    session  7863       12         validuser
4    session  7680       1          sdn-acl
5    session  7684       1          uplink-lb-cfg-racl
6    session  7685       1          uplink-lb-sys-racl
7    role     7909       12         guest
8    session  7680       1          apprf-guest-sacl
9    role     7921       35         ap-role
10   role     7680       1          stateful-dot1x
11   session  7680       1          apprf-stateful-dot1x-sacl
12   role     8104       28         guest-logon
13   role     8892       37         sys-ap-role
14   session  7686       20         sys-control
15   session  8874       18         sys-ap-acl
16   session  8167       3          stateful-dot1x
17   session  7821       4          ap-uplink-acl
18   session  7724       1          master-boc-traffic
19   session  7680       1          name
20   session  7725       2          validuserethacl
21   session  7680       1          name2
22   session  7727       2          etherypte
23   session  7729       3          wificalling-block
24   session  7732       11         v6-control
25   session  7743       2          dns-acl
26   session  7745       3          svp-acl
27   session  7748       2          v6-http-acl
28   session  7750       2          srcnat
29   session  7680       1          apprf-authenticated-sacl
30   session  7680       1          voip-applications-acl
31   session  7752       5          allow-diskservices
32   session  7757       2          dhcp-acl
33   session  7759       6          vpnlogon
34   session  7765       2          v6-icmp-acl
35   session  7767       2          wificalling-acl
36   session  7769       2          tftp-acl
```

```
37   session  8097       7          captiveportal
38   session  7778       6          vmware-acl
39   session  7784       3          skype4b-acl
40   session  7787       7          ap-acl
41   session  7794       2          v6-allowall
42   session  7680       1          apprf-default-via-role-sacl
43   session  7796       3          jabber-acl
44   session  7680       1          apprf-default-vpn-role-sacl
45   session  7799       12         control
46   session  7811       8          logon-control
47   session  7819       2          v6-dns-acl
48   session  7825       2          noe-acl
49   session  7827       2          v6-https-acl
50   session  7829       7          v6-ap-acl
51   session  7680       1          apprf-voice-sacl
52   session  7836       2          https-acl
53   session  7838       2          skinny-acl
54   session  7840       2          vocera-acl
55   session  7842       2          http-acl
56   session  7844       7          captiveportal6
57   session  7851       4          allow-printservices
58   session  7855       2          ra-guard
59   session  7857       3          citrix-acl
60   session  7860       3          allowall
61   session  8165       2          cplogout
62   session  7877       3          sip-acl
63   session  7880       8          v6-logon-control
64   session  7888       2          icmp-acl
65   session  7890       2          v6-dhcp-acl
66   session  7892       3          h323-acl
67   role     7895       4          default-via-role
68   role     7899       5          default-vpn-role
69   role     7904       5          authenticated
70   role     8075       22         voice
```

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap ht-rates

```
show ap ht-rates bssid <bssid>
```

Description

Show high-throughput rate information for a basic service set (BSS).

Syntax

Parameter	Description
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.

Examples

The output of this command shows high-throughput rates for each supported MCS value. These values are applicable to high-throughput (802.11n-capable) APs only.

```
(host) [mynode] #show ap ht-rates bssid 00:1a:1e:1e:5a:10

AP "AL12" Radio 0 BSSID 00:1a:1e:1e:5a:10 High-throughput Rates (Mbps)
-----------------------------------------------------------------------
MCS  Streams  20 MHz  40 MHz  40 MHz SGI
---  -------  ------  ------  ----------
  0    1         6.5    13.5    15.0
  1    1        13.0    27.0    30.0
  2    1        19.5    40.5    45.0
  3    1        26.0    54.0    60.0
  4    1        39.0    81.0    90.0
  5    1        52.0   108.0   120.0
  6    1        58.5   121.5   135.0
  7    1        65.0   135.0   150.0
  8    2        13.0    27.0    30.0
  9    2        26.0    54.0    60.0
 10    2        39.0    81.0    90.0
 11    2        52.0   108.0   120.0
 12    2        78.0   162.0   180.0
 13    2       104.0   216.0   240.0
 14    2       117.0   243.0   270.0
 15    2       130.0   270.0   300.0
```

The output of this command includes the following information:

Column	Description
`MCS`	A Modulation Coding Scheme (MCS) values supported on this high-throughput SSID.
`Streams`	Number of spatial streams used by the MCS index value.
`20 MHz`	802.11n data rates for the MCS for 20 Mhz transmissions.
`40 MHz`	802.11n data rates for the MCS for 40 Mhz transmissions.
`40 MHz SGI`	802.11n data rates for the MCS for 40 Mhz transmissions using a short guard interval.

Related Commands

Command	Description
show ap vht-rates	Show very-high-throughput rate information for a basic service set (BSS).

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap image-preload status

```
show ap image-preload status
   all
   list
   summary
```

Description

Display the list of APs that will preload a new version of software from a controller with the AP preload feature activated.

Syntax

Parameter	Description
`all`	Display the complete status of AP image preload operation.
`list`	Displays the list of APs and their image preload statuses.
`summary`	Summarizes the status of AP image preload operation.

Usage Guidelines

Issue this command to display a list of APs in the AP image preload list, and monitor the download status of each AP.

Example

The example below shows the current status of APs downloading a new image using the AP image preload feature.

```
(host) #show ap image-preload status all

AP Image Preload Parameters
---------------------------
Item                         Value
----                         -----
Status                       Active
Mode                         All APs
Partition                    0
Build                        40740
Max Simultaneous Downloads   512
Start Time                   2013-11-05 15:38:50

AP Image Preload AP Status Summary
----------------------------------
AP Image Preload State  Count
----------------------  -----
Preloaded               1
TOTAL                   1

AP Image Preload AP Status
--------------------------
AP Name             AP Group    AP IP       AP Type Preload State   Start Time           End
Time             Failure Count Failure Reason
-------             --------    -----       ------- -------------   ----------           -----
---             ------------- --------------
```

```
6c:f3:7f:c3:a6:56   SecureJack  10.3.90.14  135      Preloaded      2013-11-05 15:38:50  2013-
11-05 15:39:58  0
```

(host) #show ap image-preload status list

```
AP Image Preload AP Status
--------------------------
AP Name            AP Group    AP IP       AP Type  Preload State  Start Time           End
Time             Failure Count  Failure Reason
-------            --------    -----       -------  -------------  ----------           ------
--             -------------  --------------
6c:f3:7f:c3:a6:56  SecureJack  10.3.90.14  135      Preloaded      2013-11-05 15:38:50  2013-
11-05 15:39:58  0
```

(host) #show ap image-preload status summary

```
AP Image Preload Parameters
---------------------------
Item                        Value
----                        -----
Status                      Active
Mode                        All APs
Partition                   0
Build                       40740
Max Simultaneous Downloads  512
Start Time                  2013-11-05 15:38:50
AP Image Preload AP Status Summary
----------------------------------
AP Image Preload State  Count
----------------------  -----
Preloaded               1
TOTAL                   1
```

The output of this command includes the following information:

Column	Description
`AP Image Preload Parameters`	Shows if this feature has been enabled (has an active status) or is disabled (has an inactive status).
`AP Image Preload AP Status Summary`	These two columns list the different possible preload states for APs eligible to preload a new software image, and the total number of APs in each state. ■ **Preloaded**: Number of APs that have finished preloaded a new software image. ■ **Preloading**: Number of APs that are currently downloading the new image. ■ **Waiting**: Number of APs that are waiting to start preloading the new image from the controller.
`AP Image Preload AP Status`	This section displays the following details for each preload attempt.
`AP Name`	Name of an AP eligible to preload a new software image.
`AP Group`	AP group of an AP eligible to preload a new software image.

Column	Description
AP IP	IP address of the AP.
AP Type	AP model type.
Preload State	Current state of the AP's preload attempt ■ **Preloaded**: The AP is finished preloading a new software image. ■ **Preloading**: The AP is currently downloading the new image. ■ **Waiting**: The AP is waiting to start preloading the new image from the controller.
Start Time	Time the AP starting preloading an image.
End Time	Time the AP completed the image preload.
Failure Count	Number of times that the AP failed to preload the new image.
Failure Reason	In the event of an image preload failure, this column will display the reason that the image download failed.

Related Commands

show ap image version

Command History

Release	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master or managed devices

show ap image version

```
show ap image version [ap-name <ap-name>|ip-addr <ip-addr>]
```

Description

Display an AP's image version information.

Syntax

Parameter	Description
`ap-name <ap-name>`	View image version information for an AP with a specific name.
`ip-addr <ip-addr>`	View image version information for an AP with a specific IP address. Enter the address of the AP in dotted-decimal format.

Usage Guidelines

By default, this command displays image version information for all APs associated with the controller. To view image version information for a single AP, specify an AP using the **ap-name** or **ip-addr** parameters

Example

The output in the example below shows the current running image version as well as the image version stored in the controller's flash memory.

```
(host) [mynode] #show ap image version ip-addr 192.0.2.45
Access Points Image Version
---------------------------
AP                              Running Image Version String
--                              ----------------------------
192.0.2.45                      6.4.0.0 Wed Nov 27 10:46:42 PDT 2013

Flash Image Version String            Matches    Num Matches
--------------------------            -------    -----------
6.4.0.0 Wed Nov 27 10:46:42 PDT 2013  Yes        3

Num Mismatches    Bad Checksums    Image Load Status
--------------    -------------    -----------------
0                                  Done
```

The output of this command includes the following information:

Column	Description
`AP`	Name or IP address of an AP
`Running Image Version String`	String identifying the number of the image version currently running on the AP, as well as the date on which that version was created.
`Flash Image Version String`	String identifying the number of the image version in the AP's flash memory, as well as the date on which that version was created.
`Matches`	If **yes**, the running image version matches the image version currently in the AP's flash memory. If **no**, the two image versions do not match.

Column	Description
`Num Matches`	Number of times the running image version matched the flash image version after a reboot.
`Num Mismatches`	Number of times the running image version did not match the flash image version after a reboot. If the images do not match, the AP will upgrade to the flash image.
`Bad Checksums`	Number of bad checksum calculations due to an invalid or corrupted image file.
`Image Load Status`	Current status of the AP following an upgrade. **Done**: This status indicates that the controller reset after the upgrade was performed, or the upgrade was performed after the AP first registered with the controller. **Completed**: The AP was updated after it was registered to the controller, and after the controller's last reset. If AP shows a status of **completed**, it will also display the time it took it update that AP. **In progress:** The AP is currently updating its image.

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap ip health-check

```
show ap ip health-check {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows health of an access point.

Syntax

Parameter	Description	Range	Default
`ap-name <ap-name>`	Shows health of an access point specified by AP name.	–	–
`ip-addr <ip-addr>`	Shows health of an access point specified by IP address.	–	–
`ip6-addr <ip6-addr>`	Shows health of an access point specified by IPv6 address.	–	–

Usage Guidelines

This command shows health of an access point. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to show health of an access point with IP address 192.0.2.1:

```
(host) [mynode] #sho ap ip health-check ip-addr 192.0.2.1

AP Health-Check Status
----------------------
Interval  Probe IP  Avg RTT(in ms)  Total_TX_Probes  Total_RX_Probes  Total_Packet Loss
--------  --------  --------------  ---------------  ---------------  -----------------
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap-lacp-striping-ip

```
show ap-lacp-striping-ip
```

Description

Profile to enable/disable AP LACP feature and to specify GRE striping IP to LMS IP mapping.

Syntax

No parameters

Usage Guidelines

Example

```
(host) [mynode] #show ap-lacp-striping-ip
AP LACP LMS map information
---------------------------
Parameter            Value
---------            -----
AP LACP Striping IP  Enabled
GRE Striping IP      2.2.2.2 LMS 3.3.3.3
GRE Striping IP      4.4.4.4 LMS 5.5.5.5
GRE Striping IP      10.65.30.50 LMS 10.65.30.60
```

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap license-usage

```
show ap license-usage
```

Description

Show AP license usage information.

Examples

The output of the command below shows that controller has 13 associated campus APs using licenses, with 3 unused campus AP licenses remaining.

```
(host) [mynode] #show ap license-usage

AP Licenses
-----------
Type                        Number
----                        ------
AP Licenses                 512
MM Licenses                 500
MC-VA Licenses              0
Controller License          True
Overall AP License Limit    0
AP Usage [Note: THIS CONTROLLER DOES NOT TERMINATE ANY AP]
-----------------------------------------------------------
Type              Count
----              -----
Active CAPs       0
Active RAPs       0
Remote-node APs   0
Tunneled nodes    0
Total APs         0
Remaining AP Capacity
---------------------
Type  Number
----  ------
CAPs  0
RAPs  0
```

The output of this command includes the following information:

Parameter	Description
AP Licenses	Number of AP licenses currently available on the managed device.
RF Protect Licenses	Number of RF Protect licenses currently available on the managed device.
PEF Licenses	Number of Policy Enforcement Firewall (PEF) licenses currently available on the managed device.
Overall AP Licenses	Total number of APs supported by licenses on the managed device.
CAPs	Number of campus APs currently using a license on the managed device.
RAPs	Number of remote APs currently using a license on the managed device.
Remote-Node APs	Number of APs currently using a license on the managed device.

Parameter	Description
`Tunneled Nodes`	Number of tunneled nodes currently using a license on the managed device.
`CAPs`	Number of unused campus APs licenses remaining on the managed device.
`RAPs`	Number of unused remote APs licenses remaining on the managed device.

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap lldp

```
show ap lldp [<profile>]
```

Description

Display a list of LLDP-MED Network Policy profiles, or display the current configuration settings of an individual profile.

Syntax

Parameter	Description
`<profile>`	Specify a LLDP profile name to view configuration settings for that profile.

Examples

The following example lists all LLDP profile profiles. The References column lists the number of other profiles with references to that LLDP-MED Network policy profile profile, and the ProfileStatus column indicates whether the profile is predefined.

The output of the command below shows that the controller has two LLDP profiles.

```
(host) #show ap lldp med-network-policy-profile
AP LLDP Profile List
---------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
video    2
Total:2
```

The following command displays configuration details for the LLDP profile named default.

```
(host) [mynode] #show ap lldp med-network-policy-profile video
AP LLDP Profile "new"
---------------------
Parameter                       Value
---------                       -----
PDU transmission                Enabled
Reception of LLDP PDUs          Enabled
Transmit interval (seconds)     30
Transmit hold multiplier        4
Optional TLVs                   port-description system-description system-name capabilities
management-address
802.1 TLVs                      port-vlan vlan-name
802.3 TLVs                      mac link-aggregation mfs power
LLDP-MED TLVs
LLDP-MED network policy profile  N/A
```

The output of this command includes the following information:

Parameter	Description
PDU transmission	Shows if LLDP PDU transmission is enabled on the AP.
Reception of LLDP PDUs	Shows if LLDP PDU reception is enabled on the AP.
Transmit interval (seconds)	The interval between LLDP TLV transmission seconds. The supported range is 1-3600 seconds and the default value is 30 seconds.
Transmit hold multiplier	This value is multiplied by the transmit interval to determine the number of seconds to cache learned LLDP information before that information is cleared. If the transmit-hold value is at the default value of 4, and the transmit interval is at its default value of 30 seconds, then learned LLDP information will be cached for 4 x 30 seconds, or 120 seconds.
Optional TLVs	The AP sends the listed optional TLVs in LLDP PDUs.
802.1 TLVs	The AP sends the listed 802.1 TLVs in LLDP PDUs. By default, the AP will send all 802.1 TLVs.
802.3 TLVs	The AP sends the listed 802.3 TLVs in LLDP PDUs. By default, the AP will send all 802.3 TLVs.
LLDP-MED TLVs	Lists the LLDP-MED TLVs the AP will send in LLDP PDUs. By default, the AP will not send any LLDP-MED TLVs
LLDP-MED network policy profile	Specifies the LLDP MED Network Policy profile to be associated with this LLDP profile.

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap lldp counters

```
show ap lldp counters
   ap-name  <ap-name>
   ip-addr <ip-addr>
   ip6-addr (ipv6-addr>
```

Description

Show LLDP counters for a specific AP, or all APs sending or receiving LLDP Protocol Data Units (PDUs).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show counter statistics for an AP with a specific name.
`ip-addr <ip-addr>`	View counter statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.
`ip6-addr <ip-addr>`	View counter statistics for an AP with a specific IPv6 address.

Examples

The output of the command below shows LLDP counter information for two interfaces.

```
(host) [mynode] #show ap lldp counters
AP LLDP Counters (Updated every 60 seconds)
-------------------------------------------
AP                Interface  Received  Unknown TLVs  Malformed  Overflow  Transmitted
--                ---------  --------  ------------  ---------  --------  -----------
00:1a:1e:ce:fb:bf  bond0      0         0             0          0         68159
00:24:6c:c0:00:86  bond0      0         0             0          0         68153
```

The output of this command includes the following information:

Parameter	Description
`AP`	Name of the AP sending or receiving LLDP PDUs.
`Interface`	Name of the AP interface sending or re ce vi ng LLDP PDUs.
`Received`	Number of packets received on the specified interface.
`Unknown TLVs`	Number of LLDP Protocol Data Units (PDUs) with an unknown type-length-value (TLV).
`Number of Malformed packets`	Number of malformed packets received on that interface
`Overflow`	Number of times that an LLDP neighbor could not be added to the neighbor table (there is a limit of 8 per port)
`Transmitted`	Number of packets transmitted from that interface

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap lldp med-network-policy-profile

```
show ap lldp med-network-policy-profile [<profile>]
```

Description

Display a list of LLDP-MED Network Policy profiles, or display the current configuration settings of an individual profile.

Syntax

Parameter	Description
<profile>	Specify a LLDP-MED Network Policy profile name to view configuration settings for that profile.

Usage Guidelines

The LLDP-MED Network policy profile allows you to configure an extension to LLDP that supports interoperability between VoIP devices and other networking clients. LLDP-MED network policy discovery lets end-points and network devices advertise their VLAN IDs (e.g. voice VLAN), priority levels, and DSCP values.allows you to define a set of provisioning parameters to an AP group.

Issue this command without the **<profile-name>** option to display the entire LLDP-MED Network policy profile list, including profile status and the number of references to each profile. Include a profile name to display the configuration settings for that profile.

Examples

The following example lists all LLDP-MED Network policy profile profiles. The **References** column lists the number of other profiles with references to that LLDP-MED Network policy profile, and the **ProfileStatus** column indicates whether the profile is predefined.

The output of the command below shows that the controller has three LLDP-MED network profiles.

```
(host) [mynode] #show ap lldp med-network-policy-profile

AP LLDP-MED Network Policy Profile List
---------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
video    2
voice    1
Total:2
The following command displays configuration details for the LLDP-MED Network Policy profile
named video.

(host) #show ap lldp med-network-policy-profile video
AP LLDP-MED Network Policy Profile "default"
--------------------------------------------
Parameter                                          Value
---------                                          -----
LLDP-MED application type                          streaming-video
LLDP-MED application VLAN                          16
LLDP-MED application VLAN tagging                  Tagged
LLDP-MED application Layer-2 priority              0
LLDP-MED application Differentiated Services Code Point  0
```

The output of this command includes the following information:

Parameter	Description
`LLDP-MED application type`	Type of application that this profile manages. This profile supports the following options: ■ **guest-voice** : The AP services a separate voice network for guest users and visitors. ■ **guest-voice-signaling** : The AP is part of a network that requires a different policy for guest voice signaling than for guest voice media. Do not use this application type if both the same network policies apply to both guest voice and guest voice signaling traffic. ■ **softphone-voice** : The AP supports voice services using softphone software applications on devices such as PCs or laptops. ■ **streaming-video** : T The AP supports broadcast or multicast video or other streaming video services that require specific network policy treatment. This application type is not recommended for video applications that rely on TCP with buffering. ■ **video-conferencing** : T The AP supports video conferencing equipment that provides real-time, interactive video/audio services. ■ **video-signaling** : T The AP is part of a network that requires a different policy for video signaling than for the video media. Do not use this application type if both the same network policies apply to both video and video signaling traffic. ■ **voice** : T he AP services IP telephones and other appliances that support interactive voice services. This is the default application type. ■ **voice-signaling** : T The AP is part of a network that requires a different policy for voice signaling than for the voice media. Do not use this application type if both the same network policies apply to both voice and voice signaling traffic.

Parameter	Description
`LLDP-MED application VLAN`	Indicates the VLAN ID (0-4094) or VLAN name of the VLAN used by the application.
`LLDP-MED application VLAN tagging`	Indicates if the policy applies to a to a VLAN that is tagged with a VLAN ID or untagged. The default value is untagged. **NOTE:** When an LLDP-MED network policy is defined for use with an untagged VLAN, then the L2 priority field is ignored and only the DSCP value is used.
`LLDP-MED application Layer-2 priority`	Displays a configured 802.1p priority level for the specified application type, where 0 is the lowest priority level and 7 is the highest priority.
`LLDP-MED application Differentiated Services Code Point`	Displays a configured Differentiated Services Code Point (DSCP) priority value for the specified application type, where 0 is the lowest priority level and 63 is the highest priority.

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap lldp neighbors

```
show ap lldp neighbors
   ap-name  <ap-name>
   ip-addr <ip-addr>
   ip6-addr (ipv6-addr>
```

Description

Show LLDP neighbors for a specific AP, or all APs sending or receiving LLDP Protocol Data Units (PDUs).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show LLDP neighbor statistics for an AP with a specific name.
`ip-addr <ip-addr>`	View LLDP neighbor statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.
`ip6-addr <ip-addr>`	View LLDP neighbor statistics for an AP with a specific IPv6 address.

Usage Guidelines

The LLDP protocol allows switches, routers, and WLAN access points to advertise information about themselves such as identity, capabilities, and neighbors to other nodes on the network. Use this command to display information about the AP's LLDP peers.

By default, this command displays LLDP neighbors for the entire list of LLDP interfaces. Include a the name of IP address of an AP to display neighbor information only for that one device.

Examples

The output of the command below shows the LLDP neighbor list for an AP named **ap12**.

```
(host) [mynode] #show ap lldp neighbors ap-name ap12
AP LLDP Neighbors (Updated every 60 seconds)
-------------------------------------------
AP  Interface  Neighbor  Chassis Name/ID    Port Name/ID  Mgmt. Address  Capabilities
--  ---------  --------  ---------------    ------------  -------------  ------------
uc  bond0      0         d8:c7:c8:c4:4f:4e  bond0         10.3.44.193
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
```

The output of this command includes the following information:

Parameter	Description
`AP`	Name of the LLDP neighbor
`Interface`	Interface on the AP sending or receiving LLDP PDUs.
`Neighbor`	LLDP neighbor number
`Chassis Name/ID`	The name of the LLDP neighbor AP
`Port Name/ID`	Port name or ID if the interface sending LLDP PDUs.

Parameter	Description
`Mgmt. Address`	Management address of the LLDP neighbor
`Capabilities`	This data column can list any of the following data codes to indicate LLDP neighbor capabilities. ■ R: Router ■ B: Bridge ■ A: Access Point ■ P: Phone ■ O: Other

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap load-balancing

```
show ap load balancing
```

Description

Show the load-balancing information for each AP with load balancing enabled.

Examples

The output of the command in the example below shows details for a single AP enabled with the load-balancing feature.

```
(host) [mynode] #show ap load-balancing
Load Balance Enabled Access Point Table
---------------------------------------
bss               ess           name    s/p  ip             phy   chan  cur-cl  util(kbps)
---               ---           ----    ---  --             ---   ----  ------  ----------
00:0b:86:cc:8e:4e Wireless_1    mp22     2/24  10.3.148.12  a-HT  413   3       14
```

The output of this command includes the following information:

Column	Description
BSS	The Basic Service Set (BSS) Identifier for the AP. This is usually the APs MAC address.
ESS	The Extended Service Set (ESS) Identifier is the user-defined name of an 802.11 wireless network.
s/p	The controller slot and port used by the AP, in the format <slot>/<module>/<port>.
ip	IP address of the AP.
phy	One of the following 802.11 types ■ a ■ a-HT (high-throughput) ■ g ■ g-HT (high-throughput)
chan	Channel number for the AP 802.11a/802.11n physical layer. The available channels depend on the AP's regulatory domain (country).
cur-cl	Current number of clients on the AP.
util (kbps)	Current bandwidth utilization, in kbps.

Command History

Version	Modification
ArubaOS 8.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh active

```
show ap mesh active [<mesh-cluster>|{page <page>}|{start <start>}]
```

Description

Show active mesh cluster APs currently registered on this Mobility Master.

Syntax

Parameter	Description
`<mesh-cluster>`	Name of a mesh cluster profile.
`page <page>`	Limit the output of this command to a specific number of entries by entering the number of entries you want to display.
`start <start>`	Start displaying the index of mesh APs at a chosen index number by entering the index number of the AP at which command output should start.

Examples

The output of this command displays a list of all active mesh points and mesh portals.

```
(host)[mynode] #show ap mesh active
Mesh Cluster Name: meshprofile1
-------------------------------
Name  Group   IP Address    BSSID             Band/Ch/EIRP/MaxEIRP  MTU   Enet 0/1
Mesh Role
----  -----   ----------    -----             --------------------  ---   --------
--------
mp1   mp1     10.3.148.245  00:1a:1e:85:c0:30  802.11a/157/19/36           Off/Off
Point
mp2   mp2     10.3.148.250  00:1a:1e:88:11:f0  802.11a/157/19/36
                                                  Bridge/Bridge Point
mp3   mp3     10.3.148.253  00:1a:1e:88:01:f0  802.11a/157/19/36           Bridge/Bridge Point
mpp   mpp125  10.3.148.252  00:1a:1e:88:05:50  802.11a/157/19/36     1578  -/Bridge
Portal

Parent  #Children  AP Type  Uptime
 ------  ---------  -------  ------
 mp3     0          125      13d:2h:25m:19s
 mpp     1          125      14d:21h:23m:49s
 mp2     1          125      14d:21h:14m:55s
 -       1          125      14d:19h:5m:3s
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP.
`Group`	AP group which includes the specified AP.
`IP Address`	IP address of the AP.
`BSSID`	BSSID for the AP. This is usually the AP's MAC address.

Column	Description
`Band/Ch/EIRP/MaxEIRP`	The RF band in which the AP should operate (**a** or **g**) or Radio channel used by the AP, or Current EIRP /maximum EIRP
`MTU`	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
`Enet 0/1`	Shows the current mode of each wired interface. ■ **Bridge**: 802.11 frames are bridged into the local Ethernet LAN. ■ **Tunnel**: 802.11 frames are tunneled to the Mobility Master using GRE. ■ **Split-tunnel**: 802.11 frames are either bridged into the local Ethernet LAN or tunneled to the Mobility Master, depending upon their destination. ■ **Off**: Interface is not available for serving clients. If an AP has only one wired interface, the output of this command will display a dash (-) for the unavailable port.
`Mesh Role`	An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
`Parent`	If the AP is operating as a mesh point, this parameter displays the name of its parent mesh portal. Mesh portals will display a dash (-).
`#Children`	If the AP is operating as a mesh portal, this parameter shows the number of mesh point children associated with that mesh portal.
`AP type`	The AP model type.
`Uptime`	Number of hours, minutes and seconds since the last Mobility Master reboot or bootstrap, in the format *hours:minutes:seconds*.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the secure enterprise mesh solution for outdoor APs require the Outdoor Mesh license.	Enable or Config mode on managed devices

show ap mesh debug counters

```
show ap mesh debug counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show counters statistics for a mesh node.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show counter statistics for an AP with a specific name.
`bssid <bssid>`	Show counter statistics for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	View counter statistics for an AP with a specific IP address. Enter the IP address of the AP in dotted-decimal format.

Example

The example below shows the Mesh Packet Counters table for an AP named meshpoint1. The **Probe Resp**, **Assoc Req**, and **Assoc Resp** data columns show both the total number of counters and, in parenthesis, the number of requests or responses with high-throughput information elements (HE IEs).

```
(host) [mynode] #show ap mesh debug counters ap-name meshpoint1
Mesh Packet Counters
--------------------
Interface  Echo Sent  Echo Recv  Probe Req  Probe Resp  Assoc Req  Assoc Resp  Assoc Fail  ---
---------  ---------  ---------  ---------  ----------  ---------  ----------  ----------

Link up/down  Resel.  Switch  Other
------------  ------  ------  ------
Parent     68865      68755      24          8(8 HT)     3(1 HT)     3(1 HT)     1
1             -       -       0
Child      68913      67373      6           8           2
1             2       0       2618886

Received Packet Statistics: Total 2890717, Mgmt 2618946 (dropped non-mesh 0), Data 271771
(dropped unassociated 1)HT: pns=8 ans=1 pnr=0 ars=0 arr=1 anr=0

Recovery Profile Usage Counters
-------------------------------
Item                          Value
----                          -----
Enter recovery mode           0
Exit recovery mode            0
Total connections to switch   0

Mesh loop-prevention Sequence No.:1256947
Mesh timer ticks:68930
```

The output of this command includes the following information:

Column	Description
`Interface`	Indicates whether the mesh interface connects to a **Parent** AP or a **Child** AP. Each row of data in the *Mesh Packet Counters* table shows counter values for an individual interface.
`Echo Sent`	Number of echo packets sent.
`Echo Recv`	Number of echo packets received.
`Probe Req`	Number of probe request packets sent from the interface specified in the **Mesh-IF** parameter.
`Probe Resp`	Number of probe response packets sent to the interface specified in the **Interface** parameter.
`Assoc Req`	Number of association request packets from the interface specified in the **Interface** parameter.
`Assoc Resp`	Number of association response packets from the interface specified in the **Interface** parameter. This number includes valid responses and fail responses.
`Assoc Fail`	Number of fail responses received from the interface specified in the **Interface** parameter.
`Link up/down`	Number of times the link up or link down state has changed.
`Resel.`	Number of times a mesh point attempted to reselect a different mesh portal.
`Switch`	Number of times a mesh point successfully switched to a different mesh portal.
`Other Mgmt`	Management frames of any type other than association and probe frames, either received on child interface, or sent on parent interface.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh debug current-cluster

```
show ap mesh debug current-cluster
   ap-name <ap-name>
   bssid <bssid>
   ip-addr <ip-addr>
```

Description

This command shows the AP mesh debug information for the mesh cluster currently used by a mesh point or mesh portal.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AP mesh debug information for the specified AP name.
`bssid <bssid>`	Shows AP mesh debug information for the specified BSSID. A BSSID is usually the MAC address of an AP.
`ip-addr <ip-addr>`	Shows AP mesh debug information for the specified IP address.

Examples

The example shows the AP mesh debug information of an AP named **mp2**.

```
(host) [mynode] #show ap mesh debug current-cluster ap-name mp2

AP "mp2" Current Cluster Profile: default
-----------------------------------------
Item            Value
----            -----
Cluster Name    smettu-mesh
RF Band         a
Encryption      opensystem
WPA Hexkey      N/A
WPA Passphrase  ********
```

The output of this command includes the following information:

Column	Description
`Cluster Name`	Name of the mesh cluster using this profile
`RF band`	The RF band in which the mesh point or mesh portal operates: ■ **g** = 2.4 GHz ■ **a** = 5 GHz
`Encryption`	Data encryption setting for the mesh cluster profile. ■ **opensystem**—No authentication and encryption. ■ **wpa2-psk-aes**—WPA2 with AES encryption using a preshared key.
`WPA Hexkey`	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
`WPA Passphrase`	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

show ap mesh debug forwarding-table

```
show ap mesh forwarding-table {ap-name <ap-name>}|{ip-addr <ip-addr>}
```

Description

Show the forwarding table for a remote mesh point or remote mesh portal.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for a remote mesh node with a specific name.
`ip-addr <ip-addr>`	Show data for a remote mesh node with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with your mesh network.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh debug hostapd-log

```
show ap mesh debug hostapd-log
   ap-name <ap-name>
   bssid <bssid>
   ip-addr <ip-addr>
```

Description

This command shows the AP mesh debug log messages for the **hostapd** process.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AP mesh debug log messages for the specified AP name.
`bssid <bssid>`	Shows AP mesh debug log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
`ip-addr <ip-addr>`	Shows AP mesh debug log messages for the specified IP address.

Usage Guidelines

This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with the **hostapd** process or your mesh network.

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

show ap mesh debug meshd-log

```
show ap mesh debug meshd-log {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} [<page>]
```

Description

Show the debug log messages for the **meshd** process.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`<page>`	Display page number 0, 1 or 2, where page 0 has the newest information and page 2 has the oldest. If this parameter is omitted, this command will display all meshd log information, oldest first.

Usage Guidelines

This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with the **meshd** process or your mesh network.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh debug provisioned-clusters

```
show ap mesh debug provisioned-clusters
   ap-name <ap-name>
   bssid <bssid>
   ip-addr <ip-addr>
```

Description

This command shows the cluster profiles provisioned on a mesh portal or mesh point.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AP mesh debug log messages for the specified AP name.
`bssid <bssid>`	Shows AP mesh debug log messages for the specified BSSID. A BSSID is usually the MAC address of an AP.
`ip-addr <ip-addr>`	Shows AP mesh debug log messages for the specified IP address.

Example

The example shows the statistics for the APs mesh cluster profile and recovery cluster profile on an AP mesh point named portal2.

```
(host) [mynode] #show ap mesh debug provisioned-clusters ap-name portal2


AP Portal Cluster Profile: mesh-cluster-profile
-----------------------------------------------
Parameter       Value
---------       -----
Cluster Name    sw-ad-GB32
RF Band         a
Encryption      opensystem
WPA Hexkey      N/A
WPA Passphrase  ********

AP "Portal" Cluster Profile: Recovery Cluster Profile
-----------------------------------------------------
Item            Value
----            -----
Cluster Name    Recovery-ZF-xAPl5z-g15VN
RF Band         a
Encryption      pa2-psk-aes
WPA Hexkey      ********
WPA Passphrase  N/A
```

The output of this command displays the following information for the AP's mesh cluster profile and recovery cluster profiles:

Column	Description
`Cluster Name`	Name of the mesh cluster using this profile
`RF band`	The RF band in which the AP should operate: ■ **g** = 2.4 GHz ■ **a** = 5 GHz
`Encryption`	Data encryption setting for the mesh cluster profile. ■ **opensystem**—No authentication and encryption. ■ **wpa2-psk-aes**—WPA2 with AES encryption using a preshared key.
`WPA Hexkey`	The WPA pre-shared key (only for mesh cluster profiles using WPA2 with AES encryption).
`WPA Passphrase`	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

show ap mesh neighbors

```
show ap mesh neighbors {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} [names]
```

Description

Show all mesh neighbors for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show mesh neighbors for an AP with a specific name.
`bssid <bssid>`	Show mesh neighbors for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show mesh neighbors for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`names`	If you include this optional parameter, the **Portal** column in the output of this command will translate the BSSIDs of mesh parent and child APs to AP names (where available).

Example

In the example below, the output has been split into two tables to better fit on the page. In the actual CLI, the output appears in a single, wide table. The **Flags** column the output of this command indicates the high-throughput (HT) properties of the mesh node. In the example below, the string "HT-40MHzsgi-2ss" indicates that the node uses a 40MHz channel with a short guard interval (sgi) and sends 2 spatial streams (ss).

```
(host) [mynode] #show ap mesh neighbors ap-name portal

Neighbor list
-------------
MAC                Portal             Channel  Age  Hops  Cost   Relation      Flags  RSSI
Rate Tx/Rx
---                ------             -------  ---  ----  ----   --------      -----  ----  --
--------
00:0b:86:e8:09:d1  00:1a:1e:88:01:f0  157      0    1     11.00  C 3h:15m:42s  -      65
54/54
00:1a:1e:88:02:91  00:1a:1e:88:01:f0  157      0    1     4.00   C 3h:35m:30s  HL     59
300/300
00:0b:86:9b:27:78  Yes                157      0    0     12.00  N 3h:22m:46s  -      26    -

00:0b:86:e8:09:d0  00:1a:1e:88:01:f0  157      0    1     11.00  N 3h:15m:36s  -      65    -

00:1a:1e:88:02:90  00:1a:1e:88:01:f0  157+     0    1     2.00   N 3h:35m:6s   HL     59    -


A-Req  A-Resp  A-Fail  HT-Details       Cluster ID
-----  ------  ------  ----------       ----------
1      1       0       Unsupported      sw-ad-GB32
1      1       0       HT-40MHzsgi-2ss  sw-ad-GB322
0      0       0       Unsupported      mc1
0      0       0       Unsupported      sw-ad-GB32
0      0       0       HT-40MHzsgi-2ss  sw-ad-GB32

Total count: 5, Children: 2
```

```
Relation: P = Parent; C = Child; N = Neighbor; B = Blacklisted-neighbor
Flags: R = Recovery-mode; S = Sub-threshold link; D = Reselection backoff; F = Auth-failure; H
= High Throughput; L = Legacy allowed
```

The output of this command includes the following information:

Column	Description
MAC	MAC address of the mesh node.
Portal	By default, this column displays the BSSID of the mesh point. If you include the optional **names** parameter, this column will display AP names, if available. The AP names will include **[p]** (parent), or **[c]** (child) suffixes to indicate the role of the mesh BSSID.
Channel	Number of a radio channel used by the AP.
Age	Number of seconds elapsed since the AP heard from the neighbor.
Hops	Indicates the number of hops it takes traffic from the mesh node to get to the mesh portal. The mesh portal advertises a hop count of 0, while all other mesh nodes advertise a cumulative count based on the parent mesh node
Cost	A relative measure of the quality of the path from the AP to the controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (e.g, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
Relation	Shows the relationship between the specified AP and the AP on the neighbor list and the amount of time that relationship has existed. ■ **P** = Parent ■ **C** = Child ■ **N** = Neighbor ■ **B** = Blacklisted-neighbor
Flags	This parameter shows additional information about the mesh neighbor. The key describing each flag appears at the bottom of the neighbor list.
RSSI	The Receive Signal Strength Indicator (RSSI) value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
Rate Tx/Rx	The rate, in Mbps, that a neighbor transmits data to or receives data from the mesh-node specified by the command.
A-Req	Number of association requests from clients
A-Resp	Number of association responses from the mesh node
A-Fail	Number of association failures
Cluster	Name of the Mesh cluster that includes the specified AP or BSSID.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh tech-support

```
show ap mesh tech-support ap-name <ap-name> <filename>
```

Description

Display all information for an AP, and save that information in a file on the controller

Syntax

Parameter	Description
`<ap-name>`	Name of an AP for which you want to create a report
`<filename>`	Filename for the report created by this command. The file can only be saved in the flash directory. If desired, you can use FTP or TFTP to copy the file to another destination.

Usage Guidelines

This command displays the output of the multiple mesh and debug CLI commands, then saves that data into a report file on the controller's flash drive, where it can be analyzed for debugging purposes. The information in this report includes the output of the following commands:

- show ap mesh neighbors
- show ap mesh debug current-cluster
- show ap mesh debug provisioned-clusters
- show ap mesh debug counters
- show ap mesh debug forwarding-table
- show ap mesh debug meshd-log
- show ap mesh debug hostapd-log

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh topology

```
show ap mesh topology [long] [page <page>] [start <start>]
```

Description

Show the mesh topology tree.

Syntax

Parameter	Description
`long`	Include the names of a mesh portal's children in the output of this command
`page <page>`	Limit the output of this command to a specific number of entries by entering the number of entries you want to display.
`start <start>`	Start displaying the mesh topology tree at a chosen index number by entering the index number of the AP at which command output should start.

Example

An **(N)** in the **Mesh Role** column indicates the node is 11N capable. An **(N)** beside the parent name in the **Parent** column indicates that the mesh node's the parent is also 11N capable.

```
(host) [mynode] #show ap mesh topology


Mesh Cluster Name: sw-ad-GB32
-----------------------------
Name Mesh Role    Parent  Path Cost  Node Cost  Link Cost  Hop Count  RSSI  Rate Tx/Rx
---- ---------    ------  ---------  ---------  ---------  ---------  ----  ----------  Last
Update  Uplink Age  #Children
----------  ----------  ---------

ad-ap Point (N)    mp3     2          0          0          1          61    300/270     6m:12s
     3h:8m:7s    0

msc-1 Point        mp3     2          0  0          1          64    54/54       6m:36s
2h:48m:12s  0

Total APs :2
(R): Recovery AP. (N): 11N Enabled. For Portals 'Uplink Age' equals uptime.
```

The output of this command includes the following information:

Column	Description
`Name`	Name of the mesh node.
`Mesh Role`	An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
`Parent`	If the AP is operating as a mesh point, this parameter displays the name of its parent mesh portal.

Column	Description
Path Cost	A relative measure of the quality of the path from the AP to the controller. A lower number indicates a better quality path, where a higher number indicates a less favorable path (e.g, a path which may be longer or more congested than a path with a lower value.) For a mesh point, the path cost is the sum of the (parent path cost) + (the parent node cost) + (the link cost).
Node Cost	A relative measure of the quality of the node, where a lower number of is more favorable than a higher number. This cost is related to the number of children on the specified node.
Link Cost	A relative measure of the quality of the link. For example, a more congested link will have a higher link cost than a similar, less-congested link.
Hop Count	Number of hops to the mesh portal.
RSSI	The Receive Signal Strength Indicator (RSSI) value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
Rate Tx/Rx	The rate, in Mbps, that a mesh point transmits and receives at on its uplink. Note that the rate information is only as current as indicated in the **Last Update** column.
Last Update	Time elapsed since the mesh node last updated its statistics.
Uplink Age	Time elapsed since the mesh node became active in the mesh topology.
#Children	Number of children associated with a parent mesh point.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh-cluster-profile

```
show ap mesh-cluster-profile [<profile>]
```

Description

Show configuration settings for a mesh cluster profile.

Syntax

Parameter	Description
`<profile>`	Name of a mesh cluster profile

Usage Guidelines

The command **show ap mesh-cluster-profile** displays a list of all mesh cluster profiles configured on the Mobility Master, including the number of references to each profile and each profile's status. Include the optional <profile> parameter to show detailed settings for an individual mesh cluster profile.

Examples

The example below shows the configuration settings for the mesh cluster profile "meshcluster2".

```
(host)[mynode] #show ap mesh-cluster-profile meshcluster2

Mesh Cluster profile "meshcluster2"
-----------------------------
Parameter       Value
---------       -----
Cluster Name    company-mesh
RF Band         a
Encryption      opensystem
WPA Hexkey      N/A
WPA Passphrase  N/A
```

The output of this command includes the following information:

Parameter	Description
`Cluster Name`	Name of the mesh cluster using this profile
`RF band`	The RF band in which the AP should operate: ■ **g** = 2.4 GHz ■ **a** = 5 GHz
`Encryption`	Data encryption setting for the mesh cluster profile. ■ **opensystem**—No authentication and encryption. ■ **wpa2-psk-aes**—WPA2 with AES encryption using a preshared key.
`WPA Hexkey`	The WPA PSK (only for mesh cluster profiles using WPA2 with AES encryption).
`WPA Passphrase`	The WPA password that generates the preshared key (only for mesh cluster profiles using WPA2 with AES encryption).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This show command is available in the base operating system. Commands to configure the mesh feature require the Mesh license.	Enable or Config mode on managed devices

show ap mesh-ht-ssid-profile

```
show ap mesh-ht-ssid-profile [<profile>]
```

Description

Show configuration settings for a mesh high-throughput Service Set Identifier (SSID) profile.

Syntax

Parameter	Description
`<profile>`	Name of a mesh high-throughput SSID profile.

Usage Guidelines

High-throughput APs support additional settings not available in legacy APs. A mesh high-throughput SSID profile can enable or disable high-throughput (802.11n) features and 40 Mhz channel usage, and define values for aggregated MAC protocol data units (MDPUs) and Modulation and Coding Scheme (MCS) ranges.

The command **show ap mesh-ht-ssid-profile** displays a list of all mesh high-throughput SSID profiles configured on the Mobility Master, including the number of references to each profile and each profile's status. Include the optional **<profile>** parameter to show detailed settings for an individual mesh high-throughput SSID profile.

Examples

The example below shows the configuration settings for the mesh high-throughput radio profile "default".

```
(host) [mynode] #show ap mesh-ht-ssid-profile default

Mesh High-throughput SSID profile "default"
-------------------------------------------
Parameter                                                    Value
---------                                                    -----
40 MHz channel usage                                         Enabled
BA AMSDU Enable                                              Enabled
Temporal Diversity Enable                                    Disabled
High throughput enable (SSID)                                Enabled
Legacy stations                                              Allowed
Low-density Parity Check                                     Enabled
Maximum number of spatial streams usable for STBC reception  1
Maximum number of spatial streams usable for STBC transmission  1
MPDU Aggregation                                             Enabled
Max received A-MPDU size                                     65535 bytes
Max transmitted A-MPDU size                                  65535 bytes
Min MPDU start spacing                                       8 usec
Short guard interval in 20 MHz mode                          Enabled
Short guard interval in 40 MHz mode                          Enabled
Supported MCS set                                            0-23
```

The output of this command includes the following information:

Column	Description
40 MHz channel usage	This parameter shows if the profile enables or disables the use of 40 MHz channels.
BA AMSDU Enable	Shows of the AP has enabled or disabled the ability to receive AMSDU in BA negotiation.
Temporal Diversity Enable	Shows if temporal diversity has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries.
High throughput enable (SSID)	Shows if 802.11n high-throughput features are enabled or disabled for this profile. By default, high-throughput features are enabled.
Legacy stations	Allow or disallow associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).
Low-density Parity Check	If enabled, the AP will advertise Low-density Parity Check (LDPC) support. LDPC improves data transmission over radio channels with high levels of background noise.
Maximum number of spatial streams usable for STBC reception	Shows the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the 130 Series, 170 Series, and AP-105 only. The configured value will be adjusted based on AP capabilities.) **NOTE:** If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
Maximum number of spatial streams usable for STBC transmission	Shows the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on 170 Series, 130 Series, and AP-105 only. The configured value will be adjusted based on AP capabilities.) **NOTE:** If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
MPDU Aggregation	Shows if the profile enables or disables MAC protocol data unit (MPDU) aggregation.
Max received A-MPDU size	Configured maximum size of a received aggregate MPDU, in bytes.
Max transmitted A-MPDU size	Configured maximum size of a transmitted aggregate MPDU, in bytes.

Column	Description
`Min MPDU start spacing`	Configured minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.
`Supported MCS set`	Displays a list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20MHz vs. 40MHz) and the number of spatial streams used by the mesh node.
`Short guard interval in 20 MHz mode`	Shows if the profile enables or disables use of short (400ns) guard interval in 20 MHz mode.
`Short guard interval in 20 MHz mode`	Shows if the profile enables or disables use of short (400ns) guard interval in 40 MHz mode.
`Explicit Transmit Beamforming`	Shows if Explicit Transmit Beamforming is enabled or disabled for 130 Series APs. **NOTE:** If this parameter is disabled, the other transmit beamforming configuration settings have no effect.
`Transmit Beamforming Compressed Steering`	When enabled, the AP can use explicit compressed feedback from clients to obtain a steering matrix. (For 130 Series APs only.)
`Transmit Beamforming non Compressed Steering`	When enabled, the AP can use explicit noncompressed feedback from clients to obtain a steering matrix. (For 130 Series only)
`Transmit Beamforming delayed feedback support`	Shows if the AP has enabled or disabled delayed feedback/report support in Transmit Beamforming. (For 130 Series only)
`Transmit Beamforming immediate feedback support`	Shows if the AP has enabled or disabled immediate feedback/report support in Transmit Beamforming. (For 130 Series only)
`Transmit Beamforming Sounding Interval`	Time interval in seconds between updates of Transmit Beamforming channel estimation. (For 130 Series only)

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh-radio-profile

```
show ap mesh-radio-profile [<profile>]
```

Description

Show configuration settings for a mesh radio profile.

Syntax

Parameter	Description
<profile>	Name of a mesh radio profile.

Usage Guidelines

The radio profile determines the radio frequency/channel used only by mesh nodes to establish mesh links. Mesh nodes operating in different cluster profiles can share the same radio profile. Conversely, mesh portals using the same cluster profile can be assigned different mesh radio profiles to achieve frequency separation.

The command s**how ap mesh-radio-profile** displays a list of all mesh radio profiles configured on the controller, including the number of references to each profile and each profile's status. Include the optional <*profile*> parameter to show detailed settings for an individual mesh radio profile.

Example

The example below shows the configuration settings for the mesh cluster profile "default".

```
(host) [mynode] #show ap mesh-radio-profile default
Mesh Radio profile "default"
----------------------------
Parameter                                                   Value
---------                                                   -----
802.11a Transmit Rates                                      6 9 12 18 24 36 48 54
802.11g Transmit Rates                                      1 2 5 6 9 11 12 18 24 36 48 54
Allowed VLANs on mesh link                                  1-4094
BC/MC Rate Optimization                                     Enabled
Heartbeat threshold                                         10
Link Threshold                                              12
Maximum Children                                            64
Maximum Hop Count                                           8
Mesh Private Vlan                                           0
Mesh High-throughput SSID Profile                           default
Mesh Survivability                                          Disabled
Metric algorithm                                            distributed-tree-rssi
Rate Optimization for delivering EAPOL frames and mesh echoes  Disabled
Reselection mode                                            startup-subthreshold
Retry Limit                                                 8
RTS Threshold                                               2333 bytes
```

The output of this command includes the following information:

Parameter	Description
802.11a Transmit Rates	Indicates the transmit rates for the 802.11a radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
802.11g Transmit Rates	Indicates the transmit rates for the 802.11g radio. The AP attempts to use the highest transmission rate to establish a mesh link. If a rate is unavailable, the AP goes through the list and uses the next highest rate.
Allowed VLANs on mesh link	Specify a list of VLAN IDs that can be used by a mesh link on APs associated with this mesh radio profile
BC/MC Rate Optimization	If enabled, the mesh node will use the slowest associated mesh-point rate for broadcast/multicast data (rather than minimum).
Heartbeat Threshold	Indicates the maximum number of heartbeat messages that can be lost between neighboring mesh nodes before the mesh node is considered inactive and is dropped as a mesh neighbor.
Link Threshold	Indicates the threshold for the lowest acceptable Receive Signal Strength Indicator (RSSI) value. Links that drop below this threshold will have an increased link cost. Default: 12.
Maximum Children	The maximum number of children a mesh portal can accept.
Maximum Hop Count	The maximum number of hops allowed between a mesh point and a mesh portal.
Mesh Private Vlan	This parameter is experimental and reserved for future use.
Mesh High-throughput SSID Profile	The High-throughput SSID Profile associated with this mesh radio profile.
Mesh Survivability	This parameter shows if mesh points and portals can become active even if the controller cannot be reached by bridging LAN traffic. This is a beta feature that is disabled by default; it should not be enabled unless you are instructed to do so by Aruba technical support.
Metric algorithm	Algorithm used by a mesh node to select its parent.
Rate Optimization for delivering EAPOL frames and mesh echoes	If this option is enabled, mesh APs will use a more conservative rate for more reliable delivery of EAPOL frames.

Parameter	Description
`Reselection Mode`	Specifies the one of the following methods used to find a better mesh link. ■ **startup-sub-threshold**: When bringing up the mesh network, mesh nodes have 3 minutes to find a better uplink. After that time, each mesh node evaluates alternative links only if the existing uplink falls below the configured threshold level (the link becomes a sub-threshold link). The reselection process is canceled if the average RSSI rises on the existing uplink rises above the configured link threshold. ■ **reselect-any-time:** Connected mesh nodes evaluate alternative mesh links every 30 seconds. If a mesh node finds a better uplink, the mesh node connects to the new parent to create an improved path to the mesh portal. ■ **reselect-never**: Connected mesh nodes do not evaluate other mesh links to create an improved path to the mesh portal. ■ **subthreshold-only**: Connected mesh nodes evaluate alternative links only if the existing uplink becomes a sub-threshold link.
`Retry Limit`	Maximum number of times a mesh node can re-send a packet.
`RTS Threshold`	The packet size sent by mesh nodes. Mesh nodes transmitting frames larger than this threshold must issue request to send (RTS) and wait for other mesh nodes to respond with clear to send (CTS) to begin transmission. This helps prevent mid-air collisions.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap mesh-recovery-profile

```
show ap mesh-recovery-profile
```

Description

This command shows the mesh recovery-profile information.

Syntax

No parameters.

Usage Guidelines

This command shows the mesh recovery-profile information.

Example

The following example shows the mesh recovery-profile information:

```
(host) [mynode] #show ap mesh-recovery-profile

AP Mesh Recovery Profile
------------------------
Item             Value
----             -----
Cluster Name     RecoveryRVOCDoNgqKqDEGOZ
RF Band          a
WPA Hexkey       ********
WPA Passphrase   N/A
Encryption       wpa2-psk-aes
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable mode on Mobility Master.

show ap monitor

```
show ap monitor
   active-laser-beams {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   [channel <channel>|phy <phy>]
   ap-list {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   channel {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   client-list {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   containment-info {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}

   debug {counters|profile-config|status}[ap-name <ap-name>|bssid <bssid>|ip-addr <ip-
   addr>|ip6-addr <ip6-addr>]
   ids-state {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   mesh-list {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   pot-ap-list {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   pot-client-list {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   routers {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   scan-info {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   stats {[ap-name <ap-name>]|[bssid <bssid>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>]|[mac
   <mac>] [duration <duration>] [verbose]}
   stats advanced {[[ap-name <ap-name>]|[ip-addr <ip-addr>]|[ip6-addr <ip6-addr>][client-mac
   <client-mac>]]|[bssid <bssid>]}
   wired-mac {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|[ip6-addr <ip6-addr>]
   {ap-bssid <ap-bssid>}|{config <config>}|{enet-mac <enet-mac>}|{gw-mac <gw-mac>}|{oui-prop
   <oui-prop>}|{system-gw-mac <system-gw-mac>}|{system-wired-mac <system-wired-mac>}
```

Description

Show information for Aruba Air Monitors.

Syntax

Parameter	Description
`active-laser-beams`	Show active laser beam generators. The output of this command shows a list of all APs that are actively performing policy enforcement containment such as rogue containment. This command can tell us which AP is sending out deauthorization frames, although it does not specify which AP is being contained.
`ap-list`	Show list of APs being monitored.
`arp-cache`	Show ARP Cache of learned IP to MAC binding
`channel`	Show state and stats of a specific channel.
`client-list`	Show list of client being monitored.

Parameter	Description
`containment-info`	Show containment events and counters triggered by the wired containment and wireless containment features configured in the ids general-profile. The output of this command shows device and target data for wired containment activity, a well as data for the following counters. Wireless Containment Counters: ■ Last Deauth Timer Tick ■ Deauth frames to AP ■ Deauth frames to Client ■ Last Tarpit Timer Tick ■ Tarpit Frames: Probe Response ■ Tarpit Frames: Association Response ■ Tarpit Frames: Authentication ■ Tarpit Frames: Data from AP ■ Tarpit Frames: Data from Client ■ Last Enhanced Adhoc Containment Timer Tick ■ Enhanced Adhoc Containment: Frames To Data Sender ■ Enhanced Adhoc Containment: Frames To Data Receiver ■ Enhanced Adhoc Containment: Response to Request ■ Enhanced Adhoc Containment: Replay Response Wired Containment Counters: ■ Last Wired Containment Timer Tick ■ Last Tagged Wired Containment Timer Tick ■ Spoof frames sent ■ Spoof frames sent on tagged VLAN
`debug`	Show the Air Monitor debugging information.
`counters`	Shows the maximum classification delay that was observed in monitored APs and clients, the number of Unclassified Device messages that were sent to the WMS, and the number of monitored APs/clients that were present in those messages. This parameter also shows the number of monitored APs/clients that were created and removed by the AP. This information is captured on an hourly basis for the last 24 hours. **NOTE:** The maximum delay for clients is not displayed if the **unclass_sta_update** parameter is not enabled.
`profile-config`	Shows the configuration received by the AP for each profile.
`status`	Shows general AP status information and the maximum classification delay that was observed in monitored APs and clients, in the **WLAN Interface** option. **NOTE:** The maximum delay for clients is not displayed if the **unclass_sta_update** parameter is not enabled.
`ids-state`	Show IDS State.
`ap-name`	Name of Access Point.
`bssid`	BSSID of Access Point.
`ip-addr`	IP Address of Access Point.
`ip6-addr`	IPv6 Address of Access Point.
`mesh-list`	Show list of Mesh APs being monitored.

Parameter	Description
`pot-ap-list`	Display the Potential AP table. The Potential AP table shows the following data: ■ **bssid**: the AP's Basic Service Set Identifier. ■ **channel**: The AP's current radio channel ■ **phy type**: The radio's PHY type. Possible values are 802.11a, 802.11a-HT-40, 802.11b/g, 802.11b/g-HT-20. ■ **num-beacons**: Number of beacons seen during a 10-second scan ■ **tot-beacons**: Total number of beacons seen since the last reset. ■ **num-frames**: Total number of frames seen since the last rest. ■ **mt**: Monitor time; the number of timer ticks elapsed since the controller first recognized the AP. ■ **at**: Active time, in timer ticks. ■ **ibss**: Shows if adhoc BSS is enabled or disabled. It will be enabled if the bssid has detected an adhoc BSS (an ibss bit in an 802.11 frame). ■ **rssi**: The Receive Signal Strength Indicator (RSSI) value displayed in the output of this command represents signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
`pot-client-list`	Display the Potential client table. The Potential Client table shows the following values: ■ **last-bssid**: the Last BSSID to which the client associated. ■ **from-bssid** ■ **to-bssid** ■ **mt:** monitor time - the number of timer ticks elapsed since the controller first recognized the client. ■ **it:** client idle time - expressed as a number of timer ticks.
`routers`	Show Router MAC Addresses learned. The output of this command includes the router's MAC address, IP address and uptime.
`scan-info`	Show AP scanning information.
`stats`	Shows statistics for an AP or a client.
`mac <mac>`	MAC address of an AP or a client
`duration <duration>`	Duration to compute average signal strength in minutes. Default is 1 minute.
`verbose`	Shows statistics in verbose mode.
`stats advanced`	Shows advanced statistics for an AP or a client.
`client-mac <client-mac>`	MAC address of client
`wired-mac`	Show Wired MAC Addresses learned.
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show data for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Parameter	Description
ap-bssid <ap-bssid>	Include the optional **ap-bssid <ap-bssid>** parameters to show how the AP is monitoring information for another AP with a specific BSSID.
enet-mac <enet-mac>	Include the optional e**net-mac <enet-mac>** parameters to show how the AP is monitoring information for an interface with a specific Ethernet MAC address.

Examples

The output of the command displays the Monitored AP table, which lists all the APs monitored by a specified AP or BSSID.

```
(host) #show ap monitor ap-list ap-name al12

Monitored AP Table
------------------
bssid              essid                chan  ap-type              phy-type        dos
dt/mt        ut/it
-----              -----                ----  -------              --------        ---      -
----        -----
24:de:c6:be:c3:fa  bridge-85            161   interfering          80211a-HT-40    disable
33633/17957  0/0
24:de:c6:8e:aa:86  ap214-tb2-%apprf%    11    interfering          80211b/g-HT-20  disable
33633/33633  0/0
24:de:c6:be:b7:3a  bridge-85            64    interfering          80211a-HT-40    disable
33633/17065  8/4
24:de:c6:be:bf:fa  bridge-85            149   interfering          80211a-HT-40    disable
33633/17404  0/0
24:de:c6:8e:9a:85  sys-tb2-4meshpt      11    interfering          80211b/g-HT-20  disable
33633/33633  0/0
9c:1c:12:89:e2:95  RBC-BYOD             153   interfering          80211a-VHT-20   disable
33633/33633  1/0
24:de:c6:be:bd:f8  Centl2-250           157   interfering          80211a-HT-40    disable
33633/17914  0/0
24:de:c6:be:bd:f9  Centl2-251           157   interfering          80211a-HT-40    disable
33633/17800  0/0
24:de:c6:8e:9a:86  ap214-tb2-%apprf%    11    interfering          80211b/g-HT-20  disable
33633/33633  0/0
9c:1c:12:89:e2:93  ssid1-vc-wpa         153   interfering          80211a-VHT-20   disable
33633/33633  0/0

encr            nstas  avg-snr  curr-snr  avg-rssi  curr-rssi  wmacs  ibss  cl-delay
----            -----  -------  --------  --------  ---------  -----  ----  --------
wpa2-psk-aes    0      37       37        57        58         0      no    0
open            0      53       55        41        40         0      no    0
wpa2-psk-aes    0      45       45        49        50         0      no    0
wpa2-psk-aes    0      37       37        57        58         0      no    0
wpa2-psk-aes    0      50       56        44        39         0      no    0
wpa2-psk-aes    0      38       40        56        55         0      no    0
wpa2-psk-aes    0      30       31        64        64         0      no    0
wpa2-8021x-aes  0      30       31        64        64         0      no    0
open            0      52       55        42        40         0      no    0
wpa-psk-tkip    0      38       40        56        55         0      no    0
```

The output of this command includes the following information:

Parameter	Description
bssid	Basic Service Set Identifier for (bssid) an AP. This is usually the AP's MAC address.
essid	Extended service set identifier that names a wireless network.
chan	Radio channel used by the BSSID.
ap-type	Shows classification of the AP.
phy-type	Radio phy type. Possible types include: ■ 802.11a ■ 802.11a-HT-40 ■ 802.11b/g ■ 802.11b/g-HT-20
dos	Shows if the feature to contain DoS attacks has been enabled or disabled.
dt/mt	**dt**—Detected time: the number of timer ticks since the AP was last detected. **mt**—Monitor time; the number of elapsed timer ticks since the AP first recognized the monitored AP.
ut/it	**ut**—Unseen time: the number elapsed timer ticks the monitored AP was not seen when scanning a channel of the device. **it**—AP idle time, the number of timer ticks since the AP last saw any frames from the monitored AP.
encr	Shows the encryption type of the BSSID. If there are multiple encryption types, this command shows the lowest encryption type.
ntsas	Shows the number of stations connected to the AP (as seen by the monitoring AP).
avg-snr	Shows the average Signal to Noise Ratio (SNR).
curr-snr	Shows the current Signal to Noise Ratio (SNR).
avg-rssi	Shows the average RSSI (Received Signal Strength) for the device. **NOTE:** RSSI is an indication of the power level being received by the antenna. Therefore, the higher the RSSI number, the stronger the signal.
curr-rssi	Shows the current RSSI for the device.
wmacs	Shows the number of unique wireless MAC addresses seen on the Wi-Fi network from the AP's BSSID.
ibss	Shows all the monitored APs (BSSIDs).
cl-delay	Shows the delay in classification of each device. **NOTE:** The maximum delay for clients is not displayed if the **unclass_sta_update** parameter is not enabled.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap monitor association

```
show ap monitor association {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>} <ap-bssid>
```

Description

Show the association table for an Air Monitor (AM).

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AM with a specific name.
`bssid <bssid>`	Show data for an AM with a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AM's MAC address.
`ip-addr <ip-addr>`	Show data for an AM with a specific IP address by entering its IP address in dotted-decimal format.
`<ap-bssid>`	BSSID of an AP.

Examples

The output of the command lists the MAC addresses associated with the Air Monitor BSSID.

```
(host) #show ap monitor association ap-name ap9 00:1a:1e:11:74:a1
Association Table
-----------------
mac                rsta-type  auth  phy-type
---                ---------  ----  --------
00:1d:d9:01:c4:50  valid      yes   80211a
00:17:f2:4d:01:e2  valid      yes   80211a
00:1f:3b:8c:28:89  valid      yes   80211a
00:1d:d9:05:05:d0  valid      yes   80211a
00:14:a4:25:72:6d  valid      yes   80211a
00:19:7d:d6:74:8d  valid      yes   80211a
```

The output of this command includes the following information:

Column	Description
`mac`	MAC address associated with the Air Monitor BSSID
`rsta-type`	Rogue station type: ■ **interfering**: Interfering station. ■ **valid**: Station is not a rogue station. ■ **DoS**: Station may have attempted a DoS attack.
`auth`	Displays a **yes** if the client has been authenticated.
`phy-type`	The RF band in which the AP should operate: **802.11g** = 2.4 GHz **802.11a** = 5 GHz

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap monitor debug

```
show ap monitor debug counters|status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
show ap monitor debug profile-config {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
am-scan|ap-radio|ap-system|arm|event-thresholds|ids-dos|ids-general|ids-impersonation|ids-
signature-matching|ids-unauthorized-device|interference|regulatory-domain|rf-behavior
```

Description

Show information for an Air Monitor's current status, message counters, or profile settings.

Syntax

Parameter	Description
`counters`	Show Air Monitor (AM) message counters.
`status`	Show the status of an Air Monitor.
`ap-name <ap-name>`	Show data for an AM with a specific name.
`bssid <bssid>`	Show data for an AM with a specific Basic Service Set Identifier (BSSID). The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AM with a specific IP address by entering its IP address in dotted-decimal format.
`profile-config`	Show an Air Monitor profile configuration.
`am-scan`	Show Air Monitor active scanning configuration.
`ap-radio`	Show the Air Monitor radio configuration parameters, as defined in the AM's 802.11a, 802.11b, or high-throughput radio profiles.
`ap-system`	Show an Air Monitor's system configuration settings, as defined in it's AP System profile.
`arm`	Show an Air Monitor's Adaptive Radio Management (ARM) settings, as defined in its current ARM profile
`event-thresholds`	Show an Air Monitor Event Thresholds settings, as defined in its current RF Event Thresholds profile
`ids-dos`	Show an Air Monitor IDS DoS settings, as defined in its current IDS DoS profile.
`ids-general`	Show an Air Monitor IDS General Configuration settings, as defined in its IDS General profile.
`ids-impersonation`	Show an Air Monitor IDS Impersonation Configuration settings, as defined in its IDS Impersonation profile.
`ids-signature-matching`	Show an Air Monitor IDS Signature Matching configuration settings, as defined in its IDS Signature Matching profile

Parameter	Description
ids-unauthorized-device	Show an Air Monitor IDS Unauthorized Device configuration settings, as defined in its IDS Unauthorized Device profile.
interference	Show an Air Monitor's interference configuration settings, as defined in its current RF Optimization profile.
regulatory-domain	Show an Air Monitor's Regulatory Domain configuration settings, as defined in its Regulatory Domain profile.
rf-behavior	Show an Air Monitor RF Behavior Configuration

Examples

The output of the following command includes the *WLAN Interface*, *Data Structures*, *WLAN InterfaceSwitch Status* and *RTLS Configuration* tables for the specified AP.

```
(host) #show ap monitor debug status ap-name ap12
WLAN Interface
--------------
bssid              scan    monitor  probe-type  phy-type        task   channel  pkts
-----              ----    -------  ----------  --------        ----   -------  ----
00:1a:1e:11:5f:10  enable  enable   sap         80211a-HT-40    tuned  153      496970814
00:1a:1e:11:5f:00  enable  enable   sap         80211b/g-HT-20  tuned  6        391278179

Wired Interface
---------------
mac                ip                   gw-ip           gw-mac             status  pkts
---                --                   -----           ------             ------  ----
macs gw-macs tagged-pkts vlan
---- ------- ----------- ----
00:1a:1e:c9:15:f0  192.0.2.32.200       192.0.2.32.254  00:0b:86:08:e1:00  enable  101960
2    3       1           03
Global Counters
---------------
key                   value
---                   -----
Packets Read          888248993
Bytes Read            2819670134
Num Interrupts        681037971
Num Buffer Overflows  591393
Max PPS               16239
Cur PPS               1130
Max PPI               20
Cur PPI               2
Uptime                3323085
AP Name               AL12
LMS IP
Master IP
AP Type               125
Country Code          2

Data Structures
----------------
ap  sta  pap  psta  ch  msg-hash  ap-l
--  ---  ---  ----  --  --------  ----
20  40   17   55    24  21        20

Other Parameters
-----------------
```

```
key                    value
---                    -----
WMS on Master          disabled
Stats Update Interval  60
Poll Interval          174000
Num Switches           1
Collect Stats          enabled

WLAN Interface Switch Status
----------------------------
Bssid              Type   Status  Last-reg  N-reg  Last-update  Next-update  N-updates  Last-
ack
-----              ----   ------  --------  -----  -----------  -----------  ---------  ------
--
00:1a:1e:11:5f:10  local  up      3321891   3821   3322965      197          10368
3322965
00:1a:1e:11:5f:00  local  up      3321891   3821   3322917      187          10378
3322965

RTLS Configuration and State
----------------------------
Type       Server IP  Port  Freq  Active  Rpt-Tags  Tag-Mcast-Addr     Tags-Sent  Rpt-Sta
Incl-Unassoc-Sta  Sta-Sent  Cmpd-Msgs-Sent
----       ---------  ----  ----  ------  --------  --------------     ---------  -------  ---
------------  --------  --------------
MMS        N/A        N/A   N/A           disable   01:0c:cc:00:00:00  N/A        disable  N/A
              N/A       N/A
Aeroscout  N/A        N/A   30     *      disable   00:00:00:00:00:00  N/A        enable
disable           2610      265
RTLS       N/A        N/A   20     *      disable   01:18:8e:00:00:00  N/A        enable
enable
```

The output of this command includes the following information:

Column	Description
bssid	The Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
scan	Indicates whether or not if active scanning is enabled on this AP.
monitor	Indicates whether the AP radio is currently enabled or disabled.
probe-type	This parameter displays one of the following options to show the AP is configured. ■ **sap**: Default AP setting. ■ **am**: AP is configured as an Air Monitor. ■ **m-portal**: AP is configured as a Mesh portal. ■ **m-point**: AP is configured as a Mesh point.
task	This parameter displays one of the following options to show the radio's current task: ■ **scan**: AP is scanning other channels. ■ **tuned**: AP is tuned on one channel. ■ **locate**: AP has been asked to locate a specific AP or client. ■ **pcap**: The AP is enabled with the Packet Capture feature.
channel	The radio channel currently used by an AP's WLAN interface.
pkts	Number of packets seen on the interface.

Column	Description
mac	MAC address for the AP's wired interface.
ip	The AP's IP address.
gw-ip	IP address for the AP's gateway.
gw-mac	MAC address for the AP's gateway.
status	Shows if the interface is currently enabled or disabled.
pkts	Number of packets seen on the AP's wired interface.
macs	Number of MAC addresses in the Wired MAC table for that interface.
gw-macs	Number of MAC addresses in the Wired MAC table for that interface.
tagged-pkts	Number VLAN-tagged packets sent to that interface.
vlan	The VLAN ID for the packets sent to that interface.
Packets read	Number of packets read by the AP since it was last reset.
Bytes read	Number of bytes read by the AP since it was last reset.
Num Intercepts	Number of interrupts from the AP's driver.
Num Buffer Overflows	Number of times excessive traffic has filled the AP's buffers.
Max PPS	Maximum throughput rate seen on the interface, in packets per second.
Cur PPS	Current throughput rate seen on the interface, in packets per second.
Max PPI	Maximum interrupt rate seen on the interface, in interrupts per second.
Cur PPI	Current interrupt rate seen on the interface, in interrupts per second.
Uptime	Number of seconds since the AP was last reset.
LMS IP	IP address of the AP's managed device
Master IP	IP address of the AP's Mobility Master.
AP type	AP model type.
Country Code	The AP's country code. Valid radio channels for your wireless network are based on your country code. If you change the AP's country code, the valid channels will be reset to the defaults for the new country.
ap	Number of other APs monitored by this AP.
sta	Number of clients and APs seen by this AP.
pap	Number of potential APs; APs which have transmitted a beacon, but have not yet been registered.
psta	Number of potential stations; AP has seen a MAC address from the station but hasn't yet received traffic from it.

Column	Description
ch	Number of channel entries in the channel table.
msg-hash	Number of different message types seen on the interface.
ap-l	(For internal use only)
WMS on Master	Indicates if the AP communicates to the wms process on Mobility Master or a managed device. **enabled**: Communicates with Mobility Master. **disabled**: Communicates with a managed device only.
Stats Update Interval	If the AP is collecting statistics, this value is the interval in seconds in which the AP sends statistics to the WMS process.
Poll Interval	Interval, in milliseconds, that the AP sends RSSI updates to the WMS process.
Num Switches	Number of controllers to which this AP has access. If the value is 1, the AP has access to Mobility Master *or* a managed device. If the value is 2, the AP has access to Mobility Master *and* a managed device.
Collect Stats	If enabled, the AP will collect statistics to send to the WMS process.
Bssid	BSSID of the radio.
Type	Indicates whether the controller type is **master** (Mobility Master) or **local** (managed device).
Status	If **up**, the AP can reach the managed device. If **down**, the AP cannot reach the managed device.
Last-reg	The time the AP last registered with the WMS process.
N-reg	Number of times the AP has registered with the WMS process.
Last-update	The last timer tick time the AP updated the WMS process.
Next-update	Interval between the last update and the next scheduled update.
N-updates	Number of updates sent to the WMS process.
Last-ack	Number of timer ticks since the AP received an acknowledgement from the WMS process.
Type	Type of RTLS server used by the AP, such as MMS or Aeroscout.
Server IP	IP address of the RTLS server.
Port	Port used by the RTLS server.
Frequency	Rate, in seconds, at which RTLS messages are sent to the server.
Active	Indicates if the server is active on the AP.
Rpt-Tags	Displays whether tag reporting is enabled or not.
Tag-Mcast-Addr	Displays MAC OUI of the tags that are forwarded to the server.

Column	Description
`Tags-Sent`	Displays the cumulative count of the tag reports sent to server.
`Rpt-Sta`	Displays whether station reporting is enabled or not.
`Incl-Unassoc-Sta`	Displays whether unassociated stations are included in station reporting or not.
`Sta-Sent`	Displays cumulative count of station reports sent to server.
`Cmpd-Msgs-Sent`	Displays cumulative count of compound messages containing station reports sent to server.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap monitor stats

```
show ap monitor stats advanced {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>} client-mac <client-mac>

show ap monitor stats {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}||{ip6-addr <ip6-addr>} mac <mac>
```

Description

Show packet, signal and channel statistics for an AP or a client.

Syntax

Parameter	Description
`advanced`	Show advanced statistics for an AP or client.
`ap-name <ap-name>`	Show statistics for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show data for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.
`mac <mac>`	Show data for a specific MAC address by entering the MAC address of a client or AP.
`client-mac <client-mac>`	Show data for a specific client MAC address by entering the MAC address of a client.

Example

The output of the following command shows monitoring statistics for the AP al12, and a client with the MAC address 00:03:2a:02:6a:d7.

```
(host) #show ap monitor stats ap-name al12 mac 00:03:2a:02:6a:d7

Aggregate Stats
---------------
retry  low-speed  non-unicast  recv-error  frag  bwidth
-----  ---------  -----------  ----------  ----  ------
0      0          0            0           0     0
RSSI
----
avg-signal  low-signal  high-signal  count  duration (sec)
----------  ----------  -----------  -----  --------------
51          51          51           4      50
Monitored Time:6626
Last Packet Time:585500
Uptime:585502

DoS Frames
----------
tx  old-tx  rx  old-rx
```

```
--  ------  --  ------
0   0       0   0
Interference Baseline
---------------------
FRR  FRER
---  ----
17   4
Handoff Assist
--------------
rssi-index  cur-signal  old-cur-signal
----------  ----------  --------------
0           51          0
High Throughput Parameters
--------------------------
ht-type  primary-channel  sec-channel  gf-supported  40mhz-intolerance
-------  ---------------  -----------  ------------  -----------------
none     0                0            0             0
```

The output of this command includes the following information:

Column	Description
retry	Percent of 802.11 retry frames sent because a client failed to send an ACK.
Low-speed	Percent of frames sent at a data rate of 18 Mbps or slower.
non-unicast	Percent of non-unicast frames
recev-error	Percent of error frames of all frames seen in the last second.
frag	Rate of fragmented packets, in frames per second
bwth	Current bandwidth, in bps.
avg-signal	Average signal-to-noise ratio over the interval since the AP's last reset.
Low-signal	Lowest signal-to-noise ratio over the interval since the AP's last reset.
high-signal	Highest signal-to-noise ratio over the interval since the AP's last reset.
count	Number of packets seen on the AP over the interval since the AP's last reset.
Duration	Time over which the AP has measured RSSI values.
tx	The total number of deauthorization frames sent to this MAC address for containment in the interval from the AP's last reset until the current timer tick.
old-tx	The total number of deauthorization frames sent to this MAC address for containment until the previous timer tick.
rx	The total number of deauthorization frames spoofing the MAC address in the interval from the AP's last reset until the current timer tick.
old-rx	The total number of deauthorization frames sent to this MAC address for containment until the previous timer tick.
FRR	Frame retry rate, in frames per second.
FRER	Frame error retry rate, in frames per second.

Column	Description
rssi-index	This value indicates the number of consecutive timer ticks over which the value of the Receive Signal Strength Indicator (RSSI) of the client has reduced by more than 3 units. **NOTE:** This value is updated only if 'handoff-assist' is enabled in the AP's RF Optimization profile.
cur-signal	The Receive Signal Strength Indicator (RSSI) of the most recent frame received from the specified MAC address.
old-cur-signal	The most recent Receive Signal Strength Indicator (RSSI) of the MAC which is 3 lower or 5 higher than the current RSSI. **NOTE:** This value is updated only if 'handoff-assist' is enabled in the AP's RF Optimization profile
ht-type	This parameter indicates support for the following HT types: **no**: No support for high-throughput. **HT-20**: Support for 20 Mhz high-throughput only. **HT-40**: Support for 40 Mhz high-throughput.
primary-channel	Primary radio channel.
sec-channel	Secondary radio channel
gf-supported	If **1**, this AP supports greenfield mode. If **0**, greenfield is not supported.
40mhz-intolerance	Indicates whether the specified MAC address is 40 Mhz intolerant.

Command History

Command	Description
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap multizone-profile

```
show ap multizone-profile <profile-name>
```

Description

This command displays an AP multizone profile.

Syntax

No syntax.

Examples

The output of the command displays the multizone profile and also provides the number of datazones and number of virtual APs available in the primary zone.

```
(host) (config) ##show ap multizone-profile MZoneProfile

Multizone Enabled

Datazone Table
--------------
Zone  IP Address   Max Vaps Allowed  Max Nodes Allowed
----  ----------   ----------------  -----------------
1     10.15.144.3  3                 2
2     10.15.144.5  3                 2

Number of datazones:2

Number of vaps available in primary zone:10 (or 2 for APs with max 8 ssids)

Number of nodes available in primary zone:8
```

Command History

Release	Modification
ArubaOS 8.0.1.0	The **num-nodes** sub-parameter was introduced.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on managed devices

show ap packet capture

```
show ap pcap status {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the status of outstanding packet capture (pcap) sessions.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

The Packet Capture (pcap) feature copies control path packets from the Aruba Control Processor, providing visibility for packets to or from the controller. This provides a useful troubleshooting tool for diagnosing communication problems with elements such as a Radius server. You can retrieve these packets by issuing the command **tar logs**, and then viewing the file filter.pcap on the controller's flash drive.

Example

The example below shows the Packet Capture Sessions table for an AP named AP16.

```
(host) #show ap pcap status ap-name AP16
Packet Capture Sessions
-----------------------
pcap-id  filter  type  intf              channel max-pkt-size  num-pkts  status       url
target
-------  ------  ----  ----              ------- ------------  --------  ------       ---  --
----
1                raw   00:1a:1e:82:ab:b0  161
                                        in-progress       10.3.9.225/5555
```

The output of this command includes the following information:

Column	Description
`pcap-id`	ID number of the packet capture session.
`filter`	Packet Capture filter specification.
`type`	A **raw** packet capture type indicates that the controller is streaming raw packets to an external viewer.
`intf`	BSSID of the interface for the PCAP session.
`channel`	Channel used by AP to capture packets.

Column	Description
`max-pkt-size`	Maximum size of all captured packets.
`num-pkts`	Number of packets captured during the session.
`status`	Shows the current status of the packet-capture session.
`url`	Packet capture data can be downloaded to this URL
`target`	IP address of the client station running Wildpacket's AiroPeek monitoring application

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap papi-err

```
show ap papi-err {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Show PAPI error messages.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show data for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.

Examples

The output of the command displays the status.

```
(host) #show ap papi-err
STM SAP PAPI Send Error
-----------------------
Name  bssid  ip  Tunnel Add  Tunnel Remove  Arp Req  Vlan Req  Sta Req  Mcast Req
----  -----  --  ----------  -------------  -------  --------  -------  ---------
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap port status

```
ap-name <ap-name>
bssid <bssid>
ip-addr <ip-addr>
ip6-addr <ip6-addr>
wired-mac <wired-mac>
```

Description

Shows the status of the AP's wired ports. The status is updated every 60 seconds.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the AP.
`bssid <bssid>`	BSSID of the AP.
`ip-addr <ip-addr>`	IP address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.
`wired-mac <wired-mac>`	MAC address of the AP.

Examples

The output of the command displays the wired port status of an AP named **LocalAP1**. In this example, the output is divided into multiple sections to fit better on the pages of this document. In the actual CLI, it appears in a single long table.

```
(host) #show ap port status ap-name LocalAP1

AP "LocalAP1" Port Status (updated every 60 seconds)
----------------------------------------------------
Port  MAC                Type  Forward Mode  Admin     Oper  Speed     Duplex  802.3az  PoE
----  ---                ----  ------------  -----     ----  -----     ------  -------  ---
0     00:1a:1e:10:05:1a  GE    N/A           enabled   up    1 Gb/s    full    N/A      N/A
1     00:1a:1e:10:05:1b  FE    tunnel        enabled   up    100 Mb/s  full    N/A      N/A
2     00:1a:1e:10:05:1c  FE    tunnel        enabled   down  N/A       N/A     N/A      N/A
3     00:1a:1e:10:05:1d  FE    N/A           disabled  down  N/A       N/A     N/A      N/A

STP         TX-Packets  TX-Bytes  RX-Packets  RX-Bytes
---         ----------  --------  ----------  --------
N/A         23697       3338307   27449       8471871
Forwarding  12185       6593226   18436       1758272
Disabled    0           0         0           0
Off         0           0         0           0
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap profile-usage

```
show ap profile-usage {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>}
```

Description

Show a complete list of all profiles referenced by an individual AP or an AP BSSID.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

Use this command to monitor the configuration profiles in use by an AP or a specific BSSID. The output of this command shows the name of each profile type that is associated with the AP or BSSID, as well as the source that associates the profile with the AP.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap provisioning

```
show ap provisioning {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show provisioning parameters currently used by an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address.

Example

```
The output of this command shows that the AP named AP8 has mostly default parameters. These
appear with the value N/A.
(host) #show ap provisioning ap-name AP8
AP "mp2" Provisioning Parameters
--------------------------------
Item                            Value
----                            -----

(host) (config) #show ap provisioning ap-name 00:24:6c:c7:d5:c8

AP "00:24:6c:c7:d5:c8" Provisioning Parameters
----------------------------------------------
Item                                                                    Value
----                                                                    -----
AP Name                                                                 00:24:6c:c7:d5:c8
AP Group                                                                default
Location name                                                           N/A
SNMP sysLocation                                                        N/A
Master                                                                  10.4.62.9
Gateway                                                                 N/A
IPv6 Gateway                                                            N/A
Netmask                                                                 N/A
IP Addr                                                                 N/A
IPv6 Addr                                                               N/A
IPv6 Prefix                                                             64
DNS IP                                                                  N/A
DNS IPv6                                                                N/A
Domain Name                                                             N/A
Server Name                                                             aruba-master
Server IP                                                               10.4.62.9
Antenna gain for 802.11a                                                N/A
Antenna gain for 802.11g                                                N/A
Antenna for 802.11a                                                     both
Antenna for 802.11g                                                     both
Single chain mode for Radio 0                                           0
Single chain mode for Radio 1                                           0
IKE PSK                                                                 N/A
PAP User Name                                                           N/A
```

```
PAP Password                                                    N/A
PPPOE User Name                                                 N/A
PPPOE Password                                                  N/A
PPPOE Service Name                                              N/A
PPPOE CHAP Secret                                               N/A
USB User Name                                                   N/A
USB Password                                                    N/A
USB Device Type                                                 any
...
...
...
```

The output of this command includes the following information:

Column	Description
AP Name	Name of the AP.
AP Group	AP group to which the AP belongs.
Location name	Fully-qualified location name (FQLN) for the AP.
SNMP sysLocation	User-defined description of the location of the AP, as defined with the command provision-ap syslocation.
Master	Name or IP address for Mobility Master.
Gateway	IP address of the default gateway for the AP.
Netmask	Netmask for the AP's IP address.
IP Addr	IP address for the AP.
IPv6	The static IP6 address of the AP.6
IPv6 Prefix	The prefix of static IPv6 address of the AP.
Dns IP	IP address of the DNS server.
DNS IPv6	The prefix of static IPv6 address of the AP.
Domain Name	Domain name used by the AP.
Server Name	DNS name of the managed device from which the AP boots.
Server IP	IP address of the managed device from which the AP boots
Antenna gain for 802.11a	Antenna gain for 802.11a (5GHz) antenna.
Antenna gain for 802.11g	Antenna gain for 802.11g (2.4GHz) antenna.
Antenna for 802.11a	Antenna use for 5 GHz (802.11a) frequency band. ■ **1**: AP uses antenna 1 ■ **2**: AP uses antenna 2 ■ **both**: AP uses both antennas

Column	Description
Antenna for 802.11g	Antenna use for 2.4 GHz (802.11g) frequency band. ■ **1**: AP uses antenna 1 ■ **2**: AP uses antenna 2 ■ **both**: AP uses both antennas
Single chain mode for Radio 0	If this parameter is set to 1 for an 802.11n-capable radio, the radio will operate in single-chain mode, and will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This parameter is set to 0 (disabled) by default.
Single chain mode for Radio 1	If this parameter is set to 1 for an 802.11n-capable radio, the radio will operate in single-chain mode, and will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This parameter is set to 0 (disabled) by default.
IKE PSK	IKE PSK The IKE pre-shared key.
PAP password	Password Authentication Protocol (PAP) password for the AP.
PAP User Name	PAP username for the AP.
PPPOE User Name	Point-to-Point Protocol over Ethernet (PPPoE) user name for the AP.
PPPOE Password	PPPoE password for the AP.
PPPOE Service Name	PPPoE service name for the AP.
PPPOE CHAP secret	PPPoE CHAP secret key for the AP.
USB User Name	The PPP username provided by the cellular service provider
USB Password	A PPP password, if provided by the cellular service provider
USB Type	The USB driver type.
USB Device Identifier	The USB device identifier.
USB Dial String	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.
USB Initialization String	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.
USB TTY device data path	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.
USB TTY device control path	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.
Uplink VLAN	If you configured an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature.
Link Priority Ethernet	Set the priority of the wired uplink, from 0-255. Each uplink type has an associated priority; wired ports having the highest priority by default.

Column	Description
`Link Priority Cellular`	The priority of the cellular uplink, from 0-255. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link.
`Mesh Role`	If the mesh role is "none," the AP is operating as a thin AP. An AP operating as a mesh node can have one of two roles: mesh portal or mesh point.
`Installation`	Indicates the type of installation (**indoor** or **outdoor**). The **default** parameter indicates that the installation mode is determined by the AP model type.
`Latitude`	Latitude coordinates of the AP, in the format *Degrees Minutes Seconds* (DMS).
`Longitude`	Longitude coordinates of the AP, in the format *Degrees Minutes Seconds* (DMS).
`Altitude`	Altitude, in meters, of the AP. This parameter is supported on outdoor APs only.
`Antenna bearing for 802.11a`	Horizontal coverage distance of the 802.11a (5GHz) antenna from true north, from 0-360 degrees. **NOTE:** This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
`Antenna bearing for 802.11g`	Horizontal coverage distance of the 802.11g (2.4GHz) antenna from true north, from 0-360 degrees. **NOTE:** This parameter is supported on outdoor APs only. The horizontal coverage pattern does not consider the elevation or vertical antenna pattern.
`Antenna tilt angle for 802.11a`	The angle of the 802.11a (5GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
`Antenna tilt angle for 802.11g`	The angle of the 802.11g (2.4GHz) antenna. This parameter can range from between -90 degrees and 0 degrees for downtilt, and between +90 degrees and 0 degrees for uptilt.
`Mesh SAE`	Shows if the AP has enabled or disabled Secure Attribute Exchange (SAE) on a mesh network.

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.
ap provisioning-profile	This command defines a provisioning profile for an AP or group of APs.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap provisioning-profile

```
show ap provisioning-profile [<profile-name>]
```

Description

This command shows information for AP provisioning profiles.

Syntax

Parameter	Description
<profile-name>	The name of an existing AP provisioning profile.

Usage Guidelines

The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group via the command **ap-group <group> provisioning-profile <profile>**.

Issue this command without the **<profile-name>** option to display the entire AP provisioning profile list, including profile status and the number of references to each profile. Include a profile name to display the authorization group defined for that profile.

Examples

The following example lists all AP provisioning profiles. The **References** column lists the number of other profiles with references to that provisioning profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined AP provisioning profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] #show ap provisioning-profile

Provisioning profile List
-------------------------
Name     References  Profile Status
----     ----------  --------------
default  12
outdoor  3
```

To display the configuration settings for an individual profile, include the <profile> parameter. The example below shows the profile details for the AP provisioning profile **Default**.

```
(host) [mynode] #show ap provisioning-profile default

Provisioning profile "default"
------------------------------
Parameter                                                  Value
---------                                                  -----
Remote-AP                                                  No
Master IP/FQDN                                             N/A
PPPOE User Name                                            N/A
PPPOE Password                                             N/A
PPPOE Service Name                                         N/A
USB User Name                                              N/A
USB Password                                               N/A
USB Device Type                                            none
USB Device Identifier                                      N/A
USB Dial String                                            N/A
USB Initialization String                                  N/A
```

```
USB TTY device data path                                          N/A
USB TTY device control path                                       N/A
USB modeswitch parameters                                         N/A
Link Priority Ethernet                                            0
Link Priority Cellular                                            0
Cellular modem network preference                                 auto
Username of AP so that AP can authenticate to 802.1X using PEAP   N/A
Password of AP so that AP can authenticate to 802.1X using PEAP   N/A
Uplink VLAN                                                       0
USB power mode                                                    auto
AP POE Power optimization                                         disabled
```

Description

This command defines a provisioning profile for an AP or group of APs.

Syntax

Parameter	Description
`Remote-AP`	Indicates that the profile is associated with a remote AP using certificates.
`Master IP/FQDN`	The FQDN or IP address for Mobility Master.
`PPPOE User Name`	PPPoE username for the AP.
`PPPOE Password`	Point-to-Point Protocol over Ethernet (PPPoE) password for the AP.
`PPPOE Service Name`	PPPoE service name for the AP.
`USB User Name`	The PPP username provided by the cellular service provider
`USB Password`	A PPP password, if provided by the cellular service provider
`USB Device Type`	The USB driver type.
`USB Device Identifier`	The USB device identifier.
`USB Dial String`	The dial string for the USB modem. This parameter only needs to be specified if the default string is not correct.
`USB Initialization String`	The initialization string for the USB modem. This parameter only needs to be specified if the default string is not correct.
`USB TTY device data path`	The TTY device path for the USB modem. This parameter only needs to be specified if the default path is not correct.
`USB TTY device control path`	The TTY device control path for the USB modem. This parameter only needs to be specified if the default path is not correct.
`USB modeswitch parameters`	All the parameters that is required to be passed to the USB mode switch utility.
`Link Priority Ethernet`	Set the priority of the wired uplink, from 0-255. Each uplink type has an associated priority; wired ports having the highest priority by default.

Parameter	Description
`Link Priority Cellular`	The priority of the cellular uplink, from 0-255. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link.
`Cellular modem network preference`	Multi-mode cellular modem network preference type.
`Username of AP so that AP can authenticate to 802.1X using PEAP`	If your AP uses PEAP authentication, this field displays the AP username.
`Password of AP so that AP can authenticate to 802.1X using PEAP`	If your AP uses PEAP authentication, this field displays the AP password.
`Uplink VLAN`	If you configured an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. By default, an AP has an uplink vlan of 0, which disables this feature.
`USB power mode`	The USB power mode to control the power to the USB port.
`AP POE Power optimization`	Displays the AP POE power optimization status.

Usage Guidelines

The AP provisioning profile allows you to define a set of provisioning parameters to an AP group. These settings can be saved or assigned to an AP group via the command **ap-group <group> provisioning-profile <profile>**.

Related Commands

Command	Description
provision-ap	Change provisioning parameters for an individual AP. This command does not save the provisioning parameters settings in a reusable profile.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap radio-database

```
show ap radio-database [band a|g] [group <group>] [mode access-point|air-
monitor|disabled|ht|ht-40mhz|legacy|sap-monitor] [sort-by ap-group|ap-ip|ap-name|ap-
type|switch-ip] [sort-direction ascending|descending] [start <start>] [switch <switch-ip-
addr>]
```

Description

Show radio information for Access Points visible to this controller.

Syntax

Parameter	Description
band	Show only APs with a radio operating in the specified band.
a	Show only APs with a radio operating in the 802.11a band (5 GHz).
g	Show only APs with a radio operating in the 802.11g band (2.4 GHz).
group <group>	Show only APs associated with the specified AP group.
mode	Show only APs with a radio operating in the specified mode.
access-point	Show only APs operating as access points.
air-monitor	Show only APs operating as air monitors.
disabled	Show only disabled APs.
ht	Show only high-throughput APs.
ht-40mhz	Show only 40 Mhz high-throughput APs.
legacy	Show only legacy (not high-throughput) APs.
sap-monitor	Show only APs operating as SAP monitors.
sort-by	Sort the output of this command by a specific data column.
ap-group	Sort the output of this command by AP group name.
ap-ip	Sort the output of this command by AP IP address.
ap-name	Sort the output of this command by AP name.
ap-type	Sort the output of this command by AP model type.
switch-ip	Sort the output of this command by controller ip address.
sort-direction	Select a sort direction for the output of this command.
ascending	Sort the output in ascending order.
descending	Sort the output in descending order.

Parameter	Description
start	Start displaying the output of this command at a chosen index number by entering the index number of the AP at which command output should start.
switch <switch-ip-addr>	Display information for APs associated with a specific controller by entering the IP address of that controller.

Example

The output of the command shows that the AP is aware of five other access points, three of which are active.

```
(host) #show ap radio-database
AP Radio Database
-----------------
Name             Group    AP Type  IP Address   Status          Flags  Switch IP     11g
Mode/Chan/EIRP/Cli  11a Mode/Chan/EIRP/Cli
----             -----    -------  ----------   ------          -----  ---------     ----------
------------  ----------------------
mp3              default  125      10.3.129.96  Up 14h:45m:0s   M      10.3.129.232  AP(HT)
/10/0/0            AP(HT)/100/4/0
sw-ad-ap124-11   default  124      10.3.129.99  Up 14h:43m:18s  M      10.3.129.232  AP(HT)
/10/0/0            AP(HT)/100+/2/0
sw-ad-ap125-13   default  125      10.3.129.98  Up 14h:49m:36s  M      10.3.129.232  AP(HT)
/10/2.5/0          AP(HT)/100/4/0
sw-ad-ap65-19    default  65       10.3.129.95  Down                   10.3.129.232

   Flags: U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed
          R = Remote AP; I = Inactive; X = Maintenance Mode; P = PPPoE AP; B = Built-in AP
          S = RFprotect Sensor; d = Disconnected Sensor; H = Using 802.11n license
       M = Mesh node; Y = Mesh Recovery
```

The output of this command includes the following information:

Column	Description
Name	Name of the AP.
Group	AP group to which the AP is associated.
AP Type	AP model type.
IP address	IP address of the AP.
Status	Current AP status. If the AP is currently up, this data column also shows the amount of time for which the AP has been active.
Flags	This column displays a letter that corresponds to some type of additional information for the AP. The key to the list of possible flags appears at the bottom of the output of this command.
Switch IP	IP address of the AP's controller.
11g Mode/Chan/EIRP/Cli	802.1g radio type and mode/802.11g radio channel used by the AP/current Effective Isotropic Radiated Power (EIRP)/Number of Clients associated with the radio
11a Mode/Chan/EIRP/Cli	802.1a radio type and mode/802.11a radio channel used by the AP/current Effective Isotropic Radiated Power (EIRP)/Number of Clients associated with the radio.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap radio-summary

```
show ap radio-summary
   ap-group <ap-group>
   ap-name <ap-name>
   dot11a
   dot11g
   ip-addr <ip-addr>
   ip6-addr <ip6-addr>
```

Description

Show AP radios registered to this controller.

Syntax

Parameter	Description
`ap-group`	Allows you to filter radio information by AP group.
`ap-name <ap-name>`	Allows you to filter radio information by AP name.
`dot11a`	Allows you to filter 802.11a radio information.
`dot11g`	Allows you to filter 802.11g radio information.
`ip-addr <ip-addr>`	Allows you to filter radio information by IP address.
`ip6-addr <ip-addr>`	Allows you to filter radio information by IPv6 address.

Example

The output of the command in the example below displays statistics for the AP's radio, as well as statistics for transmitted and received frames.

In the actual CLI, it will appear in a single, long table.

```
(host) [mynode] #show ap radio-summary
APs Radios information
----------------------
Name              Group               AP Type  IP Address     Band  Mode
----              -----               -------  ----------     ----  ----
172.17.153-7      172.17.153          104      55.55.57.44    2.4   AP:1
172.17.150-5      172.17.150          104      55.55.57.42    2.4   AP:6
172.17.153-13     172.17.153          104      55.55.57.35    2.4   AP:6
172.17.151-42     172.17.151          104      55.55.57.34    2.4   AP:11
172.17.151-34     172.17.151          104      55.55.57.33    2.4   AP:11
172.17.155-26     172.17.155          104      55.55.57.22    2.4   AP:1

EIRP/MaxEIRP  NF/U/I        TD                 TM                 TC
------------  ------        --                 --                 --
28/29.5       -96/ 67/  5   0/0/0/0/0/0        33/33/33/32/32/32  0/0/0/0/0/0
29.5/29.5     -96/ 27/  3   0/0/0/0/0/0        12/11/12/12/12/11  0/0/0/0/0/0
29.5/29.5     -96/ 31/  3   0/0/0/0/0/0        13/13/14/14/12/14  0/0/0/0/0/0
25/29.5       -96/ 28/  6   0/0/0/0/0/0        10/10/10/9/11/10   0/0/0/0/0/0
25/29.5       -96/ 32/  7   0/0/0/0/0/0        10/11/11/10/11/11  0/0/0/0/0/0
28/29.5       -96/ 70/  4   0/0/0/0/0/0        27

NF: Noise Floor(dBm); U: Utilization(%); I: Interference(%)
```

```
TD: Time used by data frames (%); TM: time used by mgnt frames(%); time used by ctrl frames
(%)
Total Radios:6
```

The output of this command includes the following information:

Parameter	Description
`Name`	Name of the AP.
`Group`	Group to which AP radio is assigned.
`AP Type`	AP model.
`IP Address`	Radio IP address.
`Band`	Band on which radio is operating on (2.4 or 5 GHz).
`Mode`	Mode on which radio is operating; AP: AP Mode; AM: Air Monitor Mode, Spectrum: Spectrum Monitor Mode. Optionally, you can also specify the channel number.
`EIRP/Max EIRP`	Current EIRP output and maximum EIRP allowed for this radio (dBm).
`NF/U/I`	Noise Floor (dBm) / Utilization (%) / Interference (%).
`TD`	Time used by data frames (%).
`TM`	Time used by mgmt frames(%).
`TC`	Time used by ctrl frames (%).

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap regulatory

```
show ap regulatory
```

Description

Shows the currently active Regulatory Cert.

Syntax

None.

Usage Guidelines

Issue this command to view the currently active Regulatory Cert

Examples

The example below shows the version of Regulatory Cert currently active on the controller.

```
(host) [mynode] #show ap regulatory
Regulatory Version :1.0_43859
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap regulatory-domain-profile

```
show ap regulatory-domain-profile [<profile-name>]
```

Description

Show the list of regulatory domain profiles, or the settings in an individual regulatory domain profile

Syntax

Parameter	Description
<profile-name>	Show data for a specific regulatory domain profile

Usage Guidelines

Issue this command without the **<profile>**parameter to display the entire regulatory domain profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three regulatory domain profiles. The **References** column lists the number of other profiles with references to the regulatory domain profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) [mynode] # show ap regulatory-domain-profile
Regulatory Domain profile List
------------------------------
Name                            References  Profile Status
----                            ----------  --------------
corp-channel-profile            8
default                         10
channel-test                           1.
```

This example displays the configuration settings for the profile **corp-channel-profile**. The output of this command shows the profile's country code and the valid channel and channel pairs for that profile.

```
host) #show ap regulatory-domain-profile corp-channel-profile
Regulatory Domain profile "corp-channel-profile"
-------------------------------------------------
Parameter                       Value
---------                       -----
Country Code                    US
Valid 802.11g channel           1
Valid 802.11g channel           6
Valid 802.11a channel           36
Valid 802.11a channel           40
Valid 802.11a channel           44
Valid 802.11a channel           48
Valid 802.11a channel           149
Valid 802.11a channel           153
Valid 802.11g 40MHz channel pair  N/A
Valid 802.11a 40MHz channel pair  36-40
Valid 802.11a 40MHz channel pair  44-48
Valid 802.11a 40MHz channel pair  149-153
Valid 802.11a 80MHz channel group 36-48
```

```
Valid 802.11a 80MHz channel group 52-64
Valid 802.11a 80MHz channel group 100-112
Valid 802.11a 80MHz channel group 116-128
Valid 802.11a 80MHz channel group 132-144
Valid 802.11a 80MHz channel group 149-161
```

The output of this command includes the following information:

Column	Description
`Country Code`	Code that represents the country in which the APs will operate. The country code determines the 802.11 wireless transmission spectrum.
`Valid 802.11g channel`	Selected 802.11b/g channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the profile's country code.
`Valid 802.11a channel`	Selected 802.11a channel available for use by an AP using the specified regulatory domain profile. These channels are limited to those valid for the country code.
`Valid 802.11g 40MHz channel pair`	Selected 802.11b/g 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.
`Valid 802.11a 40MHz channel pair`	Selected 802.11a 40 MHz channel pair available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.
`Valid 802.11a 80MHz channel group`	Selected 802.11a 80 MHz channel group available for use by an AP using the specified domain profile. These channels are limited to those valid for the profile's country code.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show ap remote auth-trace-buf

```
show ap remote auth-trace-buf {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
```

Description

This command shows authentication trace buffer on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows authentication trace buffer on an AP for specified AP name.
`bssid <bssid>`	Shows authentication trace buffer on an AP for specified BSSID.
`ip-addr <ip-addr>`	Shows authentication trace buffer on an AP for specified IP address.
`ip6-addr <ip6-addr>`	Shows authentication trace buffer on an AP for specified IPv6 address.

Usage Guidelines

This command shows authentication trace buffer on an AP. For the remaining parameters, see the command syntax.

Example

The following example shows authentication trace buffer on an AP named ap-205:

```
(host) [mynode] #show ap remote auth-trace-buf ap-name ap-205

Auth Trace Buffer
-----------------
```

Command History:

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap remote blacklist-clients

```
show ap remote blacklist-clients [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>]
```

Description

This command shows all clients blacklisted.

Syntax

Parameter	Description	Range	Default
`ap-name <ap-name>`	Shows all blacklisted clients filtered by AP name.	—	—
`bssid <bssid>`	Shows all blacklisted clients filtered by BSSID.	—	—
`ip-addr <ip-addr`	Shows all blacklisted clients filtered by IP address.	—	—

Usage Guidelines

This command shows all blacklisted clients. For the remaining parameters, see the command syntax.

Example

The following example shows all blacklisted clients:

```
(host) [mynode] #show ap remote blacklist-clients ap-name ap-205

Blacklisted Clients
-------------------
STA  reason  block-time(sec)  remaining time(sec)  Flags
---  ------  ---------------  -------------------  -----

Flags: R: reject associations
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap remote blacklist-clients-driver

```
show ap remote blacklist-clients-driver [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>]
```

Description

This command shows all clients blacklisted in the driver.

Syntax

Parameter	Description	Range	Default
`ap-name <ap-name>`	Shows all clients blacklisted in the driver filtered by AP name.	—	—
`bssid <bssid>`	Shows all clients blacklisted in the driver filtered by BSSID.	—	—
`ip-addr <ip-addr`	Shows all clients blacklisted in the driver filtered by IP address.	—	—
`ip6-addr <ip6-addr`	Shows all clients blacklisted in the driver filtered by IPv6 address.	—	—

Usage Guidelines

This command shows all clients blacklisted in the driver. For the remaining parameters, see the command syntax.

Example

The following example shows all clients blacklisted in the driver:

```
(host) [mynode] #show ap remote blacklist-clients-driver ap-name ap-205

Clients Blacklisted in Driver
-----------------------------
STA
---
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap remote bss-table

```
show ap remote bss-table [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>] [ip6-addr
<ip6-addr>]
```

Description

This command shows BSSIDs of all APs registered on the managed device.

Syntax

Parameter	Description	Range	Default
`ap-name <ap-name>`	Shows BSSIDs of all APs registered on the managed device filtered by AP name.	—	—
`bssid <bssid>`	Shows BSSIDs of all APs registered on the managed device filtered by BSSID.	—	—
`ip-addr <ip-addr`	Shows BSSIDs of all APs registered on the managed device filtered by IP address.	—	—
`ip6-addr <ip6-addr>`	Shows BSSIDs of all APs registered on the managed device filtered by IPv6 address.	—	—

Usage Guidelines

This command shows BSSIDs of all APs registered on the managed device. For the remaining parameters, see the command syntax.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows BSSIDs of all APs registered on the managed device:

```
(host) [mynode] #show ap remote bss-table ap-name ap-205

Aruba AP BSS Table
------------------
bss                ess            port  ip               phy
---                ---            ----  --               ---
40:e3:d6:76:19:70  aruba-ap       ?/?   191.191.191.252  a-VHT
40:e3:d6:76:19:71  guestthistime  ?/?   191.191.191.252  a-VHT
40:e3:d6:76:19:60                 ?/?   191.191.191.252  g-HT

type  ch/EIRP/max-EIRP  cur-cl  ap name  in-t(s)  tot-t
----  ----------------  ------  -------  -------  -----
ap    149E/12/24        0       ap-205   0        19d:13h:46m:14s
ap    149E/12/24        0       ap-205   0        19d:13h:46m:14s
am    ?/?/?             0       ap-205   0        19d:13h:46m:13s

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:3
Num Associations:0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap remote client status

```
show ap remote client status [ap-name <ap-name>] [bssid <bssid>] [ip-addr <ip-addr>] [ip6-addr <ip6-addr>] <client-mac>
```

Description

This command shows association state of clients.

Syntax

Parameter	Description	Range	Default
`ap-name <ap-name>`	Shows association state of clients filtered by AP name.	—	—
`bssid <bssid>`	Shows association state of clients filtered by BSSID.	—	—
`ip-addr <ip-addr`	Shows association state of clients filtered by IP address.	—	—
`ip6-addr <ip6-addr`	Shows association state of clients filtered by IPv6 address.	—	—
`<client-mac>`	MAC address of client.	—	—

Usage Guidelines

This command shows association state of clients. For the remaining parameters, see the command syntax.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows association state of clients:

```
(host) [mynode] #show ap remote client status ap-name ap-205 00:1a:1e:aa:bb:cc
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ap remote counters

```
show ap remote counters {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
```

Description

Show the numbers of message counters for Remote APs

Syntax

Parameter	Description
`ap-name <ap-name>`	Show data for an AP with a specific name.
`bssid <bssid>`	Show data for a specific Basic Service Set Identifier (BSSID) on an AP. You must specify an AP's BSSID, which is usually the AP's MAC address
`ip-addr <ip-addr>`	Show data for an AP with a specific IP address.

Examples

Use this command to determine the number of message counters recorded for each counter type seen by the remote AP. The output of the command in the example below shows counters for Remote AP State and VoIP CAC State Announcements.

```
(host) #show ap remote counters ap-name al22

Counters
--------
Name                          Value
----                          -----
Remote AP State               62851
VoIP CAC State Announcement   13605
```

The output of this command includes the following information:

Column	Description
`Name`	Name of the counter type.
`Value`	Number of counters recorded since the AP was last reset.

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ap remote debug anul-sta-entries

```
show ap remote debug anul-sta-entries {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

Displays a list of VAPs and stations stored in the AP's datapath.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show LACP information for an AP with a specific name.
`radio <radio>`	Shows the radio ID. Valid values are 0 and 1.
`ip-addr <ip-addr>`	Show LACP information for an AP with a specific IPv4 address.
`ip6-addr <ip6-addr>`	Show LACP information for an AP with a specific IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example 1

Using the following example, for 320 Series check LAG columns to see if any packets are dropped.

```
#show ap remote  debug anul-sta-entries ap-name ap325
ANUL BSS Table for Radio 0
--------------------------
bssid              num_stas  data ready drops
-----              --------  ----------------
AC:A3:1E:53:5C:F0  2         0
ANUL STA State
--------------
mac                bssid              aid  data ready  bss  Drops  LAG  LAG drops
---                -----              ---  ----------  ---  -----  ---  ---------
3C:A9:F4:24:B2:54  AC:A3:1E:53:5C:F0  2    Yes         B    0      Yes  0
78:31:C1:BC:D6:12  AC:A3:1E:53:5C:F0  1    Yes         B    0      Yes  0
```

The following parameters appear in the output of the **show ap remote debug anul-sta-entries** command, and are useful for debugging purposes.

Parameter	Description
`bssid`	The BSS Id of the VAP.
`num_stas`	Indicates the number of stations associated to a VAP.
`data ready drops`	Indicates the total packets received and dropped before clients were ready to receive data packets.

Parameter	Description
ANUL STA State	
mac	The MAC address of a client.
bssid	The BSS Id of the VAP that the client is associated to.
aid	The association ID of the station.
data ready	Indicates if the client has completed authentication.
bss	Indicates if a client is associated to a BSS or not. The **B** flag indicates that the client is associated to a BSS. The **F** flag indicates that the entry is free and not attached to any BSS.
Drops	Indicates the number of data packets received and dropped before data ready is set to yes.
LAG	Indicates if link aggregation is used to achieve HT by transmitting the packets on both Ethernet ports, for a given station. This field is displayed only in 320 Series access points.
LAG drops	Indicates the number of packets dropped by the AP due to packets reordered in the network by link aggregation. This field is displayed only in 320 Series access points.

Command History

Version	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on managed devices

show ap remote debug association

```
show ap remote debug association
   {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}[uac <uac>]
```

Description

This command shows the association table of the AP to identify the clients associated to each AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows client associations for the specified AP name.
`bssid <bssid>`	Show client associations for an specific BSSID. A BSSID is usually the MAC address of an AP.
`ip-addr <ip-addr>`	Shows client associations for the specified IP address.
`ip6-addr <ip6-addr>`	Shows client associations for the specified IPv6 address.

Usage Guidelines

Use this command to verify if a remote user is connected to an AP and to validate the AP to which is connected.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command displays information about the remote clients associated with an AP with the IP address 192.0.2.32.

```
(host) [mynode] #show ap remote debug association ip-addr 192.0.2.32

Flags: W: WMM client, A: Active, R: RRM client

PHY Details: HT: High throughput; 20: 20MHz; 40: 40MHz
             <n>ss: <n> spatial streams

Association Table
-----------------
Name  bssid              mac               auth  assoc  aid  l-int  essid
----  -----              ---               ----  -----  ---  -----  -----
AP71  00:0a:23:c1:d4:11  00:16:6d:08:1s:f1  y     y      1    10     t-lab

vlan-id  tunnel-id  phy  assoc. time  num assoc  Flags
-------  ---------  ---  -----------  ---------  -----
111      0x108e     a    23s          1          A

Num Clients:1
```

The output of this command includes the following information:

Column	Description
Name	Name of an AP.
bssid	The AP BSSID.
mac	MAC address of the client.
auth	This column displays a **y** if the AP has been configured for 802.11 authorization frame types. Otherwise, it displays an **n**.
assoc	This column displays a **y** if the AP has been configured for 802.11 association frame types. Otherwise, it displays an **n**.
aid	802.11 association ID. A client receives a unique 802.11 association ID when it associates to an AP.
1-int	Number of beacons in the 802.11 listen interval. There are ten beacons sent per second, so a ten-beacon listen interval indicates a listen interval time of 1 second.
essid	Name that uniquely identifies the AP's ESSID.
vlan-id	Identification number of the AP's VLAN.
tunnel-id	Identification number of the AP's tunnel.
phy	The RF band in which the AP operates: **a** = 5 GHz **b**, **g** = 2.4 GHz
assoc. time	Amount of time the client has associated with the AP, in the format hours:minutes:seconds.
num assoc	Number of clients associated with the AP.
flags	This column displays any flags for this AP. The list of flag abbreviations is included in the output of the **show ap association** command.

Command History:

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on managed devices

show ap remote debug association-failure

```
show ap remote debug association-failure
   {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}[client-mac <client-
   mac>|essid <essid>]
```

Description

This command shows the association failure information.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows AP association failure for the specified AP name. You may include the **client-mac** or **essid** to filter the output.
`bssid <bssid>`	Shows AP associations for the specified BSSID. A BSSID is usually the MAC address of an AP.
`ip-addr <ip-addr>`	Shows AP associations for the specified IP address. You may include the **client-mac** or **essid** to filter the output.
`ip6-addr <ip6-addr>`	Shows AP associations for the specified IPv6 address. You may include the **client-mac** or **essid** to filter the output.

Usage Guidelines

Use this command to see association failure information.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command displays information about the association failure for an AP named **ap-205**:

```
(host) [mynode] #show ap remote debug association-failure ap-name ap-205

Association Failure Table
-------------------------
MAC Address  AP Name  BSSID  ESSID  State  Radio  Idle Time  Reason
-----------  -------  -----  -----  -----  -----  ---------  ------
Num Association Failures:0
```

Command History:

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on managed devices

show ap remote debug association-failure

```
show ap remote debug association-failure [{ap-name <ap-name>}|{bssid <bssid>}{essid <essid>}]
```

Description

Display association failure information that can be used to troubleshoot problems on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Filter the Association Failure Table by AP name.
`bssid <bssid>`	Filter the Association Failure Table by BSSID. The BSSID is usually the AP's MAC address.
`essid <essid>`	Filter the Association Failure Table by ESSID of an AP.

Usage Guidelines

Use this command to determine whether the client is associated, and identify the last AP to which it was connected.

Example

The output of the command show ap remote debug association-failure displays the Association Failure Table show below. If the **Idle time** column in the output of this command is a low value, **reason** column will describe why association failed.

```
(host)#show ap remote debug association-failure ap-name AP-65-port3
Association Failure Table
-------------------------
MAC Address         AP Name  BSSID              ESSID  State  Radio    Idle Time    Reason
-----------         -------  -----              -----  -----  -----    ---------    ------
00:16:6f:09:54:3e   AL29     00:1a:1e:11:6f:00  guest          802.11g  20h:39m:33s  Denied; AP
Going Down
00:16:6f:09:54:3e   AL33     00:1a:1e:11:6e:60  guest  auth    802.11g             20h:39m:33s
Unspecified Failure
00:16:6f:09:54:3e   AL40     00:1a:1e:8d:5b:20  guest          802.11g  20h:39m:33s  Denied;
Ageout
Num Association Failures:3
```

The output of this command includes the following parameters:

Column	Description
`MAC address`	MAC address of the client that failed to associate with an AP.
`AP Name`	Name of an AP to which the client attempted to associate.
`BSSID`	BSSID of an AP.
`ESSID`	ESSID of an AP.

Column	Description
`State`	This data column shows if the client is currently authorized or both authorized and ESSID associated with an AP.
`Radio`	The AP radio type.
`Idle Time`	Amount of time that the client has been idle, in the format *hours:minutes:seconds*.
`Reason`	A brief description of the reason why the client failed to associate.

Command History

Command	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ap remote debug bss-config

```
show ap remote debug bss-config {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr
<ip6-addr>}
```

Description

Show the configuration for each BSSID of an AP. This information can be used to troubleshoot problems on an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Filter the AP Config Table by AP name.
`bssid <bssid>`	Shows AP associations for the specified BSSID. A BSSID is usually the MAC address of an AP.
`ip-addr <ip-addr>`	Filter the AP Config Table by IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Filter the AP Config Table by IPv6 address by entering an IPv6 address in dotted-decimal format.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

The output of this command shows the AP configuration table for a specific BSSID.

```
host) #show ap remote debug bss-config ap-name ap93-3
Aruba AP Config Table

bss                ess    vlan  ip            phy   type  fw-mode  max-cl  rates tx-rates  preamble  mtu

---                ---    ----  --            ---   ----  -------  ------  ----- --------  --------  --- status
 wmm
------  ---
00:1a:1e:11:24:c2  cera2  66    10.6.1.203    g-HT  ap    tunnel   64      0x3   0xfff     enable    0
enable  enable

00:1a:1e:8d:5b:11  wpa2   65    10.6.1.198    a-HT  ap    tunnel   20      0x150 0xff0     -         0
enable  enable

00:0b:86:9b:e5:60  guest  63    10.6.14.79    g     ap    tunnel   20      0x2   0x3fe     enable    0
enable  enable

00:1a:1e:97:e5:41  voip   66    10.6.1.199    g-HT  ap    tunnel   20      0xc   0x14c     enable    0
enable  enable

00:1a:1e:11:74:a1  voip   66    10.6.1.197    g-HT  ap    tunnel   20      0xc   0x14c     enable    0
enable  enable

00:1a:1e:11:5f:11  wpa2   65    10.6.1.200    a-HT  ap    tunnel   20      0x150 0xff0     -         0
enable  enable
```

The output of this command includes the following information:

Column	Description
bss	BSS identifier, which is usually the AP's MAC address.
ess	ESS identifier; a user-defined name for a wireless network.
vlan	The BSSID VLAN number.
IP	The AP IP address.
phy	One of the following 802.11 types ■ a ■ a-HT ■ g ■ g-HT
type	This column shows if the BSSID is for an AP or an AM.
fw-mode	The configured forward mode for the AP's virtual AP profile. ■ **bridge**: Bridge locally ■ **split-tunnel**: Tunnel to controller or NAT locally ■ **tunnel**: Tunnel to controller
max-cl	The maximum number of clients allowed for this BSSID.
preamble	Shows if short preambles are enabled for 802.11b or 802.11g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using a short preamble.
MTU	MTU size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
status	Shows if this BSSID is enabled or disabled.
wmm	Shows if the BSSID has enabled or disabled WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF) WMM provides prioritization of specific traffic relative to other traffic in the network.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on managed devices

show ap remote debug bucketmap datapath

```
show ap remote debug bucketmap datapath {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr
<ip6-addr>} essid <essid>
```

Description

This command shows bucket maps in AP datapath.

Syntax

Parameter	Description
`ap-name <ap-name> essid <essid>`	Shows bucket maps filtered by specified AP name and ESSID.
`ip-addr <ip-addr> essid <essid>`	Shows bucket maps filtered by specified IP address of an AP and ESSID.
`ip6-addr <ip6-addr> essid <essid>`	Shows bucket maps filtered by specified IPv6 address of an AP and ESSID.

Usage Guidelines

This command shows bucket maps in AP datapath. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to show bucket maps in AP datapath filtered by the AP **test** and ESSID **default**:

```
(host) [mynode] #show ap remote debug bucketmap datapath ap-name test essid default

Essid default radio=0 zone=1 - Num UACs 4
--------------------------------------------------
Index  ArrayIdx  UAC IP       Active AAC  Standby AAC  Num STAs
-----  --------  ------       ----------  -----------  --------
0      0         10.15.146.3  Yes         No           0
1      1         10.15.146.4  No          No           1
2      2         10.15.146.5  No          No           0
3      3         10.15.146.6  No          No           0
Station List
------------
UAC Index  Station Mac        BSSID
---------  -----------        -----
1          80:86:F2:40:14:8D  9C:1C:12:89:5C:9C
Bucket Map
----------
Bucket Idx Range  Bucket Map
----------------  ----------
[0-31]            0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3
[32-63]           0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3
[64-95]           0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3
[96-127]          0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3
[128-159]         0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 3 0
[160-191]         1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3
[192-223]         0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1 3 0 1
[224-255]         0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
-                 Standby Map
[0-31]            1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
```

```
[32-63]           1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
[64-95]           1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1
[96-127]          1 0 1 1 1 0 1 1 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0
[128-159]         3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 0 3 0 0 3
[160-191]         0 0 3 0 0 3 0 0 3 0 0 3 0 0 3 0 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2
[192-223]         3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3 2 3 3
[224-255]         3 3 3 3 3 3 3 3 3 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Statistics:Bmap Updates=0; UAC:Adds=4 Deletes=0; STA:Adds=0 Deletes=494 moves=0 errs=0
copies=0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on managed devices

show ap remote debug bucketmap sapd

```
show ap remote debug bucketmap sapd {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} essid <essid>
```

Description

This command shows bucket map received from cluster by SAPD process.

Syntax

Parameter	Description
`ap-name <ap-name> essid <essid>`	Shows bucket maps received from cluster by SAPD filtered by specified AP name and ESSID.
`ip-addr <ip-addr> essid <essid>`	Shows bucket maps received from cluster by SAPD filtered by specified IP address of an AP and ESSID.
`ip6-addr <ip6-addr> essid <essid>`	Shows bucket maps received from cluster by SAPD filtered by specified IPv6 address of an AP and ESSID.

Usage Guidelines

This command shows bucket map received from cluster by SAPD process. For the remaining parameters, see the command syntax.

Example

Access the CLI and use the following command to show bucket map received from cluster by SAPD process filtered by AP **test** and ESSID **default**:

```
(host) [mynode] #show ap remote debug bucketmap sapd ap-name test essid default

Bucket map for essid default (Rcvd at Tue May 31 16:29:08 2016 [19h:39m:41s ago]);gen_num=1
-------------------------------------------------------------------------------------------------
---------
Item                        Value
----                        -----
Essid                       default
UAC 0                       10.15.146.3
UAC 1                       10.15.146.4
UAC 2                       10.15.146.5
UAC 3                       10.15.146.6
Active Map [0-31]           00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [32-63]          00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [64-95]          00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [96-127]         00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [128-159]        00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 03 00
Active Map [160-191]        01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
03 00 01 03 00 01 03 00 01 03
Active Map [192-223]        00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01
Active Map [224-255]        00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01
```

```
Standby Map [0-31]          01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00
01 01 01 00 01 01 01 00 01 01
Standby Map [32-63]         01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00
01 01 01 00 01 01 01 00 01 01
Standby Map [64-95]         01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00
01 01 01 00 01 01 01 00 01 01
Standby Map [96-127]        01 00 01 01 01 00 01 01 03 00 00 00 03 00 00 00 03 00 00 00 03 00
00 00 03 00 00 00 03 00 00 00
Standby Map [128-159]       03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00
00 00 03 00 00 00 03 00 00 03
Standby Map [160-191]       00 00 03 00 00 03 00 00 03 00 00 03 00 00 03 00 02 03 03 02 03 03
02 03 03 02 03 03 02 03 03 02
Standby Map [192-223]       03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03
03 02 03 03 02 03 03 02 03 03
Standby Map [224-255]       03 03 03 03 03 03 03 03 03 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02

L2 Connectedness [0-31]     1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [32-63]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [64-95]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [96-127]   1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [128-159]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [160-191]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [192-223]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [224-255]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on managed devices

show ap remote debug bucketmap stm

```
show ap remote debug bucketmap stm {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} [essid <essid>]
```

Description

This command shows bucket map received from cluster by AP STM.

Syntax

Parameter	Description
`ap-name <ap-name> essid <essid>`	Shows bucket map received from cluster by AP STM filtered by specified AP name and ESSID.
`ip-addr <ip-addr> essid <essid>`	Shows bucket map received from cluster by AP STM filtered by specified IP address of an AP and ESSID.
`ip6-addr <ip6-addr> essid <essid>`	Shows bucket map received from cluster by AP STM filtered by specified IPv6 address of an AP and ESSID.

Usage Guidelines

This command shows bucket map received from cluster by AP STM. For the remaining parameters, see the command syntax.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

Access the CLI and use the following command to show bucket map received from cluster by AP STM filtered by AP **test** and ESSID **default**:

```
(host) [mynode] #show ap remote debug bucketmap stm ap-name test essid default

Bucket map for essid default
----------------------------------------
Item                        Value
----                        -----
Essid                       default
UAC 0                       10.15.146.3 (Up)
UAC 1                       10.15.146.4 (Up)
UAC 2                       10.15.146.5 (Up)
UAC 3                       10.15.146.6 (Up)
Current Map [0-31]          00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Current Map [32-63]         00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Current Map [64-95]         00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Current Map [96-127]        00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Current Map [128-159]       00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 03 00
Current Map [160-191]       01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
03 00 01 03 00 01 03 00 01 03
Current Map [192-223]       00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01
```

```
Current Map [224-255]       00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01

Active Map [0-31]           00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [32-63]          00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [64-95]          00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [96-127]         00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 02 03
Active Map [128-159]        00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01
02 03 00 01 02 03 00 01 03 00
Active Map [160-191]        01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01
03 00 01 03 00 01 03 00 01 03
Active Map [192-223]        00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03 00 01
Active Map [224-255]        00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01 00 01

Standby Map [0-31]          01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00
01 01 01 00 01 01 01 00 01 01
Standby Map [32-63]         01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00
01 01 01 00 01 01 01 00 01 01
Standby Map [64-95]         01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00 01 01 01 00
01 01 01 00 01 01 01 00 01 01
Standby Map [96-127]        01 00 01 01 01 00 01 01 03 00 00 00 03 00 00 00 03 00 00 00 03 00
00 00 03 00 00 00 03 00 00 00
Standby Map [128-159]       03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00 00 00 03 00
00 00 03 00 00 00 03 00 00 03
Standby Map [160-191]       00 00 03 00 00 03 00 00 03 00 00 03 00 00 03 00 02 03 03 02 03 03
02 03 03 02 03 03 02 03 03 02
Standby Map [192-223]       03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03 03 02 03
03 02 03 03 02 03 03 02 03 03
Standby Map [224-255]       03 03 03 03 03 03 03 03 03 02 02 02 02 02 02 02 02 02 02 02 02 02
02 02 02 02 02 02 02 02 02 02
L2 Connectedness [0-31]     1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [32-63]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [64-95]    1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [96-127]   1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [128-159]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [160-191]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [192-223]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
L2 Connectedness [224-255]  1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Current Map Timestamp Wed Jun  1 12:17:57 2016 (2m:29s ago); gen_num=1 Reason=Node Up
Trigger=Normal Bmap
Bucket Map Rcvd Timestamp Wed Jun  1 12:17:56 2016 (2m:30s ago)
radio_bg 0, radio_a 1:
Bucket Index 175, list 0x101ed464:
   sta:80:86:f2:41:1e:f0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on managed devices

show ap remote debug bucketmap-counters

```
show ap remote debug bucketmap-counters {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr
<ip6-addr>}
```

Description

This command shows bucket map counters.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows bucket map counters filtered by specified AP name.
`ip-addr <ip-addr>`	Shows bucket map counters filtered by specified IP address of an AP.

Usage Guidelines

This command shows bucket map counters. For the remaining parameters, see the command syntax.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

Access the CLI and use the following command to bucket map counters filtered by the AP name **test**:

```
(host) [mynode] #show ap remote debug bucketmap-couters ap-name test

Bucketmap Counters
------------------
Name                                                Value
----                                                -----
Bucketmap Updates, trunc errors                     0 0
AP Bucketmap Updates Without Initialization         0
AP Bucketmap Lookup Failed                          0
AP Bucketmap Allocation Failed                      0
On AP STA Lookup UAC Failed                         0
UAC Up/Down Events                                  4 0
UAC Changed in Bmaps                                0
Deauth dropped from non-UAC                         0
Deauths : New Bmap, Node Down not L2, node down no UAC  0, 0, 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on managed devices

show ap remote debug client-mgmt-counters

```
show ap remote debug client-mgmt-counters {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

Shows the number of each type of message from the clients of an AP. This information can be used to troubleshoot problems on an AP.

Syntax

Parameter	Description
`show ap remote debug client-mgmt-counters`	Use this command to display message counters.
`ap-name <ap-name>`	To show message counters by AP name.
`bssid <bssid>`	To show message counters by MAC address of AP.
`ip-addr <ip-addr>`	To show message counters by IP address of AP.
`ip6-addr <ip6-addr>`	To show message counters by IPv6 address of AP.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

The output of this command shows client management counters for the specified AP.

```
(host)#show ap remote debug client-mgmt-counters ap-name ap120-3
Counters
--------
Name                          Value
----                          -----
Validate Client               512
AP Stats Update Message       557750
3087                          6
Tunnel VLAN Membership        4493
Update STA Tunnel Request     229
Update STA Tunnel Response    229
ARM Update                    808921
ARM Propagate                 590567
ARM Neighbor Assigned         55396
STM SAP Down                  19
AP Message                    192
STA On Call Message           12164
STA Message                   19750
STA SIP authenticate Message  10919
STA Deauthenticate            707
Stat Update V3                441447
Remote AP State               371330
AP Message Response           164
assoc-req                     4358
```

```
assoc-resp                      4358
reassoc-req                     950
reassoc-resp                    950
disassoc                        452
deauth                          5117
sapcp                           351131
```

The output of this command includes the following information:

Parameter	Description
`Validate Client`	Number of times a client was validated.
`AP Stats Update Message`	Number of times an AP updated its statistics with the managed device.
`ARM Update`	Number of times an AP has changed its ARM settings.
`STA On Call Message`	Number of counters indicating that a station has an active phone call.
`STA SIP authenticate Message`	Number of messages indicating that a telephone has completed SIP registration and authentication.
`STA Deauthenticate`	Number of times a station sent a message to an AP to deauthenticate a client.
`assoc-req`	Number of 802.11 association request management frames from the controller.
`assoc-resp`	Number of 802.11 association responses to the controller.
`reassoc-req`	Number of 802.11 reassociation requests to the controller.
`reassoc-resp`	Number of 802.11 reassociation responses from the controller.
`disassoc`	Number of 802.11 disassociation messages to the controller.
`deauth`	Number of 802.11 deauthorization messages from the controller.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug flash-config

```
show ap remote debug flash-config {ap-name <ap-name>|bssid <bssid>|ip-addr <ip-addr>|ip6-addr
<ip6-addr>} acls | vap <vap> | vaps
```

Description

Show the remote AP configuration stored in flash memory.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows debugging data for an AP with a specific name.
`bssid <bssid>`	Shows data for a specific BSSID on an AP. The BSSID is usually the MAC address of the AP.
`ip-addr <ip-addr>`	Shows data for an AP with a specific IP address by entering its IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Shows data for an AP with a specific IP6 address by entering its IP6 address in dotted-decimal format.
`acls`	Displays ACLs of offline virtual APs.
`vap <vap>`	Displays the configuration of a specific offline virtual AP by entering the name of a virtual AP.
`vaps`	Displays the current number of offline virtual APs.

Example

The output of this command can be used to debug problems with a remote AP. The command below shows statistics for an AP with the IP address `192.0.2.64`.

```
(host) [mynode] #show ap remote debug flash-config ip-addr 192.0.2.64
   acls
Offline ACLs
------------
Item                     Value
----                     -----
Native VLAN              1
DHCP VLAN                N/A
DHCP ADDR                192.168.11.1
DHCP POOL NETMASK        255.255.255.0
DHCP POOL START          192.168.11.2
DHCP POOL END            192.168.11.254
DHCP DNS SERVER          0.0.0.0
DHCP ROUTER              192.168.11.1
DHCP DNS DOMAIN          mycompany
DHCP LEASE               0
Session ACL              N/A
Session ACL Name         N/A
Session ACL Count        N/A
Session Aces             N/A
ACL 1                    1
ACL 1 Name               logon
ACL 1 Count              21
```

```
Aces 1                  16 1 4294
...
```

The output of this command includes the following information:

Column	Description
Native VLAN	VLAN ID of the native VLAN.
DHCP VLAN	VLAN ID of Remote AP DHCP server used when the controller is unreachable.
DHCP ADDR	IP Address used as DHCP Server Identifier.
DHCP POOL NETMASK	Netmask of the DHCP server pool.
DHCP POOL START	IP Address used as the start of a range of addresses for a DHCP pool.
DHCP POOL END	IP Address used as the end of a range of addresses for a DHCP pool.
DHCP DNS SERVER	IP Address for the DHCP DNS server.
DHCP ROUTER	IP Address for the DHCP default router.
DHCP DNS DOMAIN	Domain name for the DHCP DNS server.
DHCP LEASE	Length of DHCP DNS leases in days. If this parameter displays a zero (0) the DHCP lease is has no defined end.
Session ACL	Name of the ACL applied to the user session.
Session ACL name	Name of the ACL applied to the user session.
Session ACL count	Number of rules in the applied to the user session.
Session Aces	A list of the individual rules in the session ACL.
ACL 1	This parameter shows the position of an individual ACL.
ACL1 Name	Name of the ACL in the first position.
ACL1 Count	Number of rules in the specified ACL.
ACL1 Aces	A list of the individual rules in the specified ACL.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug-mcast-forwarder

```
show ap remote debug-mcast-forwarder {ap-name <ap-name> | ip-addr <ip-addr>
```

Description

This command displays the Mcast forwarder status for the selected AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows debugging information for a specific AP.
`ip-addr <ip-addr>`	Shows debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

Use this command to display the mcast forwarder status for an AP.

```
(host) [mynode] #show ap remote debug-mcast-forwarder ip-addr 191.191.191.323
Status (0): OFF, VLANs: 1
Mcast Aggregation Forwarder election status:
-------------------------------------------
VLAN  Forwarder  TX  RX
----  ---------  --  --
1     itself     0   0
Forwarder:mcast packets forwarder on the VLAN
TX:output announcement number for forwarder election on the VLAN
RX:input announcement number for forwarder election on the VLAN
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug mgmt-frames

```
show ap remote debug mgmt-frames {ap-name <ap-name>}|{ip-addr <ip-addr>}|{ip6-addr <ip6-addr>}
[client-mac <client-mac>] [count <count>]
```

Description

This command shows traced 802.11 management frames for a remote AP.

Syntax

Parameter	Description	Range
`ap-name <ap-name>`	Show debugging information for a specific AP.	—
`ip-addr <ip-addr>`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.	—
`ip6-addr <ip6-addr>`	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.	—
`client-mac <client-mac>`	Show the AP associations for a specific MAC address by entering the MAC address of the client.	—
`count <count>`	Limit the amount of information displayed by specifying number of frames to appear in the output of this command.	1–128

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

Use this command to debug 802.1 authentication on a remote AP. The example below shows that a client successfully associated with the remote AP, then was later deauthenticated.

```
(host) [mynode] #show ap remote debug mgmt-frames ap-name AP32
```

The output of this command includes the following information:

Column	Description
`Timestamp`	The time the management frame was sent.

Column	Description
stype	One of the following 802.11 frame types: auth: Authorization frame deauth: Deauthorization frame assoc-resp: Association response assoc-req: Association request
SA	Source MAC address.
DA	Destination MAC address.
BSS	BSSID of the AP.
signal	Signal strength as a signal to noise ratio. For example, a value of 30 would indicate that the power of the received signal is 30 dBm above the signal noise threshold.
Misc	Additional information describing the client's action. In the case of deauthentication, a reason associated with the event will be displayed in this column.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug nodelist history

```
show ap remote debug nodelist history {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows cluster node history for a remote AP.

Syntax

Parameter	Description	Range
`ap-name <ap-name>`	Show debugging information for a specific AP.	—
`ip-addr <ip-addr>`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.	—
`ip6-addr <ip6-addr>`	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.	—

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug nodelist history ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug redun-state history

```
show ap remote debug redun-state history {ap-name <ap-name>|ip-addr <ip-addr>|ip6-addr <ip6-addr>}
```

Description

This command shows cluster node history for a remote AP.

Syntax

Parameter	Description	Range
`ap-name <ap-name>`	Show debugging information for a specific AP.	—
`ip-addr <ip-addr>`	Show debugging information for an AP with a specific IP address by entering its IP address in dotted-decimal format.	—
`ip6-addr <ip6-addr>`	Show debugging information for an AP with a specific IPv6 address by entering its IPv6 address in dotted-decimal format.	—

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug redun-state history ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug sapd

```
show ap remote debug sapd cluster-nodestate
   ap-name
   ip-addr
   ip6-addr
```

Description

This command displays the state of cluster node in the SAPD process.

Syntax

Parameter	Description
`ap-name`	Shows state of cluster node for specified AP name.
`ip-addr`	Shows state of cluster node for specified IP address.
`ip6-addr`	Shows state of cluster node for specified IP6 address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode in managed devices

show ap remote debug stale_sta

```
show ap remote debug stale_sta {ap-name <ap-name> | bssid <bssid>| ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows information for debugging an AP.

Syntax

Parameter	Description
`show ap remote debug stale_sta`	Shows stale station entries stored on the AP.
`ap-name <ap-name>`	Shows stale stations based on the AP name filter.
`bssid <bssid>`	Shows stale stations based on the AP MAC address filter.
`ip-addr <ip-addr>`	Shows stale stations based on the IP address filter of the AP.
`ip6-addr <ip6-addr>`	Shows stale stations based on the IPv6 address filter of the AP.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug stale_sta ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug sta-msg-sta-down-entries

```
show ap remote debug sta-msg-sta-down-entries {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows STA message for STA Down list.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows STA message for STA Down list of the specified AP.
`ip-addr <ip-addr>`	Shows STA message for Down list of the specified IP address.
`ip6-addr <ip6-addr>`	Shows STA message for Down list of the specified IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The execution of the following command displays the STA Down list.

```
(host) [mynode] #show ap remote debug sta-msg-sta-down-entries ap-name ap-205
```

Command History:

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug sta-msg-stats

```
show ap remote debug sta-msg-stats {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows statistics of messages between AP and AC relating to STA associations on the AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows statistics of messages between AP and AC relating to STA associations for specified AP name.
`ip-addr <ip-addr>`	Shows statistics of messages between AP and AC relating to STA associations for specified IP address.
`ip6-addr <ip6-addr>`	Shows statistics of messages between AP and AC relating to STA associations for specified IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows an example for executing this command:

```
(host) [mynode] #show ap remote debug sta-msg-stats ap-name ap-205
```

Command History:

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug stm cluster-nodestate

```
show ap remote debug stm cluster-nodestate {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows the cluster node state in AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the cluster node state for specified AP name.
`ip-addr <ip-addr>`	Shows the cluster node state for specified IP address.
`ip6-addr <ip6-addr>`	Shows the cluster node state for specified IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug stm cluster-nodestate ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug stm trace-files

```
show ap remote debug stm trace-files {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows STM trace files for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the STM trace files for specified AP name.
`ip-addr <ip-addr>`	Shows the STM trace files for specified IP address.
`ip6-addr <ip6-addr>`	Shows the STM trace files for specified IP6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug stm trace-files ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote debug uac-list

```
show ap remote debug uac-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

This command shows user anchor controller (UAC) list in AP datapath.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the UAC list in AP datapath for the specified AP name.
`ip-addr <ip-addr>`	Shows the UAC list in AP datapath for the specified IP address.
`ip6-addr <ip6-addr>`	Shows the UAC list in AP datapath for the specified IP6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap remote debug uac-list ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote essid

```
show ap remote essid {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

Show an ESSID summary for the Managed Device, including the numbers of APs and clients connected to a managed device.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the ESSID summary for the specified AP name.
`bssid <bssid>`	Shows the ESSID summary for the specified MAC address.
`ip-addr <ip-addr>`	Shows the ESSID summary for the specified IP address.
`ip6-addr <ip6-addr>`	Shows the ESSID summary for the specified IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

The following is an example for executing the **show ap remote essid** command:

```
(host) [mynode] #show ap remote essid ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap remote wmm-flow

```
show ap remote wmm-flow {ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr
<ip6-addr>}
```

Description

This command shows the Wireless Multimedia (WMM) flows that are active on an AP connected to a Managed Device.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the WMM flows that are active for a specified AP name.
`bssid <bssid>`	Shows the WMM flows that are active for a specified MAC address.
`ip-addr <ip-addr>`	Shows the WMM flows that are active for a specified IP address.
`ip6-addr <ip6-addr>`	Shows the WMM flows that are active for a specified IPv6 address.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing the **show ap remote wmm-flow** command.

```
(host) #show ap remote wmm-flow ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ip6-addr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap sapd-debug log

```
show ap sapd-debug log {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>} | <page>
```

Description

This command displays the SAPD debug log for an AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Shows the SAPD debug log for the specified AP name.
`ip-addr <ip-addr>`	Shows the SAPD debug log for the specified IP address.
`ip6-addr <ip6-addr>`	Shows the SAPD debug log for the specified IP6 address.
`<page>`	Displays the specified page of the SAPD debug log information.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing the **show ap sapd-debug log** command.

```
(host) #show ap sapd-debug log ap-name ap-205
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform s	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap snmp

```
show ap snmp
   wlsxSwitchStationMgmtTable
   wlsxSwitchStationStatsTable
   wlsxWlanAPBssidTable
   wlsxWlanAPTable
   wlsxWlanESSIDTable
   wlsxWlanRadioTable
```

Description

This command displays the AP-related SNMP tables.

Syntax

Parameter	Description
`wlsxSwitchStationMgmtTable`	Display user tree.
`wlsxSwitchStationStatsTable`	Display user statistics tree.
`wlsxWlanAPBssidTable`	Display BSSID SNMP tree.
`wlsxWlanAPTable`	Display SNMP tree.
`wlsxWlanESSIDTable`	Displays ESSID SNMP tree.
`wlsxWlanRadioTable`	Display radio table SNMP tree.

Example

Access the Mobility Master's CLI and use the following command to display BSSID SNMP tree:

```
(host)[mynode] #show ap snmp wlsxWlanAPBssidTable

SNMP - AP BSSID Table
---------------------
AP MAC             Radio  BSSID             Phy Type  Status  Channel
------             -----  -----             --------  ------  -------
00:24:6c:c3:d6:82  1      00:24:6c:bd:68:30  1         1       149
00:24:6c:c3:d6:82  2      00:24:6c:bd:68:20  2         1       11

Num BSSIDs:2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on managed devices

show ap spectrum ap-list

```
show ap spectrum ap-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[channel <channel> | essid <essid> | freq-band {2.4ghz | 5ghz} | limit <limit> | or | page
<page> |  sort <sort> | start <start>]
```

Description

This command shows spectrum data seen by an access point that has been converted to a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor for which you want to view spectrum information.
`channel <channel>`	View spectrum information for a specific radio channel.
`essid <essid>`	View spectrum information for a specific ESSID.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`limit <limit>`	Limit the displayed output to the specified number of entries
`or`	Use this parameter to display information that meets either of two criteria, such as a specified ESSID or channel.
`page <page>`	Enter a number from 10–100 (inclusive) to specify the number of entries that should appear in each page of the output for this command. For example, if the output of this command has 100 entries and you select a page value of 20, the output will appear in 5 pages each with 20 entries. If you selected a page value of 10, the output would appear in 10 pages with 10 entries.
`sort <sort>`	Sort the output by the specified data column.
`start <start>`	Start displaying the output at specific spectrum index value.

Usage Guidelines

The Spectrum Analysis feature provides visibility into RF coverage, allowing you to troubleshoot RF interference and identify 802.11 devices on the network. Issue this command to display and sort APs seen by a specific spectrum monitor.

Examples

The output of this example shows spectrum data seen by spectrum monitor ap123. The output in the example below has been divided into two tables to better fit this document. In the ArubaOS CLI, the output appears as a single, long table.

```
(host) [mynode]# show ap spectrum ap-list ap-name ap123
```

```
Spectrum AP Table
-----------------
bssid              essid          spectrum-id  chan  phy-type        signal(dBm)
-----              -----          -----------  ----  --------        ---------------
00:0b:86:cd:22:d0  ECSD Wireless  2            161   80211a          62
00:0b:86:cb:cf:30  ECSD Wireless  3            157   80211a          68
00:0b:86:f6:f6:a0  osuwireless    3            1     80211b/g        48
00:0b:86:f6:f6:a1  osuvoice       4            1     80211b/g        47
00:0b:86:f6:f6:a2  osuguest       5            1     80211b/g        45

avg-rssi(dB)  curr-rssi(dB)  ibss  add-time             last-seen
------------  -------------  ----  --------             -----------
29            31             no    2010-05-16 17:41:36  2010-05-18 13:39:38
24            25             no    2010-05-16 17:41:36  2010-05-18 14:19:03
37            38             no    2010-05-16 17:41:36  2010-05-18 15:06:02
38            38             no    2010-05-16 17:41:36  2010-05-18 15:04:23
37            40             no    2010-05-16 17:41:36  2010-05-18 15:07:32
```

The output of this command includes the following information:

Column	Description
bssid	Basic Service Set Identifier for an AP. This is usually the MAC address of the AP.
essid	Extended service set identifier that names a wireless network.
spectrum-id	Identifier assigned to the device by the spectrum monitor.
chan	Radio channel used by the BSSID.
freq-band	Radio phy type. Possible types include: ■ 2.4 GHz ■ 5 GHz
signal (dBm)	Strength of the signal received by the device, in dBm.
avg-rssi	The average signal-to-noise ratio seen by the AP.
curr-rssi	Most recent signal-to-noise ratio seen by the AP.
ibss	Shows if ad hoc BSS is enabled or disabled. It will be enabled if the bssid has detected an ad hoc BSS (an ibss bit in an 802.11 frame).
add-time	Time when the AP was first detected by the spectrum monitor.
last-seen	Time when the AP was last seen by the spectrum monitor.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemode spectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensse	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum channel-metrics

```
show ap spectrum channel-metrics {ap-name <ap-name>|ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[freq-band {2.4ghz | 5ghz}]
```

Description

This command shows channel quality, availability, and utilization metrics as seen by a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guideline

This chart displays channel utilization data, showing the percentage of each channel that is currently being used by Wi-Fi devices, and the percentage of each channel being used by non-Wi-Fi devices and 802.11 adjacent channel interference (ACI).

ACI refers to the interference on a channel created by a transmitter operating in an adjacent channel. A transmitter on a nonadjacent or partially overlapping channel may also cause interference, depending on the transmit power of the interfering transmitter and/or the distance between the devices. In general, ACI may be caused by a Wi-Fi transmitter or a non-Wi-Fi interferer. However, whenever the term ACI appears in Spectrum Analysis graphs, it refers to the ACI caused by Wi-Fi transmitters. The channel utilization option in the Channel Metrics Chart shows the percentage of the channel utilization due to both ACI and non-Wi-Fi interfering devices. Unlike the ACI shown in the show ap spectrum interference-power output, the ACI shown in this graph indicates the percentage of channel time that is occupied by ACI or unavailable for Wi-Fi communication due to ACI.

The Channel Metrics table can also show channel availability, the percentage of each channel that is available for use, or display the current relative quality of selected channels in the 2.4 GHz or 5 GHz radio bands. In the spectrum analysis feature, channel quality is a relative measure that indicates the ability of the channel to support reliable Wi-Fi communication. Channel quality, which is represented as a percentage in this chart, is a weighted metric derived from key parameters that can affect the communication quality of a wireless channel, including noise, non-Wi-Fi (interferer) utilization and duty-cycles, and certain types of retries. Note that channel quality is not directly related to Wi-Fi channel utilization, as a higher quality channel may or may not be highly utilized.

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The output of this example shows part of the channel metrics table for channels seen by the spectrum monitor ap123.

```
(host) [mynode] #show ap spectrum channel-metrics ap-name ap123 freq-band 2.4ghz

Channel Metrics Table
---------------------
Channel  Quality(%)  Availability(%)  Utilization(%)  WiFi Util(%)  Interference Util(%)
-------  ----------  ---------------  --------------  ------------  --------------------
1        97          57               43              40            3
2        80          58               42              22            20
3        63          58               42              5             37
4        71          57               43              16            27
5        88          54               46              36            10
6        98          51               49              47            2
7        88          54               46              35            11
8        69          56               44              14            30
9        60          57               43              3             40
10       30          29               71              1             70
11       0           0                100             0             100
12       25          50               50              0             50
13       50          99               1               0             1
14       99          99               1               0             1
1+/5-    63          54               46              36            10
2+/6-    63          51               49              47            2
3+/7-    63          51               49              47            2
4+/8-    69          51               49              47            2
5+/9-    60          51               49              47            2
6+/10-   30          29               71              1             70
7+/11-   0           0                100             0             100
```

The output of this command includes the following information:

Column	Description
`channel`	An 802.11a or 82.11g radio channel.
`Quality(%)`	Current relative quality of selected channels in the 802.11a or 802.11g radio bands, as determined by the percentage of packet retries, the current noise floor, and the duty cycle for non-Wi-Fi devices on that channel.
`Availability(%)`	The percentage of the channel currently available for use.
`Utilization(%)`	The percentage of the channel being used.
`WiFi Util(%)`	The percentage of the channel currently being used by Wi-Fi devices.
`Interference Util(%)`	The percentage of the channel currently being used by non-Wi-Fi interference + Wi-Fi ACI (Adjacent Channel Interference)

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profile mode spectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profile mode spectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum channel-summary

```
show ap spectrum channel-summary {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[freq-band {2.4ghz | 5ghz}]
```

Description

This command displays a summary of the 802.11a or 802.11g channels seen by a spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor for which you want to view spectrum information.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either **2.4 GHz** or **5 GHz**.

Usage Guidelines

This table can display data aggregate data for each channel seen by the spectrum monitor radio, including the maximum AP power, interference and the signal-to-noise-and-interference Ratio (SNIR).

SNIR is the ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The output of the example below shows information for 802.11a radio channels seen by the spectrum monitor **ap999**.

```
(host) [mynode] #show ap spectrum channel-summary ap-name ap999 freq-band 5ghz

Channel Summary Table
---------------------
Channel   KnownAPs   UnknownAPs   Util(%)   MaxAPSignal(dBm)   MaxInterference(dBm)   SNIR(dB)
-------   --------   ----------   -------   ----------------   --------------------   -------
149       69         0            5         -39                -69                    30
153       20         0            100       -42                -60                    18
157       56         0            6         -53                -59                    6
161       54         0            4         -43                -71                    28
165       32         0            3         -27                -70                    43
149+      69         0            100       -39                -60                    21
157+      20         0            6         -43                -59                    16
```

The output of this command includes the following information:

Column	Description
Channel	An 802.11a or 802.11g radio channel.
Known APs	Number of valid APs identified on the radio channel.
UnKnown APs	Number of invalid or rogue APs identified on the radio channel.
Channel Util (%)	Percentage of the channel currently in use.
Max AP Signal (dBm)	Signal strength of the AP that has the maximum signal strength on a channel.
Max Interference(dBm)	Signal strength of the non-Wi-Fi device that has the highest signal strength.
SNIR (db)	The ratio of signal strength to the combined levels of interference and noise on that channel. This value is calculated by determining the maximum noise-floor and interference-signal levels, and then calculating how strong the desired signal is above this maximum.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum client-list

```
show ap spectrum client-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[ap-bssid <ap-bssid> | channel <channel> | essid <essid> | freq-band {2.4ghz | 5ghz} | limit
<limit> | mac <mac> | or  | page <page> | sort <sort> | start <start>]
```

Description

This command shows details for clients seen by a specified spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor for which you want to view spectrum information.
`ap-bssid <ap-bssid>`	View information for a client with a specific BSSID.
`channel <channel>`	view information for clients on a specific radio channel.
`essid <essid>`	View information for clients using a specific ESSID.
`mac <mac>`	View information for a client with a specific MAC address.
`or`	Use this parameter to display information that meets either or two criteria, such as a specified ESSID or channel.
`page <page>`	Enter a number from 10–100 (inclusive) to specify the number of entries that should appear in each page of the output for this command. For example, if the output of this command has 100 entries and you select a page value of 20, the output will appear in 5 pages each with 20 entries. If you selected a page value of 10, the output would appear in 10 pages with 10 entries.
`sort <sort>`	Sort the output by the specified data column.
`start <start>`	Start displaying the output at specific spectrum index value.

Usage Guidelines

Use this command to view channel and signal information for wireless clients seen by the spectrum monitor.

Examples

The example shows that the spectrum monitor **ap999** sees eight different clients on channel 149. The output in the example below has been divided into two tables to better fit this document. In the ArubaOS CLI, the output appears as a single, long table.

```
(host) [mynode] #show ap spectrum client-list ap-name ap999 channel 149

Spectrum Client Table
---------------------
mac                bssid              essid              spectrum-id  channel  phy-type
```

```
---                 -----               -----               -----------  -------  --------
00:14:a4:d1:34:63   00:24:6c:80:48:79   ethersphere-wpa2    14           149      80211a
00:19:7d:3a:96:d9   00:24:6c:80:7b:c9   ethersphere-wpa2    198          149      80211a
00:16:cf:af:3e:e1   00:24:6c:80:48:79   ethersphere-wpa2    80           149      80211a
00:1c:26:5b:a7:ac   00:24:6c:81:8b:19   ethersphere-wpa2    125          149      80211a
00:21:6b:c6:b2:12   00:24:6c:80:48:79   ethersphere-wpa2    118          149      80211a-HT-40
00:21:6a:9c:0e:36   00:24:6c:81:8b:19   ethersphere-wpa2    121          149      80211a
00:21:6a:51:e4:30   00:1a:1e:87:c1:91   ethersphere-wpa2    164          149      80211a-HT-40
00:24:d6:65:a9:e6   00:24:6c:80:48:7a   ethersphere-voip    222          149      80211a-HT-40

signal(dBm)       add-time             last-seen
---------------   --------             -----------
-71               2010-05-17 09:53:47  2010-05-17 12:36:54
-66               2010-05-17 12:01:01  2010-05-17 12:36:42
-74               2010-05-17 09:54:59  2010-05-17 12:35:55
-79               2010-05-17 10:23:29  2010-05-17 12:37:28
-66               2010-05-17 10:17:05  2010-05-17 12:31:58
-72               2010-05-17 10:20:05  2010-05-17 12:37:30
-63               2010-05-17 11:07:21  2010-05-17 12:29:01
-69               2010-05-17 12:37:25  2010-05-17 12:37:25

start:0
Length:8
Total:8
```

The output of this command includes the following information:

Column	Description
mac	MAC address of the client.
bssid	Basic Service Set Identifier for a client. This is usually the device's MAC address.
essid	Extended service set identifier that names a wireless network.
spectrum-id	Identifier assigned to the client by the spectrum monitor.
chan	Radio channel used by the BSSID.
phy-type	Radio phy type. Possible types include: ■ 802.11a ■ 802.11a-HT-40 ■ 802.11b/g ■ 802.11b/g-HT-20
signal(dBm)	Client signal strength, in dBm.
add-time	Time when the client was first detected by the spectrum monitor.
last-seen	Time when the spectrum monitor last detected that the client was active.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug

```
show ap spectrum debug {channel-info | channel-quality | classify |classify-device | classify-
fft | device-details | device-info | devices-seen} {ap-name <ap-name> | ip-addr <ip-addr> |
ip6-addr <ip6-addr>}  freq-band {2.4ghz | 5ghz} [<count>]
```

Description

This command saves spectrum analysis channel information to a file on the spectrum monitor.

Syntax

Parameter	Description
`channel-info`	Save channel information for later analysis.
`channel-quality`	Save channel quality information for later analysis
`classify`	Save information on classification for later analysis.
`classify-device`	Save information on classification-related debugging with device-type for later analysis
`classify-fft`	Save information on classification and FFT data for later analysis.
`device-details`	Save device details for later analysis.
`device-info`	Save device information for later analysis.
`devices-seen`	Save information on devices seen by the spectrum monitor.
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IP6 address of the spectrum monitor for which you want to view spectrum information.
`freq-band {2.4ghz | 5ghz}`	Save information for a specific radio type, either **2.4 GHz** or **5 GHz**.
`<count>`	Specify the number of samples to save.

Usage Guidelines

Use this command under the supervision of your Aruba technical support representative to troubleshoot spectrum analysis issues or errors. If a dump-server is defined in the AP system profile of the AP, the file created by this command will be sent from the AP to the dump-server using TFTP.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum debug channel-info ap-name ap-205 freq-band 2.4ghz 22
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug fft

```
show ap spectrum debug fft {ap-name <ap-name> | ip-addr <ip-addr>} | ip-6 addr <ipg-addr>}
freq-band {2.4ghz | 5ghz} [avg | duty-cycle |fft-to-controller | max | normalized | raw | raw-
normalized] [<count>]
```

Description

This command helps you save Fast Fourier Transform (FFT) power data to a file on the spectrum monitor.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor.
`freq-band {2.4ghz | 5ghz}`	Save information for a specific radio type, either **2.4 GHz** or **5 GHz**.
`avg`	Save FFT average information.
`duty-cycle`	Save FFT duty-cycle data.
`fft-to-controller`	Save the FFT max, average and duty-cycle data.
`max`	Save the maximum FFT power measured for all samples taken over the last second.
`normalized`	Save normalized FFT information.
`raw`	Save the raw FFT information received from driver.
`raw-normalized`	Save FFT information received from driver and its normalized FFT.
`count`	Save a specific number of samples.

Usage Guidelines

Use this command under the guidance of your Aruba technical support representative to troubleshoot FFT power issues.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum debug fft ap-name ap-205 freq-band 5ghz avg 20
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profile mode spectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug monitors

```
show ap spectrum debug monitors
```

Description

Show a detailed description of all spectrum monitors on the controller.

Syntax

No parameters.

Examples

The output of this command shows a list of available spectrum monitor or hybrid AP devices, a list of spectrum devices currently subscribed to a spectrum client, message counters for subscribed spectrum devices and the subscription history.

```
(host) [mynodr] #show ap spectrum debug monitors
List of Available Sensors
---------------------------------
AP name  Phy  Band
-------  ---  ----
ap999    G    2GHz
ap999    A    5GHz
Total: 2
List of Subscriptions
---------------------
AP name  Band        Client IP      Subscribe Time          HTTPD pid  Last Data Sent  Send
Failed
-------  ----        ---------      --------------          ---------  --------------  -------
----
ap123    2GHz        10.100.100.67  2010-05-18 03:49:44 PM  1711       1s              0
ap123    5GHz        10.100.100.67  2010-05-18 03:49:51 PM  1711       1s              0
Num Subscriptions: 2
Current Time: 2010-05-18 03:49:54 PM
Message Counters
----------------
AP name  Band        FFT Data  FFT Duty Cycle  Device Info  Device Details  Devices Seen
Channel Info
-------  ----        --------  --------------  -----------  --------------  ------------  ----
--------
ap123    2GHz        4         4               1            194             1             1
ap123    5GHz        0         0               0            0               0             0
Subscription History
--------------------
Message          AP/Radio/Band          Client IP      HTTPD  Timestamp               Result
        pid
-------          -------------          ---------      ------ ---------               ------
Subscribe        "ap123"/1/2GHz         10.240.16.165  1701   2010-05-17 01:29:16 PM  Success
Re-subscribe     "ap123"/0/5GHz         10.240.16.165  1700   2010-05-17 01:29:16 PM  Success
Unsubscribe-All  "ap123"/-/-            10.240.16.165  1701   2010-05-17 02:44:18 PM  Client
Not found
Subscribe        "ap123"/1/2GHz         10.100.100.67  1716   2010-05-18 03:44:28 PM  Success
```

Usage Guidelines

Use this command under the guidance of an Aruba technical support representative to troubleshoot spectrum analysis errors.

Related Commands

Command	Description
ap spectrum local-override	Convert an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profile mode spectrum-mode	Set an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profile mode spectrum-mode	Set an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum debug status

```
show ap spectrum debug status {ap-name <ap-name> | ip-addr <ip-addr>
| ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz}]
```

Description

This command shows detailed status and statistics for a spectrum monitor or hybrid AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum device for which you want to view status information.
`ip-addr <ip-addr>`	IP address of the spectrum device for which you want to view status information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum device for which you want to view status information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

Use this command under the guidance of an Aruba technical support representative to troubleshoot spectrum analysis errors.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum debug status ap-name ap-205 freq-band 5ghz
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Set an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-duty-cycle

```
show ap spectrum device-duty-cycle {ap-name <ap-name>| ip-addr <ip-addr> | ip6-addr <ip6-addr>} [freq-band {2.4ghz | 5ghz}]
```

Description

This command shows the current duty cycle for devices on all channels being monitored by the spectrum monitor or hybrid AP radio.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum device for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum device for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum device for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

The FFT Duty Cycle table in the output of this command shows the duty cycle for each radio channel. The duty cycle is the percentage of time each device type operates or transmits on that channel. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 1540.

Examples

The output of this command shows that video devices sent a signal on channels 153 and 157 during 99% of the last sample interval.

```
Device Duty Cycle Table (in %)
------------------------------
Device Type          149  153  157  161  165  149+  157+
-----------          ---  ---  ---  ---  ---  ----  ----
Generic Interferer   0    0    0    0    0    0     0
WIFI                 5    0    5    12   8    0     12
Microwave            0    0    0    0    0    0     0
Bluetooth            0    0    0    0    0    0     0
Generic Fixed Freq   0    0    0    0    0    0     0
Cordless Phone FF    0    0    0    0    0    0     0
Video                0    99   99   0    0    0     0
Audio                0    0    0    0    0    0     0
Generic Freq Hopper  0    0    0    0    0    0     0
Cordless Network FH  0    0    0    0    0    0     0
Xbox                 0    0    0    0    0    0     0
Microwave Inverter   0    0    0    0    0    0     0
Cordless Base FH     5    5    5    5    5    0     0
Total:7
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-history

```
show ap spectrum device-history {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[freq-band {2.4ghz | 5ghz}] [type {audio | bluetooth | cordless-ff-phone | cordless-fh-base |
cordless-fh-network | generic-ff | generic-fh | generic-interferer | microwave | microwave-
inverter   |video | xbox}]
```

Description

This command shows the history of the last 256 non-Wi-Fi devices.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`type`	Show information for one type of device only by specifying a non-Wi-Fi device.
`audio`	View information for audio devices seen by the spectrum device.
`bluetooth`	View information for bluetooth devices seen by the spectrum device. **NOTE:** This option is available only for 2.4 GHz spectrum devices.
`cordless-ff-phone`	View information for frequency-hopping cordless phones seen by the spectrum device.
`cordless-fh-base`	View information for frequency-hopping cordless phone bases seen by the spectrum device.
`cordless-fh-network`	View information for frequency-hopping cordless network devices seen by the spectrum device.
`generic-ff`	View information for generic fixed-frequency devices seen by the spectrum device.
`generic-fh`	View information for generic frequency-hopping devices seen by the spectrum device.
`generic-interferer`	Show only generic interfering devices.
`microwave`	View information for microwave-emitting devices seen by the spectrum device. **NOTE:** This option is available only for 2.4 GHz spectrum devices.

Parameter	Description
`microwave-inverter`	View information for inverter microwave devices seen by the spectrum device. **NOTE:** This option is available only for 2.4 GHz spectrum devices.
`video`	View information for video devices seen by the spectrum device.
`xbox`	View information for Xbox devices seen by the spectrum device. **NOTE:** This option is available only for 2.4 GHz spectrum devices.

Usage Guidelines

Use this command to view channel, signal, and duty-cycle information as well as addor delete times for the last 256 devices seen by a spectrum monitor or hybrid AP.

Non-Wi-Fi Interferers

The following table describes each type of of non-Wi-Fi interferer detected by a spectrum monitor or hybrid AP. Note also that a hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Non-Wi-Fi Interferer Type	Description
Bluetooth	Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a *Bluetooth* device. Bluetooth uses a frequency hopping protocol.
Fixed Frequency (Audio)	Some audio devices such as wireless speakers and microphones also use fixed frequency to continuously transmit audio. These devices are classified as *Fixed Frequency (Audio)*.
Fixed Frequency (Cordless Phones)	Some cordless phones use a fixed frequency to transmit data (much like the fixed frequency video devices). These devices are classified as *Fixed Frequency (Cordless Phones)*.
Fixed Frequency (Video)	Video transmitters that continuously transmit video on a single frequency are classified as *Fixed Frequency (Video*). These devices typically have close to a 100% duty cycle. These types of devices may be used for video surveillance, TV or other video distribution, and similar applications.
Fixed Frequency (Other)	All other fixed frequency devices that do not fall into one of the above categories are classified as *Fixed Frequency (Other*). Note that the RF signatures of the fixed frequency audio, video and cordless phone devices are very similar and that some of these devices may be occasionally classified as Fixed Frequency (Other).
Frequency Hopper (Cordless Base)	Frequency hopping cordless phone base units transmit periodic beacon-like frames at all times. When the handsets are not transmitting (i.e., no active phone calls), the cordless base is classified as *Frequency Hopper (Cordless Base*).
Frequency Hopper (Cordless Network)	When there is an active phone call and one or more handsets are part of the phone conversation, the device is classified as *Frequency Hopper (Cordless Network*). Cordless phones may operate in 2.4 GHz or 5 GHz bands. Some phones use both 2.4 GHz and 5 GHz bands (for example, 5 GHz for Base-to-handset and 2.4 GHz for Handset-to-base). These phones may be classified as unique Frequency Hopper devices on both bands.

Non-Wi-Fi Interferer Type	Description
Frequency Hopper (Xbox)	The Microsoft Xbox device uses a frequency hopping protocol in the 2.4 GHz band. These devices are classified as *Frequency Hopper (Xbox*).
Frequency Hopper (Other)	When the classifier detects a frequency hopper that does not fall into one of the above categories, it is classified as Frequency Hopper (Other). Some examples include IEEE 802.11 FHSS devices, game consoles and cordless or hands-free devices that do not use one of the known cordless phone protocols.
Microwave	Common residential microwave ovens with a single magnetron are classified as a *Microwave*. These types of microwave ovens may be used in cafeterias, break rooms, dormitories and similar environments. Some industrial, healthcare or manufacturing environments may also have other equipment that behave like a microwave and may also be classified as a Microwave device.
Microwave (Inverter)	Some newer-model microwave ovens have the inverter technology to control the power output and these microwave ovens may have a duty cycle close to 100%. These microwave ovens are classified as *Microwave (Inverter)*. Dual-magnetron industrial microwave ovens with higher duty cycle may also be classified as Microwave (Inverter). As in the Microwave category described above, there may be other equipment that behave like inverter microwaves in some industrial, healthcare or manufacturing environments. Those devices may also be classified as Microwave (Inverter).
Generic Interferer	Any non-frequency hopping device that does not fall into one of the other categories described in this table is classified as a *Generic Interferer*. For example a Microwave-like device that does not operate in the known operating frequencies used by the Microwave ovens may be classified as a Generic Interferer. Similarly wide-band interfering devices may be classified as Generic Interferers.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ap spectrum device-history ap-name ap-205 type audio
```

The output of this example shows details for fixed-frequency video devices seen by a spectrum monitor or hybrid AP radio.

```
host) [mynode] #show ap spectrum device-history ap-name ap123 freq-band 5ghz type video

Non-Wifi Device History Table
-----------------------------
Type    ID  Cfreq(Khz)  Bandwidth(KHz)  Channels-affected  Signal-strength  Duty-cycle
----    --  -----       ---------       -----------------  ---------------  ----------
Add-time              Delete-time
--------              -----------
Video   1   5745312     6000            149                76               99
2010-05-16 20:07:08   -
Video   2   5745312     6000            149                75               99
2010-05-16 20:07:39   2010-05-17 16:50:24
Video   3   5745312     6000            149                74               99
2010-05-16 20:20:25   2010-05-16 20:20:36
Video   4   5745312     6000            149                76               99
2010-05-16 20:32:44   2010-05-16 20:33:07
Video   5   5742031     6000            149                79               99
2010-05-16 20:33:43   2010-05-16 20:33:53
Video   6   5745312     6000            149                75               99
2010-05-16 20:34:08   2010-05-16 20:34:20
```

The output of this command includes the following information:

Column	Description
Type	Device type. This parameter can be any of the following: ■ audio FF (fixed frequency) ■ bluetooth ■ cordless base FH (frequency hopper) ■ cordless phone FF (fixed frequency ■ cordless network FH (frequency hopper) ■ generic FF (fixed frequency ■ generic FH (frequency hopper) ■ generic interferer ■ microwave ■ microwave inverter ■ video ■ xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 1540.
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device, in KHz.
Channels-affected	Radio channels affected by the wireless device, in KHz.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts on the specified channel or frequency.
Add-time	Time at which the device was first detected.
Delete-time	Time at which the device was aged out.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-list

```
show ap spectrum device-list {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[freq-band {2.4ghz | 5ghz} [type {audio | bluetooth | cordless-ff-phone | cordless-fh-base |
cordless-fh-network | generic-ff | generic-fh | generic-interferer | microwave | microwave-
inverter   |video | xbox}]
```

Description

Show a device summary table and channel information for non-Wi-Fi devices currently seen by a spectrum monitor or hybrid AP radio.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip6-addr <ip-addr>`	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`type`	Show data for a specific device type only.
`audio`	Show only audio fixed frequency devices.
`bluetooth`	Show only bluetooth devices. **NOTE:** This option is available only for 2.4 GHz spectrum devices.
`cordless-ff-phone`	View information for frequency-hopping cordless phones seen by the spectrum device.
`cordless-fh-base`	View information for frequency-hopping cordless phone bases seen by the spectrum device.
`cordless-fh-network`	View information for frequency-hopping cordless network devices seen by the spectrum device.
`generic-ff`	View information for generic fixed-frequency devices seen by the spectrum device.
`generic-fh`	View information for generic frequency-hopping devices seen by the spectrum device.
`generic-interferer`	Show only generic interfering devices.
`microwave`	Show only microwave devices. **NOTE:** This option is available only for 2.4 GHz spectrum devices.
`microwave-inverter`	Show only microwave inverter devices. **NOTE:** This option is available only for 2.4 GHz spectrum devices.

Parameter	Description
`video`	Show only video fixed frequency devices.
`xbox`	Show only xbox frequency hopper devices. **NOTE:** This option is available only for 2.4 GHz spectrum devices.

Usage Guidelines

Issue this command to view detailed information about currently active non-Wi-Fi devices on the network. Use the optional **type** parameter to display data for one specific device type only. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 1540.

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The output of this example shows that the spectrum monitor **ap123** is able to see data for a single non-Wi-Fi device on its 802.11a radio. Note that the output below is divided into two sections to better fit on the page of this document. In the ArubaOS CLI, this information is displayed in a single long table.

```
(host) [mynode] #show ap spectrum device-list ap-name ap123 freq-band 5ghz
Non-Wifi Device List Table
--------------------------
Type               ID  Cfreq    Bandwidth  Channels-affected  Signal-strength
----               --  -----    ---------  -----------------  ---------------
Cordless Phone FH  3   5826093  80000      149 157 161 165    49
Duty-cycle  Add-time             Update-time
----------  --------             -----------
5           2010-05-17 10:04:53  2010-05-17 10:04:55
Total:1
Current Time:2010-05-17 10:04:56
```

The output of this command includes the following information:

Column	Description
`Type`	Device type. This parameter can be any of the following: ■ audio FF (fixed frequency) ■ bluetooth ■ cordless base FH (frequency hopper) ■ cordless phone FF (fixed frequency ■ cordless network FH (frequency hopper) ■ generic FF (fixed frequency ■ generic FH (frequency hopper) ■ generic interferer ■ microwave ■ microwave inverter ■ video ■ xbox **NOTE:** For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 1540.

Column	Description
ID	ID number assigned to the device by the spectrum monitor or hybrid AP radio. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Cfreq	Center frequency of the signal sent from the device.
Bandwidth	Channel bandwidth used by the device.
Channels-affected	Radio channels affected by the wireless device.
Signal-strength	Strength of the signal sent from the device, in dBm.
Duty-cycle	Device duty cycle. This value represents the percent of time the device broadcasts a signal.
Add-time	Time at which the device was first detected.
Update-time	Time at which the status of the device was updated.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-log

```
show ap spectrum device-log {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[freq-band {2.4ghz | 5ghz} [type {audio | bluetooth | cordless-ff-phone | cordless-fh-base |
cordless-fh-network | generic-ff | generic-fh | generic-interferer | microwave | microwave-
inverter   |video | xbox}]
```

Description

This command shows a time log of add and delete events for non-Wi-Fi devices.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor for hybrid AP or which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`freq-band 2.4ghz|5ghz`	View information for a specific radio type, either 2.4 GHz or 5 GHz.
`type`	Show data for a specific device type only.
`audio`	Show only audio fixed frequency devices.
`bluetooth`	Show only bluetooth devices. **NOTE:** This option is available only for 2.4 GHz spectrum device radios.
`cordless-ff-phone`	View information for frequency-hopping cordless phones seen by the spectrum device.
`cordless-fh-base`	View information for frequency-hopping cordless phone bases seen by the spectrum device.
`cordless-fh-network`	View information for frequency-hopping cordless network devices seen by the spectrum device.
`generic-ff`	View information for generic fixed-frequency devices seen by the spectrum device.
`generic-fh`	View information for generic frequency-hopping devices seen by the spectrum device.
`generic-interferer`	Show only generic interfering devices.
`microwave`	Show only microwave devices. **NOTE:** This option is available only for 2.4 GHz spectrum device radios.
`microwave-inverter`	Show only microwave inverter devices. **NOTE:** This option is available only for 2.4 GHz spectrum device radios.
`video`	Show only video fixed frequency devices.

Parameter	Description
xbox	Show only xbox frequency hopper devices. **NOTE:** This option is available only for 2.4 GHz spectrum device radios.

Usage Guidelines

Use this table to show a time log of when non-Wi-Fi devices were added to and deleted from the Wi-fi Device log table. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 1540.

A hybrid AP on a 20 MHz channel will see 40 MHz Wi-Fi data as non-Wi-Fi data.

Examples

The output of this example shows that the spectrum monitor **ap123** logged data for four frequency-hopping cordless base devices seen by its 802.11g radio. Note that the output below is divided into two sections to better fit on the page of this document. In the ArubaOS CLI, this information is displayed in a single long table.

```
(host) [mynode] #show ap spectrum device-log ap-name ap123 freq-band 5ghz type cordless-fh-
base

Non-Wifi Device Log Table
-------------------------
Device Type       ID  Added/Deleted  Signal Strength  Duty Cycle  Center Freq
-----------       --  -------------  ---------------  ----------  -----------
Cordless Base FH  1   Added          78               5           5773281
Cordless Base FH  1   Deleted        78               5           5747343
Cordless Base FH  2   Added          78               5           5757656
Cordless Base FH  2   Deleted        78               5           5760469
Cordless Base FH  3   Added          80               5           5802813
Cordless Base FH  3   Deleted        80               5           5802813
Cordless Base FH  4   Added          80               5           5770781

Start Freq  End Freq  Channels Affected     Bandwidth
----------  --------  -----------------     ---------
5733281     5813281   153                   80000
5707343     5787343   149 153 157 161 165   80000
5717656     5797656   153                   80000
5720469     5800469   153 157 161 165       80000
5762813     5842813   161                   80000
5762813     5842813   161                   80000
5730781     5810781   153                   80000

Total:7
Current Time:2012-09-25 12:04:54
```

The output of this command includes the following information:

Column	Description
Device Type	Type of non-Wi-Fi device detected by the spectrum monitor or hybrid AP

Column	Description
ID	The spectrum ID number assigned to that device. Spectrum monitors and hybrid APs assign a unique spectrum ID per device type.
Added/Deleted	The non-Wi-Fi Device Log table can show signal data for a device when that device was added or removed from the log table.
Signal Strength	Strength of the signal sent by the device.
Duty Cycle	Device duty cycle. This value represents the percent of time a signal is broadcast on a specific channel or frequency.
Center Freq	Center frequency of the signal sent by the device.
Start Freq	Lowest signal frequency sent by the device.
End Freq	Highest signal frequency sent by the device.
Channels affected	Radio channels affected by the device signal.
Bandwidth	Amount of signal bandwidth used by the device, in kilohertz.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum device-summary

```
show ap spectrum device-summary {ap-name <ap-name> | ip-addr <ip-addr> | ip6-addr <ip6-addr>}
[freq-band {2.4 ghz | 5ghz}]
```

Description

This command shows the numbers of Wi-Fi and non-Wi-Fi device types on each channel monitored by a spectrum monitor or hybrid AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

Use this command to show the types of devices that the spectrum device can detect on each channel it monitors. For additional details about non-Wi-Fi device types shown in this table, see Non-Wi-Fi Interferers on page 1540.

Examples

The output of this example shows that the spectrum monitor **ap123** is able to detect 61 Wi-Fi devices on channel 149.

```
(host) [mynode] #show ap spectrum device-summary ap-name ap123 freq-band 5ghz

Device Summary Table
--------------------
Device                149  153  157  161  165
-------               ---  ---  ---  ---  ---
Unknown               0    0    0    0    0
WIFI                  61   6    14   29   9
Microwave             0    0    0    0    0
Bluetooth             0    0    0    0    0
Generic Fixed Freq    0    0    0    0    0
Cordless Phone FF     0    0    0    0    0
Video                 0    0    0    0    0
Audio                 0    0    0    0    0
Generic Freq Hopper   0    0    0    0    0
Cordless Phone FH     0    0    0    0    0
Xbox                  0    0    0    0    0
Microwave Inverter    0    0    0    0    0
Total:12
```

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemodespectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemodespectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum interference-power

```
show ap spectrum interference-power {ap-name <ap-name>}|{ip-addr <ip-addr>} [freq-band {2.4
ghz | 5ghz}]
```

Description

This command shows the interference power detected by a 802.11a or 802.11g radio on a spectrum monitor or hybrid AP.

Syntax

Parameter	Description
`ap-name <ap-name>`	Name of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip-addr <ip-addr>`	IP address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`ip6-addr <ip6-addr>`	IPv6 address of the spectrum monitor or hybrid AP for which you want to view spectrum information.
`freq-band {2.4ghz | 5ghz}`	View information for a specific radio type, either 2.4 GHz or 5 GHz.

Usage Guidelines

This table displays information about AP power levels, channel noise, and adjacent channel interference seen on each channel by a spectrum monitor or hybrid AP radio.

The output of this command displays the noise floor of each selected channel in dBm. The noise floor of a channel depends on the noise figure of the RF components used in the radio, temperature, presence of certain types of interferers or noise, and the width of the channel. For example, in a clean environment, the noise floor of a 20 MHz channel will be around -95 dBm and that of a 40 MHz channel will be around -92 dBm. Certain types of fixed frequency continuous transmitters such as video bridges, fixed frequency phones, and wireless cameras typically elevate the noise floor as seen by the Wi-Fi radio. Other interferers such as the frequency hopping phones, Bluetooth, and Xbox devices may not affect the noise floor of the radio. A Wi-Fi radio can only reliably decode Wi-Fi signals that are a certain dB above the noise floor and therefore estimating and understanding the actual noise floor of the radio is critical to understanding the reliability of the RF environment.

The ACI column displayed in the Interference Power Chart displays adjacent-channel interference (ACI) power levels based on the signal strength(s) of the Wi-Fi APs on adjacent channels. A higher ACI value in Interference Power Chart does not necessarily mean higher interference since the AP that is contributing to the maximum ACI may or may not be very actively transmitting data to other clients at all times. The ACI power levels are derived from the signal strength of the beacons.

Examples

The output of this example shows interference power levels for each channel seen by the spectrum monitor **ap123**.

```
(host) [mynode] #show ap spectrum interference-power ap-name ap123 freq-band 5ghz


Interference Power Table
```

```
------------------------
Channel  Noise Floor(dBm)  Max AP Signal(dBm)  Max AP SSID        Max AP BSSID       ACI(dBm)
Max Interference(dBm)
-------  ----------------  ------------------  -----------        ------------       --------
---------------------
149      -91               -40                 ethersphere-wpa2   00:24:6c:80:7b:c9  -77
-71
153      -63               -42                 guest              00:1a:1e:87:c1:90  -63
-58
157      -92               -48                 alpha              00:1a:1e:50:01:30  -74
-60
161      -94               -39                 00:24:6C:C0:15:EB  00:24:6c:81:57:c8  -61
-70
165      -93               -26                 sw-jfb-attack      00:1a:1e:9b:1d:c8  -74
-69
149+     -60               -40                 ethersphere-wpa2   00:24:6c:80:7b:c9  -0
-58
157+     -89               -39                 00:24:6C:C0:15:EB  00:24:6c:81:57:c8  -0
-60
```

The output of this command includes the following information:

Column	Description
`Channel`	An 802.11a or 802.11g radio channel.
`Noise Floor (dBm)`	Current noise floor recorded on the channel.
`Max AP Signal (dBm)`	Power level of the AP on the channel with the highest signal power.
`Max AP SSID`	SSID of the AP on the channel with the highest signal power.
`Max AP BSSID`	BSSID of the AP on the channel with the highest signal power.
`ACI (dBm)`	Adjacent channel interference level detected by the spectrum device.
`Max Interference Power (dBm)`	Signal strength of the non-Wi-Fi device that has the highest signal strength.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum-load-balancing

```
show ap spectrum-load-balancing [group <group>]
```

Description

This command shows spectrum load balancing information for an AP with this feature enabled.

Syntax

Parameter	Description
`group <group>`	Filter this information to show only data for the specified spectrum load balancing domain.

Examples

The output of the command below shows the APs currently using the spectrum load-balancing domain **default-1**.

```
(host)[mynode] #show ap spectrum-load-balancing group default-1

Spectrum Load Balancing Group
-----------------------------
Name     IP Address       Domain     Assignment  Clients
----     ----------       ------     ----------  -------
ap121-1  192.168.151.253  default-1  149/21      3
ap124-1  192.168.151.254  default-1  48/15       3
ap125-1  192.168.151.251  default-1  44/15       2
```

The output of this command includes the following information:

Column	Description
`Name`	Name of an AP.
`IP address`	IP address of the AP.
`Domain`	Name of the spectrum load balancing domain assigned to the AP.
`Assignment`	Current channel and power assignment for the AP.
`Clients`	Number of clients currently using the AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum local-override

```
show ap spectrum local-override
```

Description

This command shows a list of AP radios currently converted to spectrum monitors through the spectrum local-override list.

Syntax

No parameters

Examples

The output of this example shows that three APs each have two radios defined as spectrum monitors.

```
(host)[mynode] #show ap spectrum local-override
Spectrum Local Override Profile
-------------------------------
Parameter       Value
---------       -----
Override Entry  AP ap125 band 2ghz
Override Entry  AP ap125 band 5ghz
Override Entry  AP ap105 band 2ghz
Override Entry  AP ap105 band 5ghz
Override Entry  AP apcorp1 band 2ghz
Override Entry  AP APcorp1 band 5ghz
```

The Value column in the output of this command includes the following information:

Parameter	Description
`Override Entry`	Indicates that an AP radio has been added to the local override list.
`Value`	Radio that has been added to the override list, and the band used by that radio.

Related Commands

Command	Description
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
rf dot11a-radio-profilemode spectrum-mode	Sets an 802.11a radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.
rf dot11g-radio-profilemode spectrum-mode	Sets an 802.11g radio so that the device operates as a spectrum monitor, and can send spectrum analysis data to a desktop or laptop client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum monitors

```
show ap spectrum monitors {ap-group <ap-group>|ap-name <ap-name>|ap-type <ap-type>|channel
<channel>|freq-band <freq-band>|ip-addr <ip-addr>|ip6-addr <ip6-addr>|or [page <page>|sort
<sort>]}
```

Description

This command shows a list of APs terminating on the controller that are currently configured as spectrum monitors or hybrid APs.

Syntax

Parameter	Description
`ap-group <ap-group>`	Specify the spectrum device's AP group.
`ap-name <ap-name>`	Specify the AP name configured as a spectrum monitor or hybrid AP.
`ap-type <ap-type>`	Specify the AP type.
`channel <channel>`	Specify the channel of hybrid monitor.
`freq-band <freq-band>`	Specify the frequency band.
`ip-addr <ip-addr>`	Specify the IP address of spectrum monitor
`ip6-addr <ip6-addr>`	Specify the IPv6 address of spectrum monitor
`or`	Show spectrum monitors that satisfy any of the given conditions:
`page <page>`	Enter a value greater than 1 for Page Number. The number of Spectrum Monitors displayed per page is 50.
`sort <sort>`	Sort criteria based on pairs of column name and order, e.g. ap-name,asc,channel,desc, and so on.

Examples

The output of this example shows that the 802.11a radio on a spectrum monitor named **ap123** is sending spectrum analysis data to a client with the IP address 10.240.16.177.

```
(host)#show ap spectrum monitors

List of Sensors
---------------
AP name            Group    AP Type  Phy  Band       Channel  Mode
    Subscribe Time
-------            -----    -------  ---  ----       -------  ----             -----
         --------------
00:24:6c:c0:0c:89  default  105      G    2GHz       1        Access Point
    10.240.16.177  2011-01-21 07:09:32 AM
00:24:6c:c0:0c:89  default  105      A    5GHz       44+      Access Point     10.240.16.177
2011-01-21 07:17:57 AM
00:24:6c:c7:d6:1c  default  93       A    5GHz        -        Spectrum Monitor 10.240.16.177
 2011-01-21
07:18:22 AM
```

The output of this command includes the following information:

Column	Description
AP name	Name of an AP configured as a spectrum monitor or hybrid AP.
Group	Name of the spectrum device's AP group.
Ap Type	**The AP model number .**
Phy	The radio's PHY type. Possible values are **A** for 802.11a and **G** for 802.11b/g,
Band	Spectrum band that the spectrum monitor or hybrid AP radio is currently monitoring.
Mode	This column shows whether the device is an access point configured as a hybrid AP, or a spectrum monitor.
Client IP	IP address of the client to which the spectrum monitor or hybrid AP is sending data.
Subscribe time	Time at which the spectrum monitor or hybrid AP was connected to the client.

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: ■ **ap-group** ■ **ap-name** ■ **ap-type** ■ **channel** ■ **freq-band** ■ **ip-addr** ■ **ip6-addr** ■ **sort**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap spectrum tech-support

```
show ap spectrum tech-support ap-name <ap-name> [<filename>]
```

Description

Save spectrum data for later analysis by technical support.

Syntax

Parameter	Description
`ap-name <ap-name>`	Save technical support information for a specific spectrum monitor.
`<filename>`	Name of the file to which this data should be saved. This file does not have to already exist on the controller, the **show ap spectrum technical-support** command will create this file.

Usage Guidelines

Use this command under the supervision of your Aruba technical support representative to troubleshoot spectrum analysis issues or errors.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap standby

```
show ap {ap-name <ap-name> | bssid <bssid> | details |ip-addr <ip-addr> | ip6-addr <ip6-addr>}
```

Description

Show all APs in standby mode currently registered to a managed device.

Syntax

Parameter	Description
`ap-name <ap-name>`	View data for an AP with a specified name.
`bssid <bssid>`	View data for a specific BSSID.
`details`	View AP data detailed columns.
`ip-addr <ip-addr>`	View data for an AP with a specified IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	View data for an AP with a specified IPv6 address.

Usage Guidelines

This command displays details for all APs connected to a controller in standby mode.

Example

Execute the following command to view AP data detailed columns:

```
(host) [mynode] #show ap standby details
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap system-profile

```
show ap system-profile [<profile-name>]
```

Description

This command show the system profile settings of an AP.

Syntax

Parameter	Description
<profile-name>	Name of a system profile.

Examples

The output of the command shows the current configuration settings for the default system profile.

```
(host) [mynode] #show ap system-profile default

AP system profile "default"
---------------------------
Parameter                                 Value
---------                                 -----
RF Band                                   g
RF Band for AM mode scanning              all
Native VLAN ID                            1
Tunnel Heartbeat Interval                 10
Session ACL                               ap-uplink-acl
Corporate DNS Domain                      N/A
SNMP sysContact                           N/A
LED operating mode (11n/11ac APs only)    normal
LED override                              Disabled
Driver log level                          emergencies
SAP MTU                                   N/A
RAP MTU                                   1200 bytes
LMS IP                                    N/A
Backup LMS IP                             N/A
LMS IPv6                                  N/A
Backup LMS IPv6                           N/A
LMS Preemption                            Disabled
LMS Hold-down Period                      600 sec
LMS ping interval                         20
Remote-AP DHCP Server VLAN                N/A
Remote-AP DHCP Server Id                  192.168.11.1
Remote-AP DHCP Default Router             192.168.11.1
Remote-AP DHCP DNS Server                 N/A
Remote-AP DHCP Pool Start                 192.168.11.2
Remote-AP DHCP Pool End                   192.168.11.254
Remote-AP DHCP Pool Netmask               255.255.255.0
Remote-AP DHCP Lease Time                 0 days
Remote-AP uplink total bandwidth          0 kbps
Remote-AP bw reservation 1                N/A
Remote-AP bw reservation 2                N/A
Remote-AP bw reservation 3                N/A
Remote-AP Local Network Access            Disabled
Bootstrap threshold                       8
Double Encrypt                            Disabled
Dump Server                               N/A
```

```
Heartbeat DSCP                          0
Maintenance Mode                        Disabled
Maximum Request Retries                 10
Request Retry Interval                  10 sec
Number of IPSEC retries                 85
AeroScout RTLS Server                   N/A
RTLS Server configuration               N/A
RTLS Server Compatibility Mode          Enabled
Telnet                                  Disabled
Spanning Tree                           Disabled
AP multicast aggregation                Disabled
AP ARP attack protection                Disabled
AP multicast aggregation allowed VLANs  none
Console enable                          Enabled
Shell Password                          N/A
Password for Backup                     ********
AP USB Power override                   Disabled
RF Band for Backup                      all
Operation for Backup                    off
BLE Endpoint URL                        N/A
BLE Auth Token                          N/A
BLE Operation Mode                      Disabled
```

The output of this command includes the following information:

Column	Description
RF Band	For dual-band radios, this parameter displays the RF band in which the AP should operate: ■ **g** = 2.4 GHz ■ **a** = 5 GHz
RF Band for AM mode scanning	Scanning band for multiple RF radios. ■ **g** = 2.4 GHz ■ **a** = 5 GHz ■ **all** = Radio scans both bands. This is the default setting.
Native VLAN ID	Native VLAN for bridge mode virtual APs (frames on the native VLAN are not tagged with 802.1q tags).
Tunnel Heartbeat Interval	Interval between heartbeat messages between a remote or campus AP and its associated managed device. An increase in the heartbeat interval increases the time it will take for an AP to detect the loss in connectivity to the managed device, but can reduce internet bandwidth consumed by a remote AP.
Session ACL	This parameter shows the ACL applied on the uplink of a remote AP.
Corporate DNS Domain	DNS name used by the corporate network.
SNMP sysContact	SNMP system contact information.
LED operating mode	Displays the LED operating mode for indoor 802.11n APs. LEDs display as usual in the default **normal** operating mode, but are all turned off in **off** mode.

Column	Description
SAP MTU	Maximum Transmission Unit (MTU) size, in bytes. This value describes the greatest amount of data that can be transferred in one physical frame.
LMS IP	The IP address of the local management switch (LMS)—the Aruba managed device which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. **NOTE:** If the LMS-IP is blank, the access point will remain on the managed device that it finds using methods like DNS or DHCP. If an IP address is configured for the LMS IP parameter, the AP will be immediately redirected to the managed device at that address.
Backup LMS IP	For networks with multiple managed devices, this parameter displays the IP address of a backup to the IP address specified with the lms-ip parameter.
LMS IPv6	For IPv6 networks with multiple managed devices, this parameter specifies the IPv6 address of the local management switch (LMS)—the Aruba managed device—which is responsible for terminating user traffic from the APs, and processing and forwarding the traffic to the wired network. This can be the IP address of the managed device or Mobility Master.
Backup LMS IPv6	In multi-controller ipv6 networks, this parameter specifies the IPv6 address of a backup to the IPv6 address specified with the **LMS IPv6** setting.
LMS Preemption	When this parameter is enabled, the local management switch automatically reverts to the primary LMS IP address when it becomes available.
LMS Hold-down Period	Time, in seconds, that the primary LMS must be available before an AP returns to that LMS after failover. The `rap-dhcp-server-vlan` VLAN ID of the remote AP DHCP server is used if the managed device is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN). If you enter the native VLAN ID, the DHCP server is unavailable.
Remote-AP DHCP Server VLAN	VLAN ID of the remote AP DHCP server used if the managed device is unavailable. This VLAN enables the DHCP server on the AP (also known as the remote AP DHCP server VLAN).
Remote-AP DHCP Server ID	IP address used as the DHCP server identifier.
Remote-AP DNS Server	IP address of the DNS server.
Remote-AP DHCP Default Router	IP address for the default DHCP router.
Remote-AP DHCP Pool Start	This parameter defines the starting IP address in the DHCP pool for remote APs.

Column	Description
`Remote-AP DHCP PoolEnd`	This parameter defines the last IP address in the DHCP pool for remote APs.
`Remote-AP DHCP PoolNetmask`	Configures a DHCP pool for remote APs. This is the netmask used for the DHCP pool.
`Remote-AP uplink total bandwidth`	This is the total reserved uplink bandwidth (in kilobits per second).

`Remote-AP bw reservation 1`
`Remote-AP bw reservation 2`
`Remote-AP bw reservation 3`
	Session ACLs with uplink bandwidth reservation in kilobits per second. You can specify up to three session ACLs to reserve uplink bandwidth. The sum of the three uplink bandwidths should not exceed the `rap-bw-total` value.

`Remote-AP Local Network Access`	Shows if Remote-AP Local Network Access is enabled or disabled. By enabling this option, the clients that are connected to a remote AP can communicate. **NOTE:** By default, the Remote-AP Local Network Access will be disabled.
`Bootstrap threshold`	Number of consecutive missed heartbeats on a GRE tunnel (heartbeats are sent once per second on each tunnel) before an AP rebootstraps. On the managed device, the GRE tunnel timeout is 1.5 x bootstrap-threshold; the tunnel is torn down after this number of seconds of inactivity on the tunnel.
`Double Encrypt`	This parameter applies only to remote APs. Double encryption is used for traffic to and from a wireless client that is connected to a tunneled SSID. When enabled, all traffic is re-encrypted in the IPsec tunnel. When disabled, the wireless frame is only encapsulated inside the IPsec tunnel.
`Dump Server`	(For debugging purposes.) Displays the server to receive the core dump generated if an AP process crashes.
`Heartbeat DSCP`	DSCP value of AP heartbeats (0–63).
`Maintenance Mode`	Shows if Maintenance mode is enabled or disabled. If enabled, APs stop flooding unnecessary traps and syslog messages to the NMS or network operations centers when deploying, maintaining, or upgrading the network. The managed device still generates debug syslog messages if debug logging is enabled.
`Maximum Request Retries`	Maximum number of times to retry AP-generated requests, including keepalive messages. After the maximum number of retries, the AP either tries the IP address specified by the bkup-lms-ip (if configured) or reboots.
`Request Retry Interval`	Interval, in seconds, between the first and second retries of AP-generated requests. If the configured interval is less than 30 seconds, the interval for subsequent retries is increased up to 30 seconds.

Column	Description
Number of IPSEC retries	The number of times the AP will attempt to recreate an IPsec tunnel with Mobility Master before the AP will reboot. A value of 0 disables the reboot.
AeroScout RTLS Server	IP address of an AeroScout real-time asset location (RTLS) server.
RTLS Server configuration	This parameter contains the following information, separated by colons. ■ The IP address of the RTLS server to which the AP sends RFID tag information. ■ Number of the RTLS server port to which the AP sends RFID tag information ■ Shared secret key for the server ■ Frequency at which packets are sent to the server, in seconds
Telnet	Reports whether telnet access the AP is enabled or disabled.
RF Band for Backup	If the system profile is enabled AP console access using a backup ESSID, this parameter
Operation for Backup	This parameter allows AP console access using a backup ESSID, allowing users to access an AP console after the AP has disconnected from the managed device. When the AP advertises a backup ESSID in either static or dynamic mode, a user is able to access and debug the AP remotely through a virtual AP. This feature is disabled by default.
BLE Endpoint URL	Displays the URL of the Meridian server to which the Bluetooth Low Energy (BLE) sends monitoring data.
BLE Auth Token	Displays the BLE endpoint authorization token. This token is unique for each deployment.
BLE Operation Mode	Displays the BLE operation mode of the AP.

Starting from ArubaOS 8.2.0.0, the output of the **show ap system-profile <profile-name> | include IPM** command is modified to display a new output parameter, **IPM Steps delete all**.

```
(host) [mynode]  #show ap system-profile default | include IPM
IPM activation                              Disabled
IPM power reduction steps with priorities   N/A
IPM Steps delete all                        No
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	A new output parameter, **IPM Steps delete all**, was included in the output of the **show ap system-profile <profile-name>	include IPM** command.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap tech-support

```
show ap tech-support ap-name <ap-name> [<filename>]
```

Description

This command displays all information for an AP, or save that information to a file on the controller. This information can be used by Aruba technical support to diagnose a problem with an AP.

Syntax

Parameter	Description
`<ap-name>`	Name of the AP for which you want to view tech support data.
`<filename>`	Save the output of this command to a file on the controller with the specified filename.

Usage Guidelines

This is an internal technical support command. Aruba technical support may request that you issue this command to help analyze and troubleshoot problems with an AP or your wireless network.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap uac-database

```
show ap uac-database
```

Description

This command shows user anchor controller (UAC) AP database for cluster.

Syntax

No parameters

Examples

Execute the following command to show the UAC AP database for cluster:

```
(host) [mynode] #show ap uac-database
```

Command History

Command	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap vht-rates

```
show ap vht-rates bssid <bssid>
```

Description

Show very-high-throughput (VHT) rates for an AP that supports 802.11ac.

Syntax

Parameter	Description
`bssid <bssid>`	Show VHT rates for a specific Basic Service Set Identifier (BSSID) on an 802.11ac-capable AP. The Basic Service Set Identifier (BSSID) is usually the MAC address of the AP radio.

Examples

The output of the command below shows very-high-throughput rates for 20 Mhz, 40 Mhz and 80 Mhz data streams with and without a short guard interval (SGI).

```
(host) [mynode] #show ap vht-rates bssid 6c:f3:7f:e7:51:f0
AP "Corp-ac" Radio 0 BSSID 6c:f3:7f:e7:51:f0 Very-high-throughput Rates (Mbps)
--------------------------------------------------------------------------------
MCS  Streams  20 MHz  20 MHz SGI  40 MHz  40 MHz SGI  80 MHz   80 MHz SGI
---  -------  ------  ----------  ------  ----------  ------   ----------
0    1          6.5     7.2        13.5    15.0        29.3     32.5
1    1         13.0    14.4        27.0    30.0        58.5     65.0
2    1         19.5    21.7        40.5    45.0        87.8     97.5
3    1         26.0    28.9        54.0    60.0       117.0    130.0
4    1         39.0    43.3        81.0    90.0       175.5    195.0
5    1         52.0    57.8       108.0   120.0       234.0    260.0
6    1         58.5    65.0       121.5   135.0       263.3    292.5
7    1         65.0    72.2       135.0   150.0       292.5    325.0
8    1         78.0    86.7       162.0   180.0       351.0    390.0
9    1         --      --         180.0   200.0       390.0    433.3
0    2         13.0    14.4        27.0    30.0        58.5     65.0
1    2         26.0    28.9        54.0    60.0       117.0    130.0
2    2         39.0    43.3        81.0    90.0       175.5    195.0
3    2         52.0    57.8       108.0   120.0       234.0    260.0
4    2         78.0    86.7       162.0   180.0       351.0    390.0
5    2        104.0   115.6       216.0   240.0       468.0    520.0
6    2        117.0   130.0       243.0   270.0       526.5    585.0
7    2        130.0   144.4       270.0   300.0       585.0    650.0
8    2        156.0   173.3       324.0   360.0       702.0    780.0
9    2         --      --         360.0   400.0       780.0    866.7
0    3         19.5    21.7        40.5    45.0        87.8     97.5
1    3         39.0    43.3        81.0    90.0       175.5    195.0
2    3         58.5    65.0       121.5   135.0       263.3    292.5
3    3         78.0    86.7       162.0   180.0       351.0    390.0
4    3        117.0   130.0       243.0   270.0       526.5    585.0
5    3        156.0   173.3       324.0   360.0       702.0    780.0
6    3        175.5   195.0       364.5   405.0        --       --
7    3        195.0   216.7       405.0   450.0       877.5    975.0
8    3        234.0   260.0       486.0   540.0      1053.0   1170.0
9    3        260.0   288.9       540.0   600.0      1170.0   1300.0
-- : not valid.
Range for 20 MHz:   6.5 - 288.9 Mbps
Range for 40 MHz:  13.5 - 600.0 Mbps
```

```
Range for 80 MHz:  29.3 - 1300.0 Mbps
```

The output of this command includes the following information:

Column	Description
MCS	A Modulation Coding Scheme (MCS) values supported on this high-throughput SSID.
Streams	Number of spatial streams used by the MCS index value.
20 MHz	802.11n data rates for the MCS for 20 MHz transmissions.
20 MHz SGI	802.11n data rates for the MCS for 20 MHz transmissions using a short guard interval.
40 MHz	802.11n data rates for the MCS for 40 MHz transmissions.
40 MHz SGI	802.11n data rates for the MCS for 40 MHz transmissions using a short guard interval.
80 MHz	802.11n data rates for the MCS for 80 MHz transmissions.
80 MHz SGI	802.11n data rates for the MCS for 80 MHz transmissions using a short guard interval.

Related Commands

Command	Description
show ap ht-rates	Show high-throughput rate information for a basic service set (BSS).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
This command will only show rate information for 802.11ac-capable APs	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap virtual-beacon-report

```
show ap virtual-beacon-report {all | ap-name <ap-name> | client-mac <client-mac> | ip-addr
<ip-addr> | ip6-addr <ipv6-addr>}
```

Description

If the Client Match feature is enabled, the output of this command displays the virtual beacon report for an AP or a client with a specific IP or MAC address.

Syntax

Parameter	Description
`all`	Virtual beacon report for all clients on the controller.
`ap-name <ap-name>`	Name of the AP for which you want to view a virtual beacon report.
`client-mac <client-mac>`	MAC address of a client for which you want to view a virtual beacon report.
`ip-addr <ip-addr>`	IPv4 address of an AP for which you want to view a virtual beacon report.
`ip6-addr <ipv6-addr>`	IPv6 address of an AP for which you want to view a virtual beacon report.

Usage Guidelines

Use this command to display the client RSSI from the APs in its RF neighborhood, the channel used by each AP radio, and the number of clients associated to each radio.

Example

The example below displays the virtual beacon report for a client with MAC address 24:77:03:d1:24:b8.

```
(host) [mynode] #show ap virtual-beacon-report client-mac 24:77:03:d1:24:b8

Client MAC :24:77:03:d1:24:b8
Current association :1260-205 (9c:1c:12:fe:0f:d0)
Steer attempts/Success :2/1
Consecutive (Fails/BTM Rej/BTM Timeouts) :0/0/0
Bandsteer window (Steers/Start time/Expiry time) :0/0/0
Client Device Type :Win 7
Current state :Steerable
Client Supported Channels :{36,4}{52,4}{100,11}{149,4}{165,1}
Current Time :Oct 29 15:56:06 2014

STA Beacon Report
-----------------
AP        IP address     Radio              ESSID             Signal (dBm)  Last update
Add time         Channel/EIRP/Clients  Flag
--        ----------     -----              -----             ------------  -----------      -
-------         --------------------  ----
1310-205  10.100.66.102  9c:1c:12:fd:f7:b0  ethersphere-wpa2  -64           Oct 29 15:55:59
Oct 29 09:21:56  44/20/38
1248-205  10.100.66.128  9c:1c:12:fe:19:f0  ethersphere-wpa2  -85           Oct 29 15:56:04
Oct 29 09:22:08  60/24/15
1263-205  10.100.66.126  9c:1c:12:fd:d2:10  ethersphere-wpa2  -63           Oct 29 15:55:38
Oct 29 09:22:12  52/12/0
```

```
1263-205  10.100.66.126  9c:1c:12:fd:d2:00  ethersphere-wpa2  -61          Oct 29 15:55:38
Oct 29 09:22:12  1/12/1
1362-205  10.100.66.127  9c:1c:12:fd:f2:30  ethersphere-wpa2  -53          Oct 29 15:55:55
Oct 29 15:23:35  52/12/5
1263-ac   10.100.66.121  6c:f3:7f:e7:5a:b0  ethersphere-wpa2  -55          Oct 29 15:55:54
Oct 29 09:22:17  60/18/7
AP205-TE  10.100.66.124  9c:1c:12:fd:e4:d0  ethersphere-wpa2  -69          Oct 29 15:55:36
Oct 29 09:22:21  40/20/15
1372-205  10.100.66.120  9c:1c:12:fe:13:50  ethersphere-wpa2  -63          Oct 29 15:55:33
Oct 29 09:22:23  52/12/11
1310-205  10.100.66.102  9c:1c:12:fd:f7:a0  ethersphere-wpa2  -66          Oct 29 15:52:00
Oct 29 09:23:02  1/12/4                S
1263-ac   10.100.66.121  6c:f3:7f:e7:5a:a0  ethersphere-wpa2  -51          Oct 29 15:55:54
Oct 29 09:23:22  1/12/1
1242-205  10.100.66.123  9c:1c:12:fd:d1:30  ethersphere-wpa2  -70          Oct 29 15:55:36
Oct 29 09:23:24  40/19/6
AP205-TE  10.100.66.124  9c:1c:12:fd:e4:c0  ethersphere-wpa2  -76          Oct 29 15:55:36
Oct 29 09:23:27  1/12/0
1372-205  10.100.66.120  9c:1c:12:fe:13:40  ethersphere-wpa2  -75          Oct 29 15:54:58
Oct 29 09:23:29  1/12/2
1260-205  10.100.66.100  9c:1c:12:fe:0f:d0  ethersphere-wpa2  -63          Oct 29 15:55:45
Oct 29 09:24:07  52/12/6               *
1260-205  10.100.66.100  9c:1c:12:fe:0f:c0  ethersphere-wpa2  -59          Oct 29 15:55:45
Oct 29 09:25:47  1/12/0
1362-205  10.100.66.127  9c:1c:12:fd:f2:20  ethersphere-wpa2  -55          Oct 29 15:54:47
Oct 29 15:24:38  1/12/1
1248-205  10.100.66.128  9c:1c:12:fe:19:e0  ethersphere-wpa2  -81          Oct 29 15:29:57
Oct 29 10:10:30  1/12/1                S
1242-205  10.100.66.123  9c:1c:12:fd:d1:20  ethersphere-wpa2  -69          Oct 29 15:44:03
Oct 29 10:58:40  1/12/0                S
VBR Flags *-Associated S-Stale U-Unsupported Channel
```

The output of this command includes the following parameters:

Parameter	Description
`Client MAC`	MAC address of the client.
`Current association`	MAC address of the AP radio to which the client is currently associated.
`Steer attempts/Success`	Number of steer attempts, and the number of successful steers.
`Consecutive (Fails/BTM Rej/BTM Timeouts)`	Consecutive number of failed steer attempts, rejected BSS Transition Management Requests, and BSS Transition Management timeouts.
`Bandsteer window (Steers/Start time/Expiry time)`	Number of band steers, the start time of the band steer, and the expiry time of band the steer.
`Client Device Type`	Type of device used by the client (for example, Windows).
`Current State`	Indicates whether the client is currently steerable.
`Client Supported Channels`	Lists the channels that support client use.
`Current Time`	Timestamp showing the current date and time.

Parameter	Description
AP	Name of the AP from which the client can detect a signal.
IP address	IP address of the AP from which the client can detect a signal.
Radio	MAC address of the AP radio from which the client can detect a signal.
ESSID	Identifying name of the wireless network for each AP.
Signal (dBm)	Signal strength, in dBm, from the AP radio.
Last Update	Time that the virtual beacon report last updated information for the AP radio.
Add Time	Date and time the client is successfully steered and added to the AP.
Channel/EIRP/Clients	Channel used by the AP radio, the amount of power transmitted from the AP antennae, and the number of clients associated to it.
Flag	The output of this column shows the following values: ■ *: Flag indicating that the client is currently associated to this AP ■ S: Flag indicating a stale entry, with the last client update from this radio produced 120+ seconds ago ■ U: Flag indicating that the client does not support the channel the radio is currently operating on

The following example displays a virtual beacon report for all clients in the network.

```
(host) [mynode] #show ap virtual-beacon-report all

Client MAC :60:d9:c7:a2:42:cb
Current association :1260-205 (9c:1c:12:fe:0f:d2)
Steer attempts/Success :0/0
Consecutive (Fails/BTM Rej/BTM Timeouts) :0/0/0
Bandsteer window (Steers/Start time/Expiry time) :0/0/0
Client Device Type :Unknown
Current state :Steerable
Active media sessions: No
Client Supported Channels :{36,4}{52,4}{100,11}{149,4}{165,1}
Current Time :Oct 29 12:38:35 2014

STA Beacon Report
-----------------
AP        IP address     Radio              ESSID            Signal (dBm)  Last update
Add time         Channel/EIRP/Clients  Flag
--        ----------     -----              -----            ------------  -----------      --
------         --------------------  ----
1372-205  10.100.66.120  9c:1c:12:fe:13:50  ethersphere-psk  -67           Oct 29 12:38:22
Oct 29 07:19:33  52/21/10
1260-205  10.100.66.100  9c:1c:12:fe:0f:d0  ethersphere-psk  -53           Oct 29 12:38:18
Oct 29 07:19:44  52/24/15              *
1263-ac   10.100.66.121  6c:f3:7f:e7:5a:b0  ethersphere-psk  -73           Oct 29 07:20:52
Oct 29 07:19:49  52/12/5               S
1362-205  10.100.66.127  9c:1c:12:fd:f2:30  ethersphere-psk  -73           Oct 29 07:57:21
Oct 29 07:52:31  60/12/12              S
1310-205  10.100.66.102  9c:1c:12:fd:f7:b0  ethersphere-psk  -80           Oct 29 10:36:15
Oct 29 07:52:51  44/20/34              S
1263-205  10.100.66.126  9c:1c:12:fd:d2:10  ethersphere-psk  -67           Oct 29 08:42:20
Oct 29 08:22:32  60/12/4               S
```

The output of this command includes the additional `Active Media Sessions` parameter, which indicates whether the client is involved in any active media sessions.

Related Commands

Command	Description
rf arm-profile	Configures the Adaptive Radio Management (ARM) profile.
show ap arm client-match probe-report	Displays additional statistics for the Client Match feature.
show ap arm client-match restriction-table	Displays additional statistics for the Client Match feature.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap vlan-mcast

```
show ap vlan-mcast [{ap-name <ap-name> | bssid <bssid> | ip-addr <ip-addr> | ip6-addr <ip6-addr}]
```

Description

This command shows the user count in each VLAN and timestamps for tunnel to join or leave vlan-mcast group.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show user count VLAN data for a specific AP name.
`bssid <bssid>`	Show user count VLAN data for a specific MAC address.
`ip-addr <ip-addr>`	Show user count VLAN data for a specific IP address.
`ip6-addr <ip6-addr>`	Show user count VLAN data for a specific IPv6 address.

Examples

Execute the following command to show the user count in each VLAN:

```
(host)[mynode] #show ap vlan-mcast
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap vlan-usage

```
show ap vlan-usage [{ap-name <ap-name> | bssid <bssid> | essid <essid> | ip-addr <ip-addr> |
ip6-addr <ip6-addr> | virtual-ap <virtual-ap}
```

Description

Show the numbers of clients on each VLAN.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show VLAN data for an AP with a specific name.
`bssid <bssid>`	Show VLAN data for a specific Basic Service Set Identifier (BSSID) on an AP. The Basic Service Set Identifier (BSSID) is usually the MAC address of the AP.
`essid <essid>`	Show VLAN data for a specific Extended Service Set Identifier (ESSID). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	Show VLAN data for an AP with a specific IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	Show VLAN data for an AP with a specific IPv6 address by entering an IP address in dotted-decimal format.
`virtual-ap <virtual-ap>`	Show VLAN pool allocation by VAP name.

Examples

The output of this command displays the **VLAN Usage** table.

```
(host) [mynode] #show ap vlan-usage
VLAN Usage Table
----------------
VLAN ID  Clients
-------  -------
64       1
65       32
66       44
```

The output of this command includes the following information:

Parameter	Description
`VLAN ID`	ID number of the wireless VLAN.
`Clients`	Number of clients currently using the specified VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wired-ap-profile

```
show ap wired-ap-profile [<profile-name>]
```

Description

Show a list of all wired AP profiles, or display the configuration parameters in a specific wired AP profile.

Syntax

Parameter	Description	Default
`<profile-name>`	Name of a wired AP profile.	default

Usage Guidelines

The command `show ap wired-ap-profile` displays a list of all wired AP profiles, including the number of references to each profile and the profile status. If you include the optional `<profile-name>` parameter, the command will display detailed information for that one profile.

Example

The output of this command shows the configuration parameters for the wired AP profile “default”.

```
(host) [mynode] #show ap wired-ap-profile default

Wired AP profile "default"
--------------------------
Parameter                 Value
---------                 -----
Wired AP enable           Disabled
Trusted                   not trusted
Forward mode              tunnel
Switchport mode           access
Access mode VLAN          1
Trunk mode native VLAN    1
Trunk mode allowed VLANs  1-4094
Broadcast                 Broadcast
```

The output of this command includes the following information:

Column	Description
`Wired AP enable`	Indicates whether the wired AP profile is **enabled** or **disabled**.
`Forward mode`	The configured forward mode for the profile. ■ **bridge**: Bridge locally ■ **split-tunnel**: Tunnel to controller or NAT locally ■ **tunnel**: Tunnel to controller
`Switchport mode`	The profile’s switching mode. ■ **access**: Set access mode characteristics of the interface. ■ **mode**: Set trunking mode of the interface. ■ **trunk**: Set trunk mode characteristics of the interface.
`Access mode VLAN`	VLAN ID of the access mode VLAN.

Column	Description
`Trunk mode native VLAN`	VLAN ID of the native VLAN.
`Trunk mode allowed VLANs`	Range of allowed VLAN IDs for the native VLAN.
`Trusted`	Shows if the wired port on an AP using this profile is a trusted port. Possible values are **Trusted** or **Not Trusted**.
`Broadcast`	If set to **broadcast**, the wired AP port will forward broadcast traffic. If the parameter displays **Do Not Broadcast**, broadcast traffic will not be forwarded.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wired-port-profile

```
show ap wired-port-profile [<profile-name>]
```

Description

Shows all AP wired port profiles and their status.

Syntax

Parameter	Description	Default
<profile-name>	Name of a wired AP profile.	default

Example

The example below shows that the controller has three wired port profiles. The **References** column lists the number of other profiles with references to the wired port profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] #show ap  wired-port-profile

AP wired port profile List
--------------------------
Name              References  Profile Status
----              ----------  --------------
default           3
NoAuthWiredPort   4           Predefined (editable)
shutdown          3           Predefined
Total:3
```

The following command displays information for an individual wired port profile:

```
(host)[mynode] #show ap wired-port-profile default

AP wired port profile "default"
-------------------------------
Parameter                                   Value
---------                                   -----
Wired AP profile                            default
Ethernet interface link profile             default
AP LLDP profile                             default
Shut down                                   No
Remote-AP Backup                            Enabled
AAA Profile                                 N/A
Time to wait for authentication to succeed  20 sec
Loop Protect Enable                         Disabled
Loop Detection Interval                     1
Loop Protect Auto Recovery Enable           Disabled
Loop Protect Auto Recovery Interval         300
Storm Control Broadcast                     Disabled
Storm Control Broadcast Threshold           2000
```

The output of this command includes the following information:

Parameter	Description
`Wired AP profile`	Name of a wired AP profile to be used by devices connecting the AP's wired port. The wired AP profile defines the forwarding mode and switchport values used by the port.
`Ethernet interface link profile`	An Ethernet Link profile to be used by devices connecting to the AP's wired port profile. This profile defines the duplex value and speed to be used by the port.
`AP LLDP Profile`	Name of an LLDP Profile associated with this wired port.
`Shut Down?`	Shows if the wired AP port is enabled (no) or disabled (yes).
`Remote AP Backup`	Use the rap-backup parameter to use the wired port on a Remote AP for local connectivity and troubleshooting when the AP cannot reach the controller. If the AP is not connected to the controller, no firewall policies will be applied when this option is enabled. (The AAA profile will be applied when the AP is connected to controller).
`AAA Profile`	Name of a AAA profile to be used by devices connecting to the wired port of the AP.
`Time to wait for authentication to succeed`	Authentication timeout value, in seconds, for devices connecting the AP's wired port. The supported range is 1–65535 seconds, and the default value is 20 seconds.
`Loop Protect Enable`	Shows if loop protection is enabled or disabled.
`Loop Detection Interval`	Shows time in seconds after which a loop detection packet is transmitted on the AP port.
`Loop Protect Auto Recovery Enable`	Show if automatic recovery of the port in the AP that is shut down because of loop protection is enabled or disabled.
`Loop Protect Auto Recovery Interval`	Shows time in seconds after which automatic recovery of the port in the AP that is shut down because of loop protection is attempted.
`Storm Control Broadcast`	Shows if broadcast storm control is enabled or disabled.
`Storm Control Broadcast Threshold`	Shows broadcast packets per second on each Ethernet port of an AP before the Ethernet port is shut down.

Command History

Release	Modification
ArubaOS 8.3.0.0	Following parameters were introduced: ■ Loop Protect Enable ■ Loop Detection Interval ■ Loop Protect Auto Recovery Enable ■ Loop Protect Auto Recovery Interval ■ Storm Control Broadcast ■ Storm Control Broadcast Threshold
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wired stats

```
show ap wired stats {ap-name <ap-name> | ip-addr <ip-addr>} [client-ip <client-ip> | client-mac <client-mac>]
```

Description

This command shows statistics for campus and remote AP wired clients.

Syntax

Parameter	Description
`ap-name <ap-name>`	Show wired AP statistics for a specified AP name.
`ip-addr <ip-addr>`	Show wired AP statistics for a specified AP by entering an IP address in dotted-decimal format.
`client-ip <client-ip>`	Show wired AP statistics for a specified client IP address.
`client-mac <client-mac>`	Show wired AP statistics for a specified client MAC address.

Example

```
(host) [mynode] # show ap wired stats ap-name rap5wn client-mac 00:14:d1:19:3c:0b

AP Wired User Statistics
------------------------
Counter               Value
-------               -----
Slot                  0
Port                  1
VLAN                  1
TX Packets            78
TX Bytes              7894
RX Packets            37
RX Bytes              5352
TX Broadcast Packets  36
TX Broadcast Bytes    4410
TX Multicast Packets  22
TX Multicast Bytes    1990
```

The output of this command includes the following information:

Parameter	Description
`Slot`	Slot number
`Port`	Port number
`VLAN`	Associated VLAN number
`TX Packets`	Number of packets sent
`TX Bytes`	Number of bytes sent
`RX Packets`	Number of packets received

Parameter	Description
`RX Bytes`	Number of bytes received
`TX Broadcast Packets`	Number of broadcast packets sent
`TX Broadcast Bytes`	Number of broadcast bytes sent
`TX Multicast Packets`	Number of multicast packets sent
`TX Multicast Bytes`	Number of multicast bytes sent

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap wmm-flow

```
show ap wmm-flow [ap-name <ap-name> | bssid <bssid> |  dotlla | dotllg | essid <essid> | ip-addr <ip-addr> | ip6-addr <ip6-addr>]
```

Description

This command shows the Wireless Multimedia (WMM) flow table.

Syntax

Parameter	Description
`ap-name <ap-name>`	View an AP with a specified name.
`bssid <bssid>`	View data for an AP with a specific BSSID (Basic Service Set Identifier). The Basic Service Set Identifier (BSSID) is usually the MAC address of the AP.
`dot11a`	Show the WMM flow table for a 802.11a radio.
`dot11g`	Show the WMM flow table for a 802.11g radio.
`essid <essid>`	View data for a specific ESSID (Extended Service Set Identifier). An Extended Service Set Identifier (ESSID) is a alphanumeric name that uniquely identifies a wireless network. If the name includes spaces, you must enclose the ESSID in quotation marks.
`ip-addr <ip-addr>`	View an AP with a specified IP address by entering an IP address in dotted-decimal format.
`ip6-addr <ip6-addr>`	View an AP with a specified IPv6 address by entering an IPv6 address in dotted-decimal format.

Usage Guidelines

WMM, or Wireless Multimedia Extensions, are a subset of the 802.11e standard. WMM provides for four different types of traffic classification: voice, video, best effort, and background, with voice having the highest priority and background the lowest. Issue the **show ap wmm-flow** command to view WMM flow data for all APs. Include any of the optional parameters described in the table above to filter the table by a specific AP, radio channel (a or g), or both AP and radio type.

Example

Some samples of executing this command with various options are as follows:

```
(host) [mynode] #show ap wmm-flow ap-name ap105
(host) [mynode] #show ap wmm-flow ap-name ap105 dot11g
(host) [mynode] #show ap wmm-flow dot11a
```

The following example shows WMM flow data for all APs.

```
(host)[mynode] #show ap wmm-flow

WMM Flow Table
--------------
AP Name    ESSID  Client            Description
-------    -----  ------            -----------
AP125-srk  NOE    00:90:7a:06:1f:5b  tsid 6:prio 6:inactivity 2157352960
us:bidir:apsd:normalack:tclas prio 6 ip DIP-192.168.101.194 DP-32514 DSCP-48:one-match
```

```
AP125-srk  NOE    00:90:7a:06:1f:5b  tsid 0:prio 0:inactivity 100000000
us:bidir:apsd:normalack:no-match
Num Flows:0
```

The output of this command includes the following parameters:

Parameter	Description
`AP name`	Name of an AP with recorded WMM flows
`ESSID`	Extended Service Set Identifier (ESSID) of a wireless network.
`Client`	MAC address of the client.
`Description`	The description is a long string that includes the following information. **TSID:** Traffic Stream Identifier. The TSID should match the priority level for each flow. **Priority**: One of the following IEEE 802.1p priority values: ■ 0,3 = Best Effort ■ 1,2 = Background ■ 4-5 = Video ■ 6-7 = Voice **Inactivity**: Tspec inactivity threshold, in microseconds. **<country code>**: AP country code, e.g., US. **bdir**: flow is bidirectional. **apsd**: flow has enabled auto power save delivery. **<ack>**: Displays the ack policy negotiated for the flow. Possible values are: ■ normalack ■ noack ■ blockack ■ resack (reserved ack) **Tclas**: traffic classification element. Tclas information includes one of the following classification types, the 802.1p priority and IP version (version 4 or version 6) ■ **type0**: Classification based on Ethernet parameters ■ **type1**: Classification based on TCP/UDP or IP parameters (IPv4 or IPv6) ■ **type2**: Classification based on based on IEEE802.1Q **DIP**: Destination IP address for the flow. **DP**: Destination IP Port specified in the TCLAS for flow negotiation. **DCSP**: The Differentiated Services Code Point (DSCP) priority value that matches the flows 802.1p priority.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the managed device or controller where the AP terminates.

show ap-crash-transfer

```
show ap-crash-transfer
```

Description

This command displays info for the AP crash transfer feature, which transfers AP coredump files to the controller flash memory if no dumpserver is configured.

Syntax

No Parameters

Usage Guidelines

The command **ap system-profile <profile> dump-server <server>** specifies a server to receive a core dump generated when an AP process crashes. If no dump server is configured, issue the **ap-crash-transfer** command to save dump files to the controller flash memory.

If you define a dump server and issue the ap-crash-server command, the dump server configuration takes precedence, and coredump files are sent to the dump server.

Example

```
(host)) #show ap-crash-transfer
AP Crash Transfer:enabled
AP Crash folder limit:50 MB (non-editable)
```

Related Commands

Command	Description
ap-crash-transfer	This command allows AP coredump files to be transferred to the controller flash memory if no dumpserver is configured.

Command History

Release	Modification
ArubaOS 8.0.0.0	This command is introduced.

Command Information

Platforms	License	Mode
All platforms	Base operating system	Enable or config mode on managed devices

show arp

```
show arp [counters | vlan <vlanid>
```

Description

This command show Address Resolution Protocol (ARP) entries for the controller.

Syntax

Parameter	Description	Range
`counters`	Shows ARP information on ARP counters.	—
`vlan <vlanid>`	Shows ARP information for a VLAN Interface Number.	1–4094

Example

This example shows configured static ARP entries for the controller.

```
(host) [mynode] #show arp
Protocol        Address         Hardware Address        Interface
Internet        10.3.129.98     00:1A:1E:C0:80:28       vlan1
Internet        10.3.129.253    00:0B:86:42:35:80       vlan1
Internet        10.3.129.250    00:1A:92:45:DB:00       vlan1
Internet        10.3.129.99     00:1A:1E:C0:1C:60       vlan65
Internet        10.3.129.96     00:1A:1E:C0:80:1E       vlan65
Internet        10.3.129.254    00:0B:86:02:EE:00       vlan1
```

The output of this command includes the following parameters:

Parameter	Description
`Protocol`	Protocol using ARP. Although the controller will most often use ARP to translate IP addresses to Ethernet MAC addresses, ARP may also be used for other protocols, such as Token Ring, FDDI, or IEEE 802.11, and for IP over ATM.
`Address`	IP address of the device.
`Hardware Address`	MAC address of the device.
`Interface`	Interface used to send ARP requests and replies.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show audit-trail

```
show audit-trail [history | login <number>| <number>]
```

Description

Show the controller's audit trail log.

Syntax

Parameter	Description	Range
`history`	Shows audit trail history log.	—
`login <number>`	Starts displaying the log output from the specified number of lines from the end of the login or logout log.	1–65535
`<number>`	Starts displaying the log output from the specified number of lines from the end of the log.	1–65535

Example

By default, the audit trail feature is enabled for all commands in configuration mode. The example below shows the most recent ten audit log entries for the managed device.

```
(host) [mynode] #show audit-trail 10
Feb  5 06:13:17  cli[1239]: USER: admin has logged in from 10.240.16.118.
Feb  5 06:20:13  cli[1239]: USER: admin connected from 10.240.16.118 has logged out.
Feb  5 06:24:37  cli[1239]: USER: admin has logged in from 10.240.16.118.
Feb  5 06:37:01  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mp-only" no vap-
enable > -- command executed successfully
Feb  5 06:37:14  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mp-a-only" no
vap-enable > -- command executed successfully
Feb  5 06:37:20  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "default" no vap-
enable > -- command executed successfully
Feb  5 06:37:29  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mpp-a-only" no
vap-enable > -- command executed successfully
Feb  5 06:46:10  cli[1239]: USER:admin@10.3.129.250 COMMAND:<interface gigabitethernet "1/2"
port monitor igigabitethernet "1/1" > -- command executed successfully
Feb  5 06:57:44  cli[1239]: USER:admin@10.3.129.250 COMMAND:<ap system-profile "default"
heartbeat-dscp 12 > -- command executed successfully
Feb  5 07:05:48  cli[1239]: USER:admin@10.3.129.250 COMMAND:<wlan virtual-ap "mp-a-only" vap-
enable > -- command executed successfully
```

Related Commands

Command	Description
audit-trail	Enable or disable the audit trail feature using the command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show auth-survivability

```
show auth-survivability
```

Description

This command displays the **auth-survivability** parameters that are configured in the managed device.

Example

```
host # show auth-survivability
Auth-Survivability: Enabled (Running)
Survival-Server Server-Cert: dot1x2k-server
```

Survival-Server Cache lifetime: 48 hours

Command History

Command	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show auth-survivability-cache

```
show auth-survivability-cache
```

Description

This command displays the data currently in the local Survival Server cache.

Example

```
host(config) # show auth-survivability-cache
```

Figure 1 *Displaying the Local Survival Server Cache*

```
(C) # show aaa auth-survivability-cache

Auth-Survivability Cached Data
------------------------------
Station       User Name              Authenticated Using  Authenticated By  Authenticated On
-------       ---------              -------------------  ----------------  ----------------
6427377FBC34  test1                  PAP                  RadServer1        2014-04-01 01:54
642739AFBCF0  vpnclientcert2K-xyz     EAP-TLS              RadServer2        2014-04-01 18:21
101C0C6CB16D  testcp                 QUERY                RadServer3        2014-04-01 10:07

(C) #
```

Command History

Command	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	base operating system	Enable or Config mode on Mobility Master

show auth-tracebuf

```
show auth-tracebuf [count <1-250] | [failures] | mac <address>]
```

Description

This command shows the trace buffer for authentication events.

Syntax

Parameter	Description	Range
`count <number>`	Limits the output of the command to the specified number of packets.	1–250
`failures`	Filters the output of this command to display only authentication failures	—
`mac <address>`	Filters the output of this command to display only information for a specified MAC address.	—

Usage Guidelines

Use the output of this command to troubleshoot 802.1X authentication errors. Include the **<address>** parameter to filter data by the MAC address of the client which is experiencing errors. This command can tell you, for example, when 802.1X authentication completed and when keys were plumbed correctly.

Example

The example below shows the most recent ten trace buffer entries for the controller. Each row includes the following information:

```
(host) [mynode] # show auth-tracebuf count 10
Auth Trace Buffer
-----------------
Feb  5 08:08:29  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic
failure
Feb  5 08:08:30  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:30  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic
failure
Feb  5 08:08:31  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:31  station-down          *   00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -
Feb  5 08:08:31  station-up            *   00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -    wpa2
psk aes
Feb  5 08:08:31  station-data-ready    *   00:09:ef:05:1e:b2  00:00:00:00:00:00  66  -
Feb  5 08:08:31  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:31  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic
failure
Feb  5 08:08:32  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:32  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic
failure
Feb  5 08:08:33  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:33  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic
failure
Feb  5 08:08:34  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
Feb  5 08:08:34  wpa2-key2            ->  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   119  mic
failure
Feb  5 08:08:35  wpa2-key1            <-  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   117
```

```
Feb  5 08:08:35  station-down           *  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -
Feb  5 08:08:35  station-up             *  00:09:ef:05:1e:b2  00:1a:1e:97:e5:42  -   -    wpa2
psk aes
Feb  5 08:08:35  station-data-ready     *  00:09:ef:05:1e:b2  00:00:00:00:00:00  66  -
```

Each row in the output of this table may include some or all of the following information:

- A timestamp that indicates when the entry was created
- The type of exchange that was made
- The direction the packet was sen
- The source MAC address
- The destination MAC address
- BSSID/Server Name
- The packet number
- The packet length
- Additional information (if available); for example, username, encryption and WPA type, or reason for failure

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show banner

```
show banner
show bannervia
```

Description

This command shows the current login banner.

Syntax

Parameter	Description
`banner`	Displays the Message of the Day banner.
`bannervia`	Displays the VIA login banner message.

Usage Guidelines

Issue this command to review the banner message that appears when you first log in to the controller's command-line or browser interfaces.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

```
(host) [mynode]# show banner
This testlab controller is scheduled for maintenance starting Saturday night at 11 p.m.
```

Related Commands

Command	Description
banner motd	Configures a banner message.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show ble_relay disp-attr

```
show ble relay disp-attr all
```

Description

This command shows the BLE relay attributes.

Syntax

Parameter	Description	Range	Default
`all`	Displays all the attributes.	—	—

Example

The following example displays the BLE relay attributes:

```
(host) [mynode] #show ble_relay disp-attr all
=============================================================
WebSocket Connect Request               : Yes
Tag Logging                             : Off
LogLevel                                : 31
Note: Loglevel List: Error (0x1), Warn (0x2), Notice (0x4), Info (0x8),
Debug (0x10), Parser (0x20), Header (0x40), Ext (0x80), Client (0x100), Latency (0x200).
```

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

show ble_relay iot-profile

```
show ble relay iot-profile
```

Description

This command shows the BLE relay IoT profile details.

Syntax

No parameters.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

show ble_relay jobs

```
show ble relay jobs
```

Description

This command shows the Bluetooth Low Energy (BLE) relay job queue status.

Syntax

No parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

show ble_relay tag-report

```
show ble relay tag-report <profile-name>
```

Description

This command shows the BLE relay tag data.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the IoT profile.	—	—

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

show ble_relay ws-log

```
show ble relay ws-log <profile-name>
```

Description

This command shows the BLE relay work queue session logs of each IoT transport profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the IoT profile.	—	—

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on the Mobility Master

show block-redirect-url

```
block-redirect-url <string>
```

Description

This command show redirect URL for blocked content.

Syntax

No parameters.

Example

Execute the following command to display the redirect URL for blocked content.

```
(host) [mynode] (config) #show block-redirect url
```

Related Command

Command	Description
block-redirect-url	Defines the redirect URL for blocked content.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show bocmgr

```
show bocmgr instance
   instance {device <device-id>}{interface tunnel|vlan {intf-id <intfid>}|<nodepath>| {pool
   dhcp|tunnel|vlan {pool-name <pool-name>}|<nodepath>}
   pool {dhcp|intf|tunnel|vlan {pool-name <pool-name>}|<nodepath>}|{intf tunnel|vlan {intf-id
   <intfid>}|<nodepath>}
```

Description

Show details about dynamic VLAN, tunnel and DHCP pools

Syntax

Parameter	Description
`device <device-id>`	Show pools information for a device with the specified MAC address (device ID).
`interface tunnel|vlan`	Show pool information for a specific tunnel or vlan
`intf-id <intfid>`	Show pool information for the specified tunnel or interface ID
`<nodepath>`	Show pool information for a configuration node at the specified path. (For example, /md/west/sunnyvale.)
`pool dhcp|tunnel|vlan`	Show pool information for the specified pool type.
`pool-name <pool-name>`	Show a list of devices using the specified pool.
`<nodepath>`	Show pool information for a configuration node at the specified path. (For example, /md/west/sunnyvale.)
`pool dhcp|{[intf]tunnel|vlan}`	Show pool information for the specified interface or pool type.
`pool-name <pool-name>`	Show details about a pool with the specified pool name
`intf-id <intfid>`	Display pool details info for the specified tunnel or interface ID
`<nodepath>`	Display pool details info for a configuration node at the specified path. (For example, /md/west/sunnyvale.)

Usage Guidelines

Command	Description
ip dhcp pool	Configures DHCP.
ip tunnel	Configures tunnel.
ip vlan	Configures VLAN pools.

Example

The following command shows the DHCP pool used by the configuration /md/east.

```
(host) [md])#show bocmgr instance pool dhcp /md/east
DHCP Instance(s)
----------------
```

```
Device Name        Pool Name   Net         Mask             Vlan Id  Vlan IP
-----------        ---------   ---         ----             -------  -------
00:0b:86:99:88:17  testpool    4.1.0.0     255.255.255.192  2        4.1.0.1
00:0c:29:0e:56:65  testpool    4.1.0.64    255.255.255.192  2        4.1.0.65
00:0b:86:be:81:30  testpool    4.1.0.128   255.255.255.192  2        4.1.0.129
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on the Mobility Master

show boot

```
show boot [history]
```

Description

Display boot parameters, including the boot partition and the configuration file to use when booting the controller.

Syntax

Parameter	Description
`history`	Displays the controller's reloads and upgrade history.

Example

```
(host) [mynode] #show boot history
Reboot History Table
--------------------
No  Description

User      Role  IP              Timestamp
----      --------              ---------
1   Upgrade Failed:while downloading image:ArubaOS_SC_8.0.0.0-svcs-ctrl_54589
admin     root  10.20.104.237   Thu Apr 14 21:57:01 2016
2   Upgrade to ArubaOS_SC_8.0.0.0-svcs-ctrl_54589 on partition 1 Successful.
admin     root  10.20.104.237   Thu Apr 14 22:07:39 2016
3   Controller Reboot initiated.                                        admin     root
10.20.104.237   Thu Apr 14 22:08:01 2016
4   Reboot Cause: User reboot.                                          user      root
10.11.8.227     Thu Apr 14 22:09:45 2016
```

Related Commands

Command	Description
boot	Configures boot parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show bulkedit

```
show bulkedit {headers | status}
```

Description

This command shows the bulkedit information such as the list of supported bulkedit headers or the status of the last bulkedit transaction.

Syntax

Parameter	Description
`headers`	Show list of supported bulkedit headers.
`status`	Show status of last bulkedit transaction.

Example

The following are examples of executing the **show bulkedit** command:

```
(host) [mynode] #show bulkedit headers
(host) [mynode] #show bulkedit status
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config modes on the managed device or the Mobility Master

show ccm-debug memory-usage

```
show ccm-debug memory-usage {non-profile | profile}
```

Description

This command shows the memory usage information.

Syntax

Parameter	Description
`show ccm-debug memory-usage`	Shows memory usage information.
`non-profile`	Shows memory usage - non-profile command.
`profile`	Shows memory usage - profile command.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example for executing this command:

```
(host) [mynode] #show ccm-debug memory-usage profile
```

Related Commands

Command	Description
ccm-debug	**ccm-debug config-rollback**—Rolls back the configuration of a node to the previous version. **ccm-debug full config sync**—Request a full configuration sync.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on the managed device or the Mobility Master

show cellular profile

```
show cellular profile [factory]
```

Description

This command display the cellular profiles and profile settings.

Syntax

Parameter	Description
`show cellular profile`	Displays the Cellular Profile table.
`factory`	Displays a list of factory-supported cellular profiles.

Usage Guidelines

Execute this command to display configuration parameters for the entire list of available cellular profiles. Include history to display configuration information for factory-supported cellular profiles.

Example

The output of this command displays the Cellular Profile table. The example below shows eight preconfigured cellular profiles.

```
(host) [mynode] #show cellular profile

Cellular Profile Table
----------------------
Name                   Vend      Prod      Serial  Dialer   Tty      Driver  Priority  Modeswitch
----                   ----      ----      ------  ------   ---      ------  --------  ----------
Novatel_U720           1410      2110              evdo_us  ttyUSB0  option  default
Novatel_U727           1410      4100              evdo_us  ttyUSB0  option  default
Kyocera_KPC680         0c88      180a              evdo_us  ttyUSB0  option  default
Sierra_Compass_597     1199      0023              evdo_us  ttyUSB0  sierra  default
Pantech_UM175          106c      3714              evdo_us  ttyUSB1  option  default
Sierra_USBConn_881     1199      6856              gsm_us   ttyUSB0  option  default
USBConn_Mercury_C885   1199      6880              gsm_us   ttyUSB3  option  default
Globetrotter_Icon322   0af0      d033              gsm_us   ttyHS3   hso     default
Default cellular priority:       100
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of a cellular profile.
`Vend`	Vendor ID in hexadecimal
`Prod`	USB product ID in hexadecimal
`Serial`	USB device serial number.

Parameter	Description
`Dialer`	Name of a dialer group profile.
`TTY`	Modem TTY port.
`Driver`	One of the following cellular modem drivers: ■ acm: Linux ACM driver. ■ hso: Option High Speed driver. ■ option: Option USB data card driver (default). ■ sierra: Sierra Wireless driver.
`Priority`	Displays the cellular profile priority; profiles with the default priority of 100 will display the word default in the Priority column Range: 1 to 255. Default: 100
`Modeswitch`	One of two USB device mode switch settings: ■ eject: Eject the CDROM device. ■ rezero: Send SCSI CDROM rezero command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
600 Series	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show clock

```
show clock [cli-timestamp|timezone]
```

Description

This command shows the configuration for the system clock, summer daylight savings configuration, timezone configuration, and gives details if the CLI-timestamp is enabled or disabled.

Syntax

Parameter	Description
`cli-timestamp`	Shows if clock cli-timestamp is enabled or disabled.
`summer-time`	Shows summer (daylight savings) time settings.
`timezone`	Show the configured timezone for the managed device.

Usage Guidelines

Include the optional summer-time parameter to display configured daylight savings time settings. The timezone parameter shows the current timezone, with its time offset from Greenwich Mean Time.

Example

The output below shows the current zone time on the managed device clock.

```
(host) [mynode] #show clock timezone
   clock timezone PST -8
```

Related Commands

Command	Description
clock summer-time recurring	Configures daylight savings /summer time settings
clock timezone	Configures the timezone for the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices

show cluster-config

```
show cluster-config
```

Description

This command show the cluster configuration for the control plane security feature.

Syntax

No parameter.

Usage Guidelines

When you issue this command from the cluster *root*, the output of this command shows the cluster role of the managed device, and the IP address of each member node in the cluster.

When you issue this command from a cluster *member*, the output of this command shows the cluster role of the managed device, and the IP address of the cluster root.

Example

In the example below, the **Cluster Role** section in the output of this command shows that the managed device on which the command was issued is the cluster root. The **Cluster IPSEC Controllers** section of the output shows the IP address of each cluster member.

```
(host) [mynode] (config) #show cluster-config

Cluster Role
------------
Root
----

Cluster IPSEC Controllers
-------------------------
Switch IP address of Cluster-Members  Key
-----------------------------------  ---
172.21.18.18    ********
172.21.18.19    ********
```

Related Commands

Command	Description
control-plane-security	Configures the control plane security profile.
cluster-member-ip	Sets the controller as a control plane security cluster root, and specifies the IPsec key for a cluster member.
cluster-root-ip	Sets the controller as a control plane security cluster member, and defines the IPsec key for communication between the cluster member and the controller's cluster root.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on cluster member or cluster root controllers

show cluster-switches

```
show cluster-switches
```

Description

Execute this command on a Mobility Master using control plane security in a multi-master environment to show other managed devices to which it is connected.

Syntax

No parameters

Usage Guidelines

When you issue this command from the cluster root, the output of this command displays the IP address of the VLAN used by the cluster member to connect to the cluster root.

If you issue this command from a cluster member ,the output of this command displays the IP address of the VLAN used by the cluster root to connect to the cluster member.

Example

In the example below, the **show cluster-switches** command was issued on a cluster member. The **Switch-IP** section of the output shows the IP address of a VLAN on cluster root, indicating that the cluster member can currently communicate with the cluster root. If the managed device cannot communicate with the cluster root, this table will be blank.

```
(host) [mynode] (config) #show cluster-switches

SWITCH-IP         CLUSTER-ROLE
-----------------------------
172.21.18.18      ROOT
```

In this example, the **show cluster-switches** command was issued on a cluster root. The **Switch-IP** section of the output shows the IP address of a VLAN on each cluster member that can currently communicate with the cluster root.

```
(host) [mynode] (config) #show cluster-switches

SWITCH-IP         CLUSTER-ROLE
-----------------------------
172.21.18.18     MEMBER
172.21.18.19     MEMBER
```

Related Commands

Command	Description
control-plane-security	Configuress the control plane security profile.
cluster-member-ip	Sets the controller as a control plane security cluster root, and specifies the IPsec key for a cluster member.
cluster-root-ip	Sets the controller as a control plane security cluster member, and defines the IPsec key for communication between the cluster member and the controller's cluster root.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show cluster-tech-support

```
show cluster-tech-support <filename>
```

Description

Displays cluster-related information in relation to the managed device.

Syntax

Parameter	Description
`<filename>`	Specifies the file name where the command output will be stored. Maximum length of filename is 127 characters.

Example

The following command is used to store the logged cluster data:

```
show cluster-tech-support <filename>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable on the Mobility Master

show command-details

```
show command-details <COMMAND>
```

Description

This command displays the command debugging details for a command executed in the CLI session.

Syntax

Parameter	Description
<COMMAND>	Enter the command that is executed in the CLI session and for which you need the command details. The command text must be within quotation marks

Usage Guidelines

Use this command to display the command details for a command executed in the CLI session. The following example shows the output for this command.

```
(host) [mynode] #show command-details "show cellular profile"
Command Details:
----------------
APP Name: Layer2/3 , Object:5126 , OperationType: Async
Objname/Container: /CHK_PARENT, MajorVer: 8 , MinorVer: 1 , Instance: NULL
Local Command: 0 , Remote Command: 0 , Remote IpAddr: NULL
Current config Node: /mm/mynode
Command Key Values:
-------------------
Key       Value     Instance Key
---       -----     ------------
CELLULAR  CELLULAR  FALSE
PROFILE   PROFILE   FALSE
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show command-history

```
show command-history
```

Description

This command displays the command history for the CLI session.

Syntax

No parameter.

Usage Guidelines

Use this command to display a list of commands that you have executed in the CLI session. The following example shows the output for this command.

```
(host) [mynode] #show command-history
CLI session history
-------------------
show cellular profile
show cellular profile factory
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show configuration

```
show configuration [committed <node-path> | counters platform-capability | datastore
{[committed | default | detail | inherited | json | local | node-hierarchy | non-default |
object | pending | stats | system | user]} | devices | diff | effective | failure | filtered |
node-hierarchy | partial | pending | profile-committed | received | setup-dialog <macaddr>
| similar | state | system-commands | unsaved-nodes]
```

Description

This command shows the saved configuration on the controller.

Syntax

Parameter	Description
`committed [<node-path>]`	Shows committed configuration of the configuration node.
`counters platform-capability`	Shows internal counters at the node and platform capability-based information.
`datastore [committed | default | detail |inherited | json | local | node-hierarchy | non-default | object <objname> [detail | json | <node-path>] | pending | stats | system |user] [<node-path>]`	Shows datastore configuration.
`devices [debug | <node-path>]`	Shows devices list and nodes mapped to it.
`diff <conf1> <conf2> [context | json]`	Shows the difference between two configuration items. New commands are prefixed with a plus, deleted commands are prefixed with a minus.
`effective [detail | <node-path>]`	Shows effective configuration of devices connected to the node.
`failure [all | migration {[config-node | device]}| replace-config | <A.B.C.D>]`	Shows the configuration errors.
`filtered`	Show configuration downgraded to other versions.
`node-hierarchy [debug]`	Shows the configuration node hierarchy.
`partial [<node-path>]`	Shows incremental configuration changes between last two commits.
`pending [<node-path>]`	Shows pending configuration of the configuration node.
`profile-committed [<node-path>]`	Shows committed configuration of profiles at this node.

Parameter	Description
`received`	Shows the received configuration from Mobility Master.
`setup-dialog <macaddr>`	Shows the setup-dialog configuration of the device.
`similar <conf1> conf2> [json]`	Shows the common configuration between two configuration items.
`state pending [<node-path>]`	Shows the configuration state information.
`system-commands {committed | pending} [<node-path>]`	Shows system or hidden commands at the configuration node.
`unsaved-nodes`	Shows the list of unsaved configuration nodes.

Usage Guidelines

Execute this command to view the entire configuration saved on the controller, including all profiles, ACLs, and interface settings.

Example

The following example shows part of the output for this command.

```
(host) [mynode] #show configuration
version 8.0
country US
logging level warnings security subcat ids
logging level warnings security subcat ids-ap
wms
general poll-interval 60000
general poll-retries 3
general stat-update enable
general ap-ageout-interval 30
general sta-ageout-interval 30
general learn-ap disable
general persistent-known-interfering enable
!
adp discovery
adp igmp-join
adp igmp-vlan 0
.
.
.
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters were added: ■ **filtered** ■ **received** ■ **setup-dialog**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master

show controller-ip

```
show controller-ip
```

Description

Show the country and domain upgrade trail of the managed device.

Syntax

No parameters.

Example

The output of this command shows the IP address and VLAN interface ID of the managed device.

```
(host) # show controller-ip

Switch IP Address: 10.17.24.19
Switch IP is configured to be Vlan Interface: 1501
Switch IPv6 Address: 2001::1
Switch IPv6 address is configured to be Vlan Interface: 1501
```

Related Commands

Command	Description
controller-ip	Sets the IP address of the to the loopback interface address or a specific VLAN interface address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master

show controller-ipv6

```
show controller-ipv6
```

Description

Shows the IPv6 address and VLAN interface ID of the controller.

Syntax

No parameters.

Example

```
(host) [mynode] # show controller-ipv6
Switch IPv6 Address: 2001::1
Switch IPv6 address is configured to be Vlan Interface: 1501
```

The output of this command shows the IPv6 address and VLAN interface ID of the controller.

Related Commands

Command	Description
controller-ipv6	sets the default IPv6 address of the to the IPv6 loopback interface address or a specific VLAN interface address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show control-plane-security

```
show control-plane-security
```

Description

Show the current configuration of the control plane security profile.

Syntax

No parameters.

Usage Guidelines

The control plane security profile enables and disables the control plane security feature and identifies campus APs to receive security certificates. Issue this command to view current control plane security settings.

Example

The following command shows the control plane security and auto certificate provisioning features are enabled in the control plane security profile, and that the controller will send certificates to a range of IP addresses:

```
(host)(config) #show control-plane-security
Control Plane Security Profile
------------------------------
Parameter                        Value
---------                        -----
Control Plane Security           Enabled
Auto Cert Provisioning           Disabled
Auto Cert Allow All              Enabled
Expiry timer(dd:hh)              00:02
Auto Cert Allowed Addresses      N/A
Auto Cert Allowed IPv6 Addresses N/A
```

Related Commands

Command	Description
control-plane-security	Configure the control plane security profile by identifying APs to receive security certificates.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show country

```
show country [trail]
```

Description

Show the country and domain upgrade trail of the controller.

Syntax

Parameter	Description
`trail`	Display the record showing how the switch was reconfigured for its current country domain when the controller hardware was upgraded.

Usage Guidelines

A controller's country code sets the regulatory domain for the radio frequencies that the APs use. This value is typically set during the controller's initial setup procedure. Use this command to determine the country code specified during setup.

Example

The output of this command shows the controller's country, model and hardware types.

```
(host) # show country
Country:US
Model:Aruba7240-US
Hardware:Restricted US
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices

show cp-bwcontracts

```
show cp-bwcontract
```

Description

Displays a list of Control Processor (CP) bandwidth contracts for whitelist ACLs.

Syntax

No parameters.

Example

The *CP bw contracts* table lists the contract names, the ID number assigned to each contract, and its defined traffic rate in packets per second.

```
(host) #show cp-bwcontracts

CP bw contracts
---------------
Contract                  Id     Rate (packets/second)
--------                  --     ---------------------
cpbwc-ipv4                15785  2000
cpbwc-ipv6                15798  2000
cp-rate                   15809  20
```

Related Commands

Command	Description
firewall cp	This command creates a new whitelist ACL and can associate a bandwidth contract with that ACL.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on Mobility Master

show cp-stats

```
show cp-stats
```

Description

This command shows the control plane (CP) queue statistics.

Syntax

No parameters.

Example

Execute the following command to view the control plane queue statistics.

```
(host) [mynode] #show cp-stats
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show cpuload

```
show cpuload [current | per-cpu]
```

Description

The **show cpuload** command displays the controller CPU load for application and system processes. The CPU load stats for a controller can be viewed by using the **current** parameter, or displayed per-processor by using the **per-cpu** command.

Syntax

Parameter	Description
`current`	Include this optional parameter at the request of Aruba technical support to display additional CPU troubleshooting statistics.
`per-cpu`	Displays the CPU load stats for a controller by individual processor.

Example

This example shows that the majority of the controller's CPU resources are not being used by either application (user) or system processes.

```
(host)[mynode] #show cpuload
user 6.9%, system 7.7%, idle 85.4%
```

The output of this command includes the following parameters:

Parameter	Description
`user`	Percentage of controller CPU resources used by application processes.
`system`	Percentage of controller CPU resources used by system processes.
`idle`	Percentage of unused controller CPU resources.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show crashinfo

```
show crashinfo
```

Description

This command shows the list of crashes in the system.

Syntax

No parameter.

Usage Guidelines

You can use this command to know the list of crashes that has happened in the system.

Example

The following is an example for executing this command:

```
(host) [mynode] #show crashinfo
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show crypto-local ipsec-map

```
show crypto-local ipsec [tag <ipsec-map-name>]
```

Description

Displays the current IPsec map configuration on the controller.

Syntax

Parameter	Description
`tag <ipsec-map-name>`	Display a specific IPsec map.

Usage Guidelines

The command **show crypto-local ipsec** displays the current IPsec configuration on the controller.

Examples

The command **show crypto-local ipsec-map** shows the default map configuration along with any specific IPsec map configurations.

```
(host) #show crypto-local ipsec-map
Crypto Map Template "sample" 5
IKE Version: 2
IKEv2 Policy: 20
Security association lifetime seconds : 300
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-transform }
Peer gateway: gateway.example.com
Interface: VLAN 0
Source network: 10.4.215.10/255.255.255.255
Destination network: 10.3.75.15/255.255.255.255
Pre-Connect (Y/N): Y
Tunnel Trusted (Y/N): Y
Forced NAT-T (Y/N): N
Uplink Failover (Y/N):N
IP Compression (Y/N):N
```

Related Commands

Command	Description
crypto-local ipsec-map	Use this command to configure IPsec mapping for site-to-site VPN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto dp

```
show crypto dp [peer <source-ip>]
```

Descriptions

Displays crypto data packets.

Syntax

Parameter	Description
`dp`	Shows crypto latest datapath packets. The output is sent to crypto logs.
`peer <source-ip>`	Show crypto latest datapath packets for this peer—that is, shows crypto ISAKMP state for this IP.

Usage Guidelines

Use this command to send crypto data packet information to the controller log files, or to clear a crypto ISAKMP state associated with a specific IP address.

Examples

The command show crypto dp sends debug information to CRYTPO logs.

```
(host) [mynode] #show crypto dp
Datapath debug output sent to CRYPTO logs.
```

Related Commands

Command	Description
crypto isakmp	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto dynamic-map

```
show crypto dynamic-map [tag <dynamic-map-name>]
```

Descriptions

This command displays IPsec dynamic map configurations.

Syntax

Parameter	Description
`dynamic-map`	IPsec dynamic map configuration.
`tag <dynamic-map-name>`	A specific dynamic map.

Usage Guidelines

Dynamic maps enable IPsec SA negotiations from dynamically addressed IPsec peers. Once you have defined a dynamic map, you can associate that map with the default global map using the command crypto map global-map.

Examples

The command show crypto dynamic-map shows IPsec dynamic map configuration.

```
(host) [mynode] #show crypto dynamic-map
Crypto Map Template"default-dynamicmap" 10000
IKE Version: 1
IKEv1 Policy: All
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-transform, default-aes }
```

Related Commands

Command	Description
crypto dynamic-map	Use this command to configure a dynamic map.

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto ipsec

```
show crypto ipsec {ipsec-map-id | mtu | sa [peer v6 <peer-ipv6> | peer <peer-ip>] | transform-set [tag <transform-set-name>]}
```

Descriptions

Displays the current IPsec configuration on the managed device.

Syntax

Parameter	Description
`ipsec-map-id`	Shows IPsec MAP to ID mapping.
`mtu`	Shows IPSec max mtu.
`sa`	Shows security associations (SAs).
`peer ip6 <peer-ipv6>`	Shows IPsec SAs for an IPv6 peer.
`peer <peer-ip>`	Shows IPsec SAs for this IP.
`transform-set`	Shows IPsec transform sets.
`tag <transform-set-name>`	Shows a specific transform set.

Usage Guidelines

Execute the **show crypto ipsec** command to view the Maximum Transmission Unit (MTU) size allowed for network transmissions using IPsec security. It also displays the transform sets that define a specific encryption and authentication type.

Examples

The **show crypto ipsec transform-set** command displays the settings for both preconfigured and manually configured transform sets.

```
(host) [mynode] #show crypto ipsec transform-set
Transform set default-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-ml-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-boc-bm-transform: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-cluster-transform: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-1st-ikev2-transform: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-3rd-ikev2-transform: { esp-aes128 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-gcm256: { esp-aes256-gcm esp-null-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-gcm128: { esp-aes128-gcm esp-null-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-rap-transform: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set default-remote-node-bm-transform: { esp-3des esp-sha-hmac }
```

```
         will negotiate = { Transport, Tunnel }
Transform set default-aes: { esp-aes256 esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set newset: { esp-3des esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
Transform set name: { esp-aes256-gcm esp-sha-hmac }
         will negotiate = { Transport, Tunnel }
```

Use the **peer** parameter to view details about an IPsec connection.

```
(host) [mynode] #show crypto ipsec sa peer 80.254.65.210
Initiator IP: 80.254.65.210
Responder IP: 10.69.69.16
Initiator: No
Initiator cookie:018006409496dde5 Responder cookie:659f346abddccaf7
SA Creation Date: Fri Jun 25 13:21:23 2010
Life secs: 7200
Initiator Phase2 ID: 10.69.16.7/255.255.255.255
Responder Phase2 ID: 0.0.0.0/0.0.0.0
Phase2 Transform: EncAlg:esp-3des HMAC:esp-sha-hmac
Encapsulation Mode:UDP-encapsulated Tunnel
IP Compression Disabled
PFS: No
OUT SPI 1b0aa012, IN SPI 1b5c5300
Inner IP 10.69.16.7, internal type C
Aruba VIA
Reference count: 3
```

Execute the **show crypto ipsec sa** command to check the IPsec security associations.

```
(host) [mynode] #show crypto ipsec sa
IPSEC SA (V2) Active Session Information
------------------------------------
Initiator IP                  Responder IP        SPI(IN/OUT)        Flags Start Time        Inner IP
------------                  ------------        ----------------   ----- ---------------   --------
10.17.24.20                   10.17.24.19         44e59700/2b907e00  UT2   Mar  1 20:18:09     -
Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; 2 = IKEv2
Total IPSEC SAs: 1
```

Related Commands

Command	Description
crypto ipsec	Use this command to configure IPsec parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto isakmp

```
show crypto isakmp
   block-aruba-ca
   cluster IPAssignPendingRaps
   clusterIP
   clusterMAC
   eap-passthrough
   groupname
   ipsecSPI
   key
   lc-members
   log ap <macaddr>
   packet-dump
   policy <policy-number>
   sa
   stats
   timers
   transports
   udpencap-behind-natdevice
```

Descriptions

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`block-aruba-ca`	Shows the Configuration if Aruba-certified clients are blocked.
`cluster IPAssignPendingRaps`	Shows cluster configuration.
`clusterIP`	Show clusterIP hash table entries
`clusterMAC`	Show clusterMAC hash table entries
`eap-passthrough`	Displays configured IKEv2 EAP pass-through methods.
`groupname`	Shows the IKE Aggressive group name.
`ipsecSPI`	Shows IPsec SPI hash table entries.
`key`	Shows the IKE pre-shared keys.
`lc-members`	Shows cluster members.
`log ap <macaddr>`	Shows debugging log.
`packet-dump`	Shows the packet dump configuration.

Parameter	Description
`policy <policy-number>`	Shows the following information for predefined and manually configured IKE policies: ■ IKE version ■ encryption and hash algorithms ■ authentication method ■ PRF methods, ■ DH group ■ lifetime settings
`sa`	Shows the security associations.
`[peer v6 <peer-ipv6> | peer <peer-ip>]`	Shows crypto ISAKMP security associations for this IP.
`stats`	Shows detailed IKE statistics. This information can be very useful for troubleshooting problems with ISAKMP.
`timers`	Shows IKEv1 timers.
`transports`	Shows IKE Transports.
`udpencap-behind-natdevice`	Shows the Configuration if NAT-T is enabled if managed device is behind a NAT device .

Usage Guidelines

Use the show crypto isakmp command to view ISAKMP settings, statistics and policies.

Examples

The **show crypto isakmp stats** command shows the IKE statistics.

```
(host) [mynode] #show crypto isakmp stats
Default protection suite 10001
         Version 1
         encryption algorithm: 3DES - Triple Data Encryption Standard (168 bit keys)
         hash algorithm: Secure Hash Algorithm 160
         authentication method: Pre-Shared Key
         Diffie-Hellman Group: #2 (1024 bit)
         lifetime: [300 - 86400] seconds, no volume limit
Default RAP Certificate protection suite 10002
         Version 1
         encryption algorithm: AES - Advanced Encryption Standard (256 bit keys)
         hash algorithm: Secure Hash Algorithm 160
         authentication method: Rivest-Shamir-Adelman Signature
         Diffie-Hellman Group: #2 (1024 bit)
         lifetime: [300 - 86400] seconds, no volume limit
Default RAP PSK protection suite 10003
         Version 1
         encryption algorithm: AES - Advanced Encryption Standard (256 bit keys)
         hash algorithm: Secure Hash Algorithm 160
         authentication method: Pre-Shared Key
         Diffie-Hellman Group: #2 (1024 bit)
         lifetime: [300 - 86400] seconds, no volume limit
```

The **show crypto isakmp sa** command shows the IKE security associations.

```
(host) [mynode] #show crypto isakmp sa
ISAKMP SA Active Session Information
------------------------------------
Initiator IP        Responder IP       Flags       Start Time        Private IP
------------        ------------       -----     ---------------     ----------
```

```
10.17.65.116        10.17.65.120       r-v2-p    May 14 05:32:24       -
10.17.41.82         10.17.65.120       r-v2-p    May 14 07:12:14       -
10.17.40.226        10.17.65.120       r-v2-p    May 14 07:12:15       -
10.17.41.194        10.17.65.120       r-v2-p    May 14 07:12:13       -
Flags: i = Initiator; r = Responder
m = Main Mode; a = Agressive Mode; v2 = IKEv2
p = Pre-shared key; c = Certificate/RSA Signature; e =  ECDSA Signature
x = XAuth Enabled; y = Mode-Config Enabled; E = EAP Enabled
3 = 3rd party AP; C = Campus AP; R = RAP;  Ru = Custom Certificate RAP; I = IAP
V = VIA; S = VIA over TCP
Total ISAKMP SAs: 4
```

Related Commands

Command	Description
crypto isakmp	Use this command to configure Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto-local isakmp

```
show crypto-local isakmp
   allow-via-subnet-routes
   ca-certificate
   certificate-group
   disable-aggressive-mode
   disable-ipcomp
   dpd
   key [peer <peer-ip> | fqdn <ike-id-fqdn>]
   server-certificate
   xauth
```

Descriptions

This command displays Internet Key Exchange (IKE) parameters for the Internet Security Association and Key Management Protocol (ISAKMP).

Syntax

Parameter	Description
`allow-via-subnet-routes`	Shows if the Mobility Master is configured to accept subnet routes from VIA clients.
`ca-certificate`	Shows all the Certificate Authority (CA) certificates associated with VPN clients.
`certificate-group`	Shows the existing certificate groups by server certificate name and CA certificate.
`disable-aggressive-mode`	Shows if aggressive-mode is enabled or disabled.
`disable-ipcomp`	Shows IP compression configuration.
`dpd`	Shows the IKE Dead Peer Detection (DPD) configuration on the managed device.
`key [fqdn <ike-id-fqdn> | peer <peer-ip>]`	Shows the IKE pre-shared key on the managed device for site-to-site VPN. This includes keys configured by Fully Qualified Domain Name (FQDN) and local and global keys configured by IP address.
`server-certificate`	Shows all the IKE server certificates used to authenticate the managed device for VPN clients.
`xauth`	Shows the IKE XAuth configuration for VPN clients.

Usage Guidelines

Use the **show crypto-local isakmp** command to view IKE parameters.

Examples

The examples here show sample output for the **show crypto-local isakmp ca-certificate**, **show crypto-local isakmp certificate-group**, **show crypto-local isakmp dpd**, **show crypto-local isakmp key**, **show crypto-local isakmp server-certificate**and **show crypto-local isakmp xauth** commands:

```
(host) [mynode] #show crypto-local isakmp ca-certificate
ISAKMP CA Certificates
----------------------
CA certificate name  Client-VPN  # of Site-Site-Maps
-------------------  ----------  -------------------
Aruba-Factory-CA     Y           0


(host )[mynode] #show crypto-local isakmp certificate-group

ISAKMP Certificate Groups
-------------------------
Server certificate name  CA certificate name
-----------------------  -------------------


(host) [mynode] #show crypto-local isakmp dpd
DPD is Enabled: Idle-timeout = 22 seconds, Retry-timeout = 2 seconds, Retry-attempts = 3


(host) [mynode] #show crypto-local isa
ISAKMP Local Pre-Shared keys configured for ANY FQDN
----------------------------------------------------
Key
---
ISAKMP Local Pre-Shared keys configured by FQDN
-----------------------------------------------
FQDN of the host    Key
----------------    ---
servers.mycorp.com  ********

ISAKMP Local Pre-Shared keys configured by Address
--------------------------------------------------
IP address of the host  Subnet Mask Length  Key
----------------------  ------------------  ---
10.4.62.10              32                  ********

ISAKMP Global Pre-Shared keys configured by Address
---------------------------------------------------
IP address of the host  Subnet Mask Length  Key
----------------------  ------------------  ---
0.0.0.0                 0                   ********


(host) [mynode] #show crypto-local isakmp server-certificate
ISAKMP Server Certificates
--------------------------
Server certificate name          Client-VPN  # of Site-Site-Maps
-----------------------          ----------  -------------------
Aruba-Factory-Server-Cert-Chain  RAP-only    0


(host) [mynode] #show crypto-local isakmp xauth
IKE XAuth Enabled.
```

Related Commands

Command	Description
crypto-local isakmp allow-via-subnet-routes	Use this command to push subnet routes to the Mobility Masterand managed device.
crypto-local isakmp ca-certificate	Use this command to assign the Certificate Authority (CA) certificate used to authenticate VPN clients.
crypto-local isakmp certificate-group	Use this command to assign a certificate group so you can access multiple types of certificates on the same managed device.
crypto-local isakmp disable-aggressive-mode	Use this command to disable the IKEv1 aggressive mode.
crypto-local isakmp dpd	Use this command to configure IKE Dead Peer Detection (DPD) on the managed device.
crypto-local isakmp key	Use this command to configure the IKE preshared key on the managed device for site-to-site VPN.
crypto-local isakmp server-certificate	Use this command to assign the server certificate used to authenticate the managed device for VPN clients.
crypto-local isakmp xauth	Use this command to enable the IKE XAuth for VPN clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The **allow-via-subnet-routes** subcommand was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show crypto-local pki

```
show crypto-local pki
   CRL
      [<name> [ALL | crlnumber | fingerprint | hash| issuer | lastupdate | nextupdate]]
   crl-stats
   IntermediateCA
      [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose | serial |
      subject]]
   ocsp-client-stats
   OCSPResponderCert
      [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose | serial |
      subject]]
   OCSPSignerCert
      [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose | serial |
      subject]]
   PublicCert
      [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose | serial |
      subject]]
   rcp [<name>]
   ServerCert
      [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose | serial |
      subject]]
   TrustedCA
      [<name> [alias | ALL | dates | fingerprint | hash | issuer | modulus | purpose | serial |
      subject]]
   service-ocsp-responder [stats]
```

Descriptions

Execute this command to show local certificate, OCSP signer or responder certificate, and CRL data and statistics.

Syntax

Parameter	Description
`CRL`	Shows the name, original filename, reference count and expiration status of all CRLs on this controller.
`<name> ALL`	Shows the version, signature algorithm, issuer, last update, next update, and CRL extensions and all other attributes of this CRL.
`<name> crlnumber`	Shows the number of this CRL.
`<name> fingerprint`	Shows the fingerprint of this CRL.
`<name> hash`	Shows the hash number of this CRL.
`<name> issuer`	Shows the issuer of this CRL.
`<name> lastupdate`	Shows the last update (date and time) at which the returned status is known to be correct.

Parameter	Description
<name> nextupdate	Shows the next date and time (date and time) where the responder retrieves updated status information for this certificate. If this information is not present, then the responder always holds up to date status information.
crl-stats	Shows the CRL request statistics.
IntermediateCA	Shows the name, original filename, reference count and expiration status of this certificate. **NOTE:** IntermediateCA has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
ocsp-client-stats	Shows the OCSP client statistics.
OSCPResponderCert	Shows the name, original filename, reference count and expiration status of all OCSPResponderCert certificates on this controller. **NOTE:** OCSPResponderCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
OCSPSignerCert	Shows the OCSP Signer certificate. **NOTE:** OCSPSignerCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
PublicCert	Shows Public key information of a certificate. This certificate allows an application to identify an exact certificate. **NOTE:** PublicCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
rcp	Shows the revocation check point.
ServerCert	Shows Server certificate information. This certificate must contain both a public and a private key (the public and private keys must match). You can import a server certificate in either PKCS12 or X.509 PEM format; the certificate is stored in X.509 PEM DES encrypted format on the controller. **NOTE:** ServerCert has the identical sub-parameters as those listed under the TrustedCA parameter in this table.
TrustedCA	Shows trusted CA certificate information. This certificate can be either a root CA or intermediate CA. Aruba encourages (but does not require) the signing CA of the an intermediate CA to be the controller itself.
<name> ALL	Shows the version, signature algorithm, issuer, last update, next update, and CRL extensions and all other attributes of this certificate.
<name> alias	Shows this certificate's alias, if it exists.
<name> dates	Shows the dates for which this certificate is valid.
<name> fingerprint	Shows the certificate's fingerprint.
<name> hash	Shows the hash number of this certificate.
<name> issuer	Shows the certificate issuer.
<name> modulus	Shows the modulus which is part of the public key of the certificate.

Parameter	Description
<name> purpose	Shows the certificate's purposes such as if this is an SSL server, SSL server CA and so on.
<name> serial	Shows the certificate's serial number.
<name> subject	Shows the certificate's subject identification number.
service-ocsp-responder [stats]	Shows if OCSP responder service is enabled and shows statistics.

Usage Guidelines

Use the **show crypto-local pki** command to view all CRL and certificate status, OCSP client and OCSP responder status and statistics.

Example

This example displays a list of all OCSP responder certificates on this controller.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert

Certificates
------------
Name                         Original Filename          Reference Count  Expired
--------------               -----------------          ---------------  -------
ocspJan28                    ocspresp-jan28.cer         0                No
ocspresp-standalone-feb21    ocspresp-feb21.cer         0                No
ocspRespFeb02                ocspresp-feb2.cer          1                No
OCSPresponder1               ocspresponder-new1.cer     0                No
ocspresponder2               subsubCA-ocsp-res-2.cer    0                No
OCSPresponderlatest          ocspresponder-latest.cer   0                No
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the OCSP responder certificate.
Original Filename	Name of the original certificate when it was added to the controller.
Reference Count	Number of RCPs that reference this OCSP responder certificate, signer certificate or CRL.
Expired	Shows whether the controller has enabled or disabled client remediation with Sygate-on-demand-agent.

This example shows the dates for which this OCSP responder certificate is valid.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocspJan28 dates
notBefore=Jan 21 02:37:47 2011 GMT
notAfter=Jan 20 02:37:47 2013 GMT
```

This example displays the certificate's hash number.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocspJan28 hash 91dcb1b3
```

This example shows the purpose and information about this certificate.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocspJan28 purpose
Certificate purposes:For validation
SSL client : No
```

```
SSL client CA : No
SSL server : No
SSL server CA : No
Netscape SSL server : No
Netscape SSL server CA : No
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
```

This example displays the certificate's subject.

```
(host) [mynode] #show crypto-local pki OCSPResponderCert ocspJan28 subject

subject= /CN=WIN-T1BQQFMVDED.security1.qa.mycorp.com
```

Related Commands

Command	Description
crypto-local pki	This command is saved in the configuration file and verifies the presence of the certificate in the controller's internal directory structure.
crypto-local pki rcp <name>	Specifies the certificates that are used to sign OCSP responses for this revocation check point

Command History

Command	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto map

```
show crypto map
```

Descriptions

This command displays the IPsec map configurations.

Syntax

Parameter	Description
`map`	Shows the IPsec map configurations.

Usage Guidelines

Use the **show crypto map** command to view configuration for global, dynamic, and default map configurations.

Examples

The output of the **show crypto map** command shows statistics for the global, dynamic, and default maps.

```
(host) [mynode] #show crypto map
Crypto Map "GLOBAL-IKEV2-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-rap-ipsecmap" 10001
IKE Version: 2
IKEv2 Policy: DEFAULT
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-gcm256, default-gcm128, default-rap-transform }
Crypto Map "GLOBAL-MAP" 10000 ipsec-isakmp
Crypto Map Template"default-dynamicmap" 10000
IKE Version: 1
IKEv1 Policy: All
Security association lifetime seconds : [300 -86400]
Security association lifetime kilobytes: N/A
PFS (Y/N): N
Transform sets={ default-transform, default-aes }
```

Related Commands

Command	Description
crypto map global-map	Use this command to configure the default global map.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show crypto pki

```
show crypto pki csr
```

Descriptions

This command displays the certificate signing request (CSR) for the captive portal feature.

Syntax

Parameter	Description
`csr`	Shows the certificate signing request for the captive portal feature.

Usage Guidelines

Use the **show crypto pki** command to view the CSR output.

Examples

The output of the **crypto pki csr** command.

```
(host) [mynode] #show crypto pki csr

Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CA, L=Sunnyvale, O=sales, OU=EMEA,
CN=www.mycompany.com/emailAddress=myname@mycompany.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e6:b0:f2:95:37:d0:18:c4:ee:f7:bd:5d:96:85:
                    49:a3:56:63:76:ee:99:82:fe:4b:31:6c:80:25:c4:
                    ed:c7:9e:8e:5e:3e:a2:1f:90:62:b7:91:69:75:27:
                    e8:29:ba:d1:76:3c:0b:14:dd:83:3a:0c:62:f2:2f:
                    49:90:47:f5:2f:e6:4e:dc:c3:06:7e:d2:51:29:ec:
                    52:8c:40:26:de:ae:c6:a0:21:1b:ee:46:b1:7a:9b:
                    dd:0b:67:44:48:66:19:ec:c7:f4:24:bd:28:98:a2:
                    c7:6b:fb:b6:8e:43:aa:c7:22:3a:b8:ec:9a:0a:50:
                    c0:29:b7:84:46:70:a5:3f:09
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        25:ce:0f:29:91:73:e9:cd:28:85:ea:74:7c:44:ba:b7:d0:5d:
        2d:53:64:dc:ad:07:fd:ed:09:af:b7:4a:7f:14:9a:5f:c3:0a:
        8a:f8:ff:40:25:9c:f4:97:73:5b:53:cd:0e:9c:d2:63:b8:55:
        a5:bd:20:74:58:f8:70:be:b9:82:4a:d0:1e:fc:8d:71:a0:33:
        bb:9b:f9:a1:ee:d9:e8:62:e4:34:e4:f7:8b:7f:6d:3c:70:4c:
        4c:18:e0:7f:fe:8b:f2:01:a2:0f:00:49:81:f7:de:42:b9:05:
        59:7c:e4:89:ed:8f:e1:3b:50:5a:7e:91:3b:9c:09:8f:b7:6b:
        98:80
-----BEGIN CERTIFICATE REQUEST-----
MIIB1DCCAT0CAQAwgZMxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTESMBAGA1UE
BxMJU3Vubnl2YWxlMQ4wDAYDVQQKEwVzYWxlczENMAsGA1UECxMERU1FQTEaMBgG
A1UEAxMRd3d3Lm15Y29tcGFueS5jb20xKDAmBgkqhkiG9w0BCQEWGXB3cmVkZHlA
```

```
YXJ1YmFuZXR3b3Jrcy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOaw
8pU30BjE7ve9XZaFSaNWY3bumYL+SzFsgCXE7ceejl4+oh+QYreRaXUn6Cm60XY8
CxTdgzoMYvIvSZBH9S/mTtzDBn7SUSnsUoxAJt6uxqAhG+5GsXqb3QtnREhmGezH
9CS9KJiix2v7to5DqsciOrjsmgpQwCm3hEZwpT8JAgMBAAGgADANBgkqhkiG9w0B
AQUFAAOBgQAlzg8pkXPpzSiF6nR8RLq30F0tU2TcrQf97Qmvt0p/FJpfwwqK+P9A
JZz0l3NbU80OnNJjuFWlvSB0WPhwvrmCStAe/I1xoDO7m/mh7tnoYuQ05PeLf208
cExMGOB//ovyAaIPAEmB995CuQVZfOSJ7Y/hO1BafpE7nAmPt2uYgA==
```

-----END CERTIFICATE REQUEST-----

Related Commands

Command	Description
crypto pki	Use this command to generate a certificate signing request (CSR) for the captive portal feature.
crypto pki-import	Use this command to import certificates for the captive portal feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show database

```
show database synchronize
```

Description

This command displays database synchronization status.

Syntax

Parameter	Description
`synchronize`	Shows Multiple Master Switches redundancy status (Master-Master communication).

Example

This example shows a database synchronization status.

```
(host) [mynode] #show database synchronize

Last synchronization time: Not synchronized since last reboot

Periodic synchronization is enabled and runs every 25 minutes
```

Related Commands

Command	Description
database synchronize	This command configures the Mobility Master to synchronizes the database with a standby or backup Mobility Master. This works in config mode.
database-synchronize	This command synchronizes the Mobility Master database with a standby or backup Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show datapath

```
show datapath
   acl
      ap-name <ap-name> name <acl-name> type <acl-type>
      id <id> [verbose]
      ip-addr <ip-addr> name <acl-name> type <acl-type>
   amsdu tx
   application
      [<id> | all | ap-name <ap-name>  | counters | ip-addr <ip-addr>  | verbose]
   bridge
      [ap-name <ap-name>  | counters | ip-addr <ip-addr>  | table <macaddr> | verbose]
   bwm
      [ap-name <ap-name>  | ip-addr <ip-addr>  | table | type <type-id> {[contract <contract-
      id>]}
   compression
      [<id> | all | counters | verbose]
   cp-bwm
      [table]
   crypto
      [<id> | all | counters | verbose]
   debug
      dma [counters]
      eap [counters]
      eth1info
      memory
      memory-usage
      opcode
      performance [<id> | all | counters | event-guide |verbose]
      pkttrace-buffer [log {<number> | all}]
      table-limits
      tnl-stats
      trace-buffer [lines <lines>]
      trace-route
   dhcp vm-mac
   dns-cache
      [counters]
   dpdk
      mempool-stats
      ring-stats
   dpi
      app-category <appcatid>
      application <appid>
   energy-efficiency
   error counters
   esi
      [table]
   exthdr
   firewall-agg-sess
      [counters]
   fqdn
   frame
      [<id> | all | ap-name <ap-name>  | counters | ip-addr <ip-addr>  | slot | verbose]
   hardware
      counters
      statistics
   heartbeat stats
   internal
      [dir <dir-name> file <file-name>]
   ip-fragment-table
      [ipv4 | ipv6]
```

```
ip-geolocation
   [counters]
ip-mcast
   [client <client-mac> | destination | group | station]
ip-reassembly
   [counters | ipv4 | ipv6]
ip-reputation
   [counters | rtc]
ipfix statistics
ipsec-map
ipv6-mcast
   destination
   group
   station
l3-interface
lag table
maintenance
   [counters]
message-queue
   [counters]
mobility
   discovery-table
   home-agent-table
   mcast-table
   stats
nat
   [ap-name <ap-name> | ip-addr <ip-addr>  | table]
netdest-id
   ap-name <ap-name>
   ip-addr <ip-addr>
   <id>
network
   egress
   ingress
nexthop-list
openflow
   acl
   acl-action-table
   auxiliary
   session [<A.B.C.D>]
   statistics
papi [counters | remote-device-table {counters | ipv6}]
port
   [ap-name <ap-name> [table] | ip-addr <ip-addr> [table] | untrusted-vlan <slot/-
   module/port> | vlan-table <slot/module/port>]
rap-bw-resv
   ap-name <ap-name> [advanced]
   ip-addr <ip-addr> [advanced]
rap-pkt-trace
   ap-name <ap-name>
   ip-addr <ip-addr>
rap-stats
   ap-name <ap-name>
   ip-addr <ip-addr>
route
   [ap-name <ap-name>  | counters | ip-addr <ip-addr>  | ipv4 | ipv6 | table | verbose]
route-cache
   [ap-name <ap-name>  | counters | ip-addr <ip-addr> | ipv4 | ipv6 | table | verbose]
scheduler
   interface <slot/module/port>
   table
services
session
```

```
   [ap-name <ap-name>  |
   counters |
   dpi [counters [all | top | uplink-vlan <uplinkvlan>] | table [<A.B.C.D> | appid <app-
   id>]] |
   high-value [user <macaddr>] |
   ip-addr <ip-addr>  |
   ip-classification  |
   ipv6 [counters | dpi [counters [top]] | high-value | {table [<X:X:X:X::X> | appid <app-
   id>]} | verbose]
   session-id <sid> [dpi]
   table [<A.B.C.D>]
   verbose
   web-cc]
station
   [<id> | all | counters | crypto-counters | mac <macaddr> | standby | table | verbose]
tcp
   [app <app>  | counters | tunnel table]
tunnel
   [counters | encaps | heartbeat | ipv4 | ipv6  | station-list | table | tunnel-id <tid> |
   verbose]
tunnel-group
user
   [<id> | all | ap-name <ap-name>  | counters | ip-addr <ip-addr> | ipv4 | ipv6 | rad-coun-
   ters | standby | table | verbose}
utilization
vlan
   [ap-name <ap-name>   | ip-addr <ip-addr>  | pvst | table]
vlan-mcast
   [ap-name <ap-name>    | ip-addr <ip-addr>  | table]
wan-hc
   [<id> | all | counters | verbose]
web-cc
   [counters]
wifi-reassembly
   [<id> | all | counters | verbose]
wmm
   [counters]
```

Descriptions

Displays system statistics for the managed device.

Syntax

Parameter	Description
`acl`	Displays datapath ACL entries.
`ap-name <ap-name>`	Specify the name of the AP.
`id <id-name> [verbose]`	Displays datapath statistics associated with a specified ACL. The ACL index is found in the **show rights** command. The allowed range is 1–2703.
`ip-addr <ip-addr>`	Specify the IP address of the AP.
`name <acl-name>`	Specify the name of ACL.

Parameter	Description
type <acl-type>	Specify the ACL Type. 0 - session-based; 1- role-based
amsdu tx	Shows datapath AMSDU TX queue statistics
application	Shows datapath application statistics. By default, it provides combined statistics of all CPUs.
<id>	Shows datapath application statistics by specified CPU id. Valid platform CPU range may vary.
all	Shows datapath application statistics for all CPUs, one by one.
ap-name <ap-name>	Specify the name of the AP.
counters	Shows application counters and errors generated by applications running on a particular AP. These include stateful firewall application layer statistics.
ip-addr <ip-addr>	Specify the IP address of the AP.
verbose	Shows datapath application statistics in detail.
bridge	Shows bridge table entry statistics including MAC address, VLAN, assigned VLAN, Destination, and flag information for an AP.
ap-name <ap-name>	Specify the name of the AP. Shows MAC address, VLAN, assigned VLANs, destination and flags information.
counters	Shows datapath bridge table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures, and max link length.
devices	Shows datapath bridge devices.
ip-addr <ip-addr>	Specify the IP address of the AP. Shows MAC address, VLAN, assigned VLANs, destination and flags information.
table <macaddr>	Displays the current high, maximum, and total number of bridge table entries for the Aruba controller.
verbose	Displays datapath bridge details in a tabular format.

Parameter	Description
bwm	Displays the following bandwidth management table entry statistics: ■ **Type:** Indicates whether the contract is a control plane DoS contract (0), a contract configured through the bandwidth management WebUI or CLI Interfaces (1), or a contract for multicast traffic generated by the controller(2). ■ **Cont ID:** An ID number unique to each contract. ■ **Rate:** Contract traffic rate, in 256-byte packets per second. ■ **Policed:** The number of packets dropped because the policy was applied. ■ **Avail Credits:** This value is the (contract rate) per 32, and is used for internal debugging purposes. ■ **Queued Pkts/ Bytes:** Number of bytes or packets currently being queued. ■ **Flags:** Flags applied to the contract. ■ **CPU:** A value in this column indicates that the traffic passed through the slowpath CPU, and is used for internal debugging purposes. ■ **Status:** Indicates if the bandwidth contract is successfully applied.
ap-name <ap-name>	View a bandwidth contract for a specific AP.
ip-addr <ip-addr>	View a bandwidth contract for an AP with the specified IP address.
table	Displays a table of all configured bandwidth contracts.
type <type-id>	Displays only bandwidth contracts of a specific type (0,1 or 2).
contract <contract-id>	Displays the bandwidth contracts for the specified contract id.
compression	Displays datapath compression statistics. By default, the combined statistics of all CPUs are shown.
<id>	Shows datapath compression statistics by specified CPU id. Valid platform CPU range may vary.
all	Shows datapath compression statistics for all CPUs, one by one.
counters	Shows datapath compression counters or statistics.
verbose	Shows datapath compression statistics in detail.
cp-bwm	Displays the data path CP bandwidth management table information.
table	Displays the datapath CP bandwidth management table entries.
crypto	Displays crypto parameter statistics including crypto, IPsec, PPTP, WEP, TKIP, AESCCM encryption and decryptions, WEP CRC, crypto hardware, XSEC, 802.1X, and L2TP information.

Parameter	Description
<id>	Shows datapath crypto statistics by specified CPU id. Valid platform CPU range may vary.
all	Shows datapath crypto statistics for all CPUs, one by one.
counters	Shows datapath crypto counters or statistics.
verbose	Shows datapath crypto statistics in detail.
debug	Displays datapath debug details. These are low-level datapath details.
dma [counters]	DMA statistics are displayed.
eap [counters]	EAP termination statistics are displayed.
eth1info	Displays IPv4 fragment table statistics.
memory	Displays SOS memory statistics.
memory-usage	Displays datapath memory used.
opcode	Displays datapath debugging information. **NOTE:** Use this command only under the supervision of Aruba technical support.
performance	Displays datapath debug performance statistics including the SUM or CPU, addr, and description.
<id>	Displays datapath performance counters by specified CPU ID.
all	Displays datapath debug performance for all CPUs.
counters	Displays datapath performance counters.
event-guide	Displays the following events: ■ COP0 ■ L3 Cache ■ NAE-RX ■ NAE-TX events (by register index 0-4)
verbose	Displays debug performance statistics including: SUM or CPU, address, description, value, and difference from last show.
pkttrace-buffer [log {<number> | all}]	Shows the datapath packet trace buffer from log file, either as number of lines from the end or as complete packet trace log.
table-limits	Displays the datapath table upper limits.
tnl-stats [<id> | all | counters | verbose]	Displays the Wi-Fi Tunnel Stats Exported to CP debug.

Parameter	Description
`trace-buffer [lines <lines>]`	Shows the datapath trace buffer, by number of lines from the end of log.
`trace-route`	Shows datapath route or cache tracing.
`dhcp vm-mac`	Shows datapath DHCP-related information; datapath VM to host client MAC mapping
`dns-cache [counters]`	Displays DNS cache statistics.

`dpdk`
`mempool-stats`
`ring-stats`
	Data Plane Development Kit.
	■ mempool-stats—Shows datapath DPDK memory pool statistics.
	■ ring-stats—Shows datapath DPDK ring statistics.

`dpi`
`app-category <appcatid>`
`application <appid>`
	Displays the DPI application default ports. Specify the application Group ID or the application ID.

`energy-efficiency`	Displays the energy efficiency statistics.
`error`	Displays datapath error statistics or counters.
`counters`	Show datapath errors including SUM, CPU, Address, and description information. The output counters include, but not limited to, the following: ■ BPDUs Received ■ VOQ retries ■ Invalid IP headers Received ■ IKE Throttle ■ VOQ retries ■ Ipv4 Firewall Denied Frames ■ Ipv6 Firewall Denied Frames ■ IP Reassembly Failures ■ Invalid IP headers Received ■ Dot1Q Discards ■ Dot1d Discards ■ Drop cache frames ■ AESCCM Encryption Station Not Ready ■ AESCCM Decryption Failures ■ AESCCM Decryption Invalid Replay Co
`esi [table]`	Displays the contents of the datapath ESI server table entries including server, IP, MAC, destination, VLAN, type, session and flag information.
`exthdr`	Displays the datapath default IPv6 Extended Header Map.
`firewall-agg-sess`	Displays the datapath firewall aggregated sessions table.
`counters`	Displays the datapath aggregate session statistics.
`fqdn`	Displays datapath FQDN entries.

Parameter	Description
`frame`	Displays frame statistics that are received and transmitted from the data path of the controller. Several output fields include the following descriptions: ■ **Descr failures:** This is the number of times a packet descriptor was not available and the packet dropped. ■ **Dot1QDiscards:** The number of packets received on a trunk port where the VLAN presented did not match any configured on the controller and the packet dropped. ■ **Dot1d Discards:** Spanning tree is disabled and each BPDU frame is counted and dropped. ■ **Denied Frames:** Frames that are denied by the data path of the ACL for thecontroller. See the **Example** section for a complete list of output.
`<id>`	Displays datapath frame statistics by specified CPU ID. Valid platform CPU range may vary.
`all`	Displays datapath frame statistics for all cpus, one by one.
`ap-name <ap-name> [counters]`	Name of the AP. The *counters* parameter is optional.
`counters`	Displays datapath frame statistics
`ip-addr <ip-addr> [counters]`	IP address of the AP. The *counters* parameter is optional.
`slot`	Displays datapath combined frame statistics of all CPUs, including slot specific section.
`verbose`	Displays datapath frame statistics in detail.
`hardware`	Displays datapath hardware counters or hardware packet statistics information.
`counters`	Displays hardware counters.
`statistics`	Displays Hardware packet statistics.
`heartbeat stats`	Displays Sibyte heartbeat packet stats.
`internal`	Displays Internal details .
`dir <dir-name>`	Specify the hardware directory.
`file <file-name>`	Specify the file in the directory.
`ip-fragment-table`	Displays ip-fragment statistics including CPU, current entries, high water mark, max , total, and aged entries.
`ipv4`	Displays IPv4 fragment statistics.
`ipv6`	Displays IPv6 fragment statistics.
`ip-geolocation`	Datapath IP geolocation table entries.
`counters`	Displays IP geolocation statistics.

Parameter	Description
ip-mcast	Displays the Datapath IP Multicast Entries table statistics.
client <client-mac>	Datapath Layer 3 groups for specified client.
destination	Datapath tunnel and port membership.
group	Datapath Layer 3 groups.
station	Datapath station membership.
ip-reassembly	Displays the contents of the IP Reassembly statistics tables.
counters	IP reassembly counters.
ipv4	Displays the IPv4 contents of the IP Reassembly statistics table.
ipv6	Displays the IPv6 contents of the IP Reassembly statistics table.
ip-reputation	Datapath IP reputation table entries.
counters	Displays IP reputation statistics.
rtc	Displays IP reputation real time cache.
ipfix statistics	Displays datapath IPFIX collection statistics.
ipsec-map	Displays datapath IPsec map details.
ipv6-mcast	Displays the datapath IP multicast table statistics.
destination	Displays the IPv6 tunnel and port membership.
group	Displays the IPv6 multicast group.
station	Displays the IPv6 station membership.
l3-interface	Displays datapath Layer 3 interface table.
lag table	Displays contents of the datapath LAG or port channel table.
maintenance [counters]	Displays datapath maintenance statistics.
message-queue [counters]	Displays statistics of messages received by a CPU from other datapath CPUs (only CPUs that receive messages and non-zero statistics are shown). The datapath SOS message queue statistics by CPU IDs and Opcode is displayed.
mobility	Displays datapath IP mobility information.
discovery-table	Displays the discovery count table that is used to keep track of per client home agent discovery.

Parameter	Description
`home-agent-table`	Displays the datapath HA table information.
`mcast-table`	Displays the mobility multicast-group table that is used to flood the multicast RA traffic to the roamed clients.
`stats`	Displays the statistics of the datapath mobility.
`nat`	Displays the contents of the datapath NAT entries table. It displays NAT pools as configured in the datapath. Statistics include pool, SITP start, SIP end and DIP.
`ap-name <ap-name> [table]`	Specify the name of AP.
`ip-addr <ip-addr> [table]`	Specify the IP address of the AP.
`table`	Shows the datapath NAT table entries.

`netdest-id`
`ap-name <ap-name>`
`ip-addr <ip-addr>`
`<id>`
	Shows the datapath ACL netdestination table.
	for AP name, IP address of AP, or ID.

`network {egress | ingress}`	Displays egress or ingress queue counters. The network engress output includes, but not limited to, the following fields: ■ CPU ■ DP High Prio ■ Network High Prio The network ingress output includes, but not limited to, the following fields: ■ LIFO Queue ■ Packets Received ■ Threshold count ■ Empty Count ■ Threshold Recovery ■ Empty Recovery
`nexthop-list`	Displays the following types of information about the datapath for packets routed to next-hop devices. ■ SOS Dest : Unique datapath identifier for each next-hop list ■ Active IP: ■ NhIdx: Unique identifier for each next-hop list ■ NhVer: Internally generated number used to synchronize the next-hop and session tables.
`openflow`	Displays the datapath OpenFlow information.
`acl`	Displays the datapath OpenFlow ACL table and actions.
`acl-action-table`	Displays the OpenFlow ACL action table.
`auxiliary`	Displays the datapath OpenFlow auxiliary channel information.
`session [<A.B.C.D>]`	Displays the datapath OpenFlow session table and actions. You can optionally filter the sessions based on the IP address.

Parameter	Description
`statistics`	Displays the OpenFlow statistics in datapath.
`papi`	Displays the datapath PAPI statistics.
`counters`	Displays datapath PAPI counters including: SUM or CPU, addr, description, and value.
`remote-device-table [ipv6]`	Displays the remote device table maintained in the datapath that contains PAPI entries for IPv6 devices.
`port`	Displays the datapath port table information. This includes the port number, PVID, Ingress ACL, Egress ACL, Session ACL, and the following flags: ■ B: Blocked by the Spanning Tree protocol ■ L: LSG ■ M: Tunneled node ■ Q: Trunk ■ T: Trusted ■ X: xSec ■ Z: QinQ
`ap-name <ap-name> [table]`	Specify the name of the AP. Shows the datapath port table entries for the specified AP.
`ip-addr <ip-addr> [table]`	Specify the IP address of the AP. Shows the datapath port table entries for the specified IP.
`untrusted-vlan <slot>/<module>/<port>`	Shows if there are untrusted vlan entries for the indicated slot, module, and port.
`vlan-table <slot>/<module>/<port>`	Shows datapath port-vlan table session entries for the specified slot, module, and port.

`rap-bw-resv`
`ap-name <ap-name> [advanced]`
`ip-addr <ip-addr> [advanced]`
	Displays the remote AP uplink BW reservation statistics of the Remote AP only. Specify the AP or IP address with the *advanced* parameter for Advanced Debugging Options.

`rap-pkt-trace`
`ap-name <ap-name>`
`ip-addr <ip-addr>`
	Specify the name of the Remote AP. Displays the remote AP packet-trace statistics of only the specified Remote AP.

`rap-stats`
`ap-name <ap-name>`
`ip-addr <ip-addr>`
	Specify the name of the Remote AP. Displays the remote AP statistics of only the specified Remote AP.

Parameter	Description
`route`	Displays datapath route table statistics. The output of the command includes the following fields: **Route table entries** ■ IP ■ Mask ■ Gateway ■ Cost ■ VLAN ■ Flags **IPv6 Route table entries** ■ Prefix ■ Gateway ■ Cost ■ VLAN ■ Flags
`ap-name <ap-name> [counters | table | verbose]`	Specify the name of the AP.
`counters`	Displays route table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
`ip-addr <ip-addr> [counters | table | verbose]`	Specify the IP address of the AP.
`ipv4`	Displays datapath IPv4 routing table.
`ipv6`	Displays datapath IPv6 routing table.
`table`	Displays route table entries such as IP, mask, gateway, cost, VLAN and flags.
`verbose`	Displays all detailed route table entries including IP, mask, gateway, cost, VLAN, flags, Internal VerNum Index.
`route-cache`	Displays datapath route cache table statistics.
`ap-name <ap-name> [counters | table | verbose]`	Specify the name of the AP.
`counters`	Displays route cache table statistics such as current entries, high water mark, maximum entries, total entries, allocation failures and max link length.
`ip-addr <ip-addr> [counters | table | verbose]`	Specify the IP address.
`ipv4`	Displays datapath IPv4 route cache.
`ipv6`	Displays datapath IPv6 route cache.
`table`	Displays route cache table entries such as IP, mask, gateway, cost, VLAN and flags.
`verbose`	Displays all detailed route cache table entries including IP, mask, gateway, cost, VLAN, flags, Internal VerNum Index.

Parameter	Description

`scheduler`
`interface <slot/module/port>`
`table`
	Displays the datapath scheduler table. Specify interface for scheduler output in the slot or module or port format.

`services`	Displays the datapath services table statistics including protocol, port and service.
`session`	Displays datapath session statistics. The command output includes, but not limited to, the following fields: ■ Source IP ■ Destination IP ■ SPort ■ DPort ■ Prio ■ ToS ■ Age ■ Destination ■ TAge ■ Packets ■ Bytes
`ap-name <ap-name>` `[counters | table [<A.B.C.D>]]`	Specify the name of the AP. Counters and table are optional parameters
`counters`	Displays counters statistics including current entries, high water mark, maximum entries, total entries, current maximum link length, maximum link length, stale entries, aged entries, and pending delete entries.

`dpi`
`[counters`
`[all | top | uplink-vlan <uplinkvlan>]]`
	Displays Deep Packet Information for this session. The counters parameter is optional.
	The output includes, but not limited to, the following fields:
	■ **AclVersion:** This is used to store the current version number of the ACL that is used at session creation time and is used for troubleshooting purposes.
	■ **PktsDpi:** The number of packets sent to the DPI engine for a given session.
	■ **AceIdx:** The Index of the Access List entry (in a given ACL) that triggered a match during session creation.
	■ **DpiTIdx:** This is an index to the DPI engine Tbl and is only used for troubleshooting purposes.

`high-value`	Shows high- value sessions statistics.
`ip-addr <ip-addr>` `[counters | table [<A.B.C.D>]]`	Specify the IP address of the AP. The counters and table parameters are optional.
`ip-classification`	IP reputation or geolocation information for session.

`ipv6`
`counters`
`dpi [counters [top] | table`
`[<X:X:X:X::X>] | appid <app-id>]`
`table <X:X:X:X::X>`
`verbose`
	Displays datapath IPv6 session entries and statistics including current entries, high water mark, maximum entries, total entries, allocation failures, duplicate entries, cross linked entries, number of reverse entries and maximum link length.

Parameter	Description
`session-id <sid> [dpi]`	Displays datapath session FIB for a given session index. The optional **dpi** parameter displays the deep packet information for session.
`table [<A.B.C.D>]`	Displays all the IP flows of a wireless device or Aruba AP. Statistics include table entries including source IP, destination IP, protocol, SPort, DPort, Cntr, priority, ToS, age, destination, TAge and flags.
`verbose`	Displays additional information about the session that can be used by technical support for debugging purposes. The command output includes, but not limited to, the following additional fields: ■ SIDX ■ SRTI ■ SRCI ■ UsrIdx ■ UsrVer ■ AclVer ■ NhIdx ■ NhVer
`web-cc`	Displays web-content category information about the session. The output of this command includes but not limited to the following data columns: ■ **WebCCRep**: Reputation score (integer). To see the reputation type associated with that particular score, issue the command **show web-cc reputation**. ■ **WebCCID**: Web content category ID. To see the name of the category associated with that category ID, issue the command **show web-cc category**. ■ **WebCCURL**: URL for that session entry.
`station`	Displays datapath station association table statistics.
`<id>`	Shows datapath station statistics by specified CPU id. Valid platform CPU range may vary.
`all`	Shows datapath station for all CPUs, one by one.
`counters`	Display the current and high water mark amount of 802.11 associated wireless devices on a controller. Values output from this command represent the water-marks since the last boot of the controller. This is the same value obtainable from the Num Associations output from the **show stm connectivity** command.
`crypto-counters`	Displays datapath station crypto counters or statistics.
`mac <macaddr>`	Specify the hardware address, in hexadecimal format (48-bit, station's MAC address). Shows the datapath station association with a specific MAC.
`standby`	Shows datapath station associated as standby.
`table`	Shows datapath station associations.

Parameter	Description
verbose	Shows the datapath station detail.
tcp	Displays contents of the tcp tunnel table. This command displays all TCP tunnels that are terminated by the controller.
app <app> [counters]	Specify the name of the application.
counters	Displays the TCP tunnel statistics.
tunnel table	Displays the TCP tunnel table entries. This command displays the Datapath Station Table Statistics details. Display all associated wireless devices on the controller with their corresponding AP BSSID and VLAN ID. Displays the wireless device is associated with the correct encryption type (if the device is associated to an AP BSSID that has encryption enabled and verifies whether the controller is having a problem in decrypting the wireless device's frames.
tunnel	Displays contents of the datapath tunnel table. This command displays all the tunnels that are terminated by the controller, including the GRE tunnels of Aruba AP. For example, a GRE tunnel is created and terminated on the Aruba controller for every SSID or BSSID configured on the Aruba AP. The output of the command includes, but not limited to, the following fields: ■ Source ■ Destination ■ Port ■ Type ■ MTY ■ VLAN ■ ACLs ■ BSSID ■ Decaps ■ Encaps ■ Heartbeats ■ Flags ■ Encap Bytes ■ Decap Bytes
counters	Shows tunnel counters or statistics.
encaps	Shows datapath encapsulation statistics verbose.
heartbeat	Displays the datapath heartbeat tunnel details.
ipv4	Displays the TCP tunnel table filtered on IPv4 entries.
ipv6 [encaps | verbose]	Displays the TCP tunnel table filtered on IPv6 entries. The encaps or verbose parameter is optional.
station-list	Displays the list of stations on the tunnel.

Parameter	Description
table	Tunnel table statistics.
tunnel-id <tid>	Shows datapath tunnel FIB for given tunnel index.
verbose	Shows datapath tunnel internal detail.
tunnel-group	Displays the tunnel group, active status and members.
user	Displays datapath user statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users and maximum link length.
<id>	Shows datapath user statistics by specified CPU id. Valid platform CPU range may vary.
all	Shows datapath user table for all CPUs.
ap-name <ap-name> [counters | table]	Specify the name of the AP.
counters	User counters.
ip-addr <ip-addr> [counters | table]	Specify the IP address of the AP.
ipv4	Displays datapath IPv4 user entries and statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length.
ipv6	Displays datapath IPv6 user entries and statistics such as current entries, pending deletes, high water mark, maximum entries, total entries, allocation failures, invalid users, and maximum link length.
table	User table statistics.
verbose	Shows datapath user table detail.
utilization	Displays the current CPU utilization of datapath CPUs by CPU ID. The output of the command includes CPU ID and CPU utilization during the past 1 sec, 4 sec, and 64 sec.
vlan	Displays VLAN table information such as VLAN memberships inside the datapath including Layer 2 tunnels which tunnel L2 traffic. The output fields of the command are as follows: ■ VLAN ■ Flags ■ Ingress RACL ■ Ports
ap-name <ap-name> [table]	Specify the name of the AP. Shows the datapath VLAN details.
ip-addr <ip-address> [table]	Specify the IP address of the AP. Shows the datapath VLAN details

Parameter	Description
pvst	Displays the datapath VLAN table entries.
table	Displays VLAN number, flag, port and datapath VLAN multicast entries.
vlan-mcast	Displays the datapath VLAN multicast table. The output of this command displays the datapath VLAN Multicast entries for the following fields: ■ VLAN ■ Destinations
ap-name <ap-name> [table]	Specify the name of the AP. Displays the datapath VLAN multicast table for the specific AP.
ip-addr <ip-addr> [table]	Specify the IP address of the AP. Displays the datapath VLAN multicast table for the specific IP address.
table	Displays datapath VLAN Multicast table entries.
wan-hc	Displays datapath WAN health check statistics. By default, combined statistics of all CPUs is shown.
<id>	Displays datapath WAN health check statistics by specified CPU ID. Valid platform CPU range may vary.
all	Displays datapath WAN health check statistics for all CPUs.
counters	Displays datapath WAN health check counters or statistics.
verbose	Displays datapath WAN health check detail.
web-cc [counters]	Displays web content classification table information. The output of this command includes but not limited to the following data columns: ■ Rep ■ ContentID ■ TTL ■ Age Include the optional **counters** parameter to display the maximum number of entries allowed in the web content category table.
wifi-reassembly	Displays Wi-Fi reassembly counters including CPU, current entries, high water-mark, maximum entries, total entries, and allocation failures.
<id>	Displays Wi-Fi reassembly statistics by specified CPU ID. Valid platform CPU range may vary.
all	Displays Wi-Fi reassembly statistics for all CPUs, one by one.
counters	Displays Wi-Fi reassembly counters or statistics.
verbose	Displays Wi-Fi reassembly detail.
wmm [counters]	Displays VOIP statistics, including the number of uplink and downlink resets.

Usage Guidelines

Use the **show datapath** command to display various datapath statistics for debugging purposes.

MTU guidelines

- Since MTU discovery is not enforced between an AP and standby controller in a HA setup, the value of the MTU to be passed through the tunnel is not updated.
- The size of the MTU can be set to 9000, depending on the network link and AP configuration.
- In case of a heartbeat tunnel, unanswered larger frames for MTU discovery are counted as heartbeat misses.

Example

The following example displays the discovery count table that keeps track of per client home agent discovery:

```
(host) [mynode] #show datapath mobility discovery-table
Datapath Mobility Discovery Count Table
-----------------------------------------------
Index     Valid    Version   Retry#    No-Response    Ack      Mac                Vlan
-------   ------   -------   ------    -----------    ------   --------------     -----
1         1         2        1         a              0        10:78:D2:FA:7D:38   74
```

The following example displays the datapath HA table information:

```
(host) [mynode] #show datapath mobility home-agent-table
Datapath Mobility Home Agent Table
----------------------------------
Switch IP
---------------
10.16.19.14
10.16.19.140
```

The execution of the following command displays the mobility multicast-group table that floods the multicast RA traffic to the roaming clients:

```
(host) [mynode] #show datapath mobility mcast-table
```

The following example displays the statistics of the datapath mobility:

```
(host) [mynode] #show datapath mobility stats
Datapath Mobility Stats
Mcast group entry alloc errors           : 0
Frames flooded over MMG (@HA)            : 0
Frames subjected to MMG (@FA)            : 0
Frames sent to roamed clients            : 0
HA Discovery failure to notify NACK      : 0
HA Discovery invalid DCT                 : 0
HA Discovery DCT allocation failed       : 0
HA Discovery Probes sent                 : 0
HA Discovery NULL bridge entry in DCT    : 0
HA Discovery failed to start             : 0
HA Discovery successfully started        : 0
HAT insert failure                       : 0
HAT insert success                       : 0
HAT delete failure                       : 0
HAT delete success                       : 0
```

The following example displays the mobility multicast VLAN table information:

```
(host) [mynode] #show ip mobile multicast-vlan-table
Mobility Multicast Vlan Table
-----------------------------
Client MAC           Home vlan  Current vlan
```

```
----------           ---------  ------------
40:2C:F4:36:16:07   501        501
```

The following example displays a list of tunnels.

```
(host) [mynode] #show datapath tunnel
+----+-------+-----------------------------------------------------+
|SUM/|       |                                     |               |
|CPU |  Addr | Description                                   Value |
+----+-------+-----------------------------------------------------+
|    |       |                                                     |
| G  | [000] | Current Entries                                  10 |
| G  | [002] | High Water Mark                                  12 |
| G  | [003] | Maximum Entries                               24576 |
| G  | [004] | Total Entries                                    12 |
| G  | [006] | Max link length                                   1 |
+----+-------+-----------------------------------------------------+
Datapath Tunnel Table Entries
-----------------------------
Flags: E - Ether encap,  I - Wi-Fi encap,  R - Wired tunnel,  F - IP fragment OK
W - WEP,  K - TKIP,  A - AESCCM,  G - AESGCM,  M - no mcast src filtering
S - Single encrypt,  U - Untagged,  X - Tunneled node,  1(cert-id) - 802.1X Term-PEAP
2(cert-id) - 802.1X Term-TLS,  T - Trusted,  L - No looping, d - Drop Bcast/Unknown Mcast,
D - Decrypt tunnel,  a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast
n - Convert RAs to unicast(VLAN Pooling/L3 Mobility enabled), s - Split tunnel
V - enforce user vlan(open clients only), x - Striping IP, z - Datazone
H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t - Cluster s-AAC tunnel
c- IP Compression, g - PAN GlobalProtect Tunnel, w - Tunneled Node Heartbeat
#          Source       Destination    Prt  Type  MTU   VLAN       Acls
BSSID
------  --------------  --------------  ---  ----  ----  ---- ----------------------  -------
----------
12      SPI01972200 in  10.17.41.82     50   IPSE  1500  0    routeDest 0000     0
11      SPIFC376400out  10.17.65.115    50   IPSE  1500  0    routeDest 0001     0

Decaps      Encaps     Heartbeats  Flags           EncapKBytes   DecapKBytes
---------- ---------- ----------   --------------- ------------ -----------
6602          0                    T                 0           0
0             4376                 T                 0           0
```

The following example displays output of L2 GRE Tunnel Interface.

```
(host) [mynode] #show datapath tunnel ipv6
Datapath Tunnel Table Entries
-----------------------------
Flags: E - Ether encap,  I - Wi-Fi encap,  R - Wired tunnel,  F - IP fragment OK
W - WEP,  K - TKIP,  A - AESCCM,  M - no mcast src filtering
S - Single encrypt,  U - Untagged,  X - MUX,  1 - 802.1X Term
T - Trusted,  L - No looping, d - Drop Bcast/Unknown Mcast, D - Decrypt tunnel
a - Reduce ARP packets in the air, e - EAPOL only
C - Prohibit new calls, P - Permanent, m - Convert multicast, n - Convert RAs to unicast(VLAN
Pooling/L3 Mobility enabled),
V - enforce user vlan(open clients only), z - Datazone
H - Standby (HA-Lite), u - Cluster UAC tunnel, b - Active AAC tunnel, t - Cluster s-AAC tunnel
w - Tunneled Node Heartbeat
#      Source          Destination         Prt  Type  MTU   VLAN   Acls   BSSID
------ -------------  -------------------- ---  ----  ----  ----  ------- -----------------
16     2046:eab::25    2047:eab::25        47   0     1280   0    0       00:00:00:00:00:00

Decaps     Encaps   Heartbeats   Flags
---------- --------- -----------  -----
119209     25535    28873        TEFPR
```

The following example displays the tunnel statistics.

```
(host) [mynode] #show datapath tunnel counters
+----+------+-------------------------------------------------------+
|SUM/|      |                                       |               |
|CPU | Addr | Description                                     Value |
+----+------+-------------------------------------------------------+
|    | [00] | Tunnel FIB forwarded                             38437 |
|    | [02] | GRE Encap drop                                     221 |
|    | [03] | GRE Encap fallback to session             1237276789 |
|    | [04] | Tunnel FIB stale                             1176392 |
+----+------+-------------------------------------------------------+
|    |      |                                                       |
| G  | [00] | Current Entries                                  9366 |
| G  | [02] | High Water Mark                                  9703 |
| G  | [03] | Maximum Entries                                 98304 |
| G  | [04] | Total Entries                                 2876603
| G  | [06] | Max link length                                     7 |
| G  | [07] | Current Tunnel FIB                                  1 |
| G  | [08] | Tunnel FIB recompute                         1176170 |
+----+------+-------------------------------------------------------+
```

The output parameters of the **show datapath tunnel counters** command are explained in the following table:

Output Parameter	Description
Current Entries	Number of tunnels that are active in the system.
Pending Deletes	Number of tunnel entries that are marked to be deleted.
High Water Mark	Maximum number of active entries recorded under Current Entries.
Maximum Entries	Maximum number of tunnel entries that can be supported by the platform.
Total Entries	Total number of tunnel entries in the system.
Allocation Failures	Total number of tunnel entry allocation failures.
Max Link Length	Indicates the length of the linked list that has the maximum length in the hash table.
Current Tunnel FIB	Number of tunnel FIB entries that are recomputed and have a valid session entry and route cache entry.
Tunnel FIB Recompute	Number of invalid tunnel FIB entries for which tunnel FIB is recomputed.
Tunnel FIB forwarded	Number of packets that are forwarded through tunnel.
Tunnel FIB Egress Not Unicast	Number of packets whose bridge entry is not found or whose egress destination is not unicast.
GRE Encap drop	Number of packets that are dropped due to various reasons such as destination is not a tunnel, tunnel is not valid, packet length exceeded the allowed MTU, and so on.
GRE Encap fallback to session	Number of packets that are not permitted to be directly forwarded using tunnel FIB, but rather have to fall back to the session-route processing in the pipeline.

Output Parameter	Description
Tunnel FIB stale	Number of tunnel FIB entries that are invalid due to invalid session or tunnel version number not matching the session version number.

The following example displays a partial list of crypto parameter statistics.

```
(host) [mynode] #show datapath crypto counters
+----+-------+-------------------------------------------------------+
|SUM/|       |                                       |               |
|CPU |  Addr | Description                                     Value |
+----+-------+-------------------------------------------------------+
|    | [000] | Crypto Requests Total                           25751 |
|    | [002] | Crypto Response received                        25751 |
|    | [034] | IPSec drops UDP encap NATT port mis                60 |
|    | [153] | RSA Requests                                        9 |
|    | [155] | RSA Response received                               9 |
+----+-------+-------------------------------------------------------+
|    |       |                                                       |
| G  | [001] | Crypto Cores In Use                                 4 |
| G  | [014] | DOT1X Term Buffers                               4096 |
| G  | [015] | DOT1X Term Buffers Free                          4096 |
+----+-------+-------------------------------------------------------+
| G  | [000] | Crypto Accelerator Present                       TRUE |
+----+-------+-------------------------------------------------------+
```

The following parameters appear in the output of the **show datapath crypto counters** command, and are useful for debugging purposes.

Parameter	Description
Crypto BadNPlus	Indicates a queue overrun in the output of the encryption circuit.
Crypto SendNPlusFailed	Indicates a queue overrun in the input of the encryption circuit.
IPSec Frag Failures	This counter increments when the AP detects a failure to fragment a frame before or after IPsec encryption.
IPSec Invalid Length	The inbound IPsec frame length is verified before and after decryption. If the frame length is found to be incorrect , this counter is incremented.
IKE Rate	When the managed device firewall receives a UDP packet, it determines if the packet is destined for an IKE (500) or IPsec_NATT (4500) port. This counter increments when the AP receives an initial IKE packet that has an 8-byte responder cookie defined all 0s.

The following example displays the output of the **show datapath frame** and **show datapath frame counters** commands.

```
(host) [mynode] #show datapath frame
+----+------+-------------------------------------------------------+
|SUM/|      |                                       |               |
|CPU | Addr | Description                                     Value |
+----+------+-------------------------------------------------------+
|    | [00] | Allocated Frames                                 7068 |
|    | [01] | Max Allocated Frames                             7391 |
|    | [03] | Unknown Unicast                                  6117 |
|    | [10] | IP Reassembled Datagrams                         9310 |
|    | [14] | IP Reassembly Failures                          15791 |
|    | [36] | Flood Frames                                   948757 |
|    | [60] | VOQ retries                                       536 |
```

```
+----+------+-----------------------------------------------------+
|    |      |                                                     |
| G  | [00] | BPDUs Received                                948910 |
+----+------+-----------------------------------------------------+

(host) [mynode] #show datapath frame counters
 +----+------+-----------------------------------------------------+
|SUM/|      |                                     |                 |
|CPU | Addr | Description                                   Value |
+----+------+-----------------------------------------------------+
|    | [00] | Rx Frames                                  29033086 |
|    | [01] | Rx Bytes                                  812728150 |
|    | [02] | Tx Frames                                   3515809 |
|    | [21] | Ipv4 VPN Denied Frames                            6 |
|    | [27] | Ipv4 Firewall Denied Frames                       1 |
|    | [36] | Dot1d Discards                                  313 |
+----+------+-----------------------------------------------------+
```

The following table provides description for some important output parameters of **show datapath frame** and **show datapath frame counters** commands:

Output Parameter	Description
Allocated Frames	Statically pre-allocated frames (for handling data-traffic) and dynamically allocated frames (for internal control-traffic).
Max Allocated Frames	Max watermark of Allocated Frames.
TX Underrun	Hardware counter if MAC was fetching packet data while packet is being transmitted.
TX Max Collision-Late Abort	Hardware counter if packet transmission was aborted due to maximum collision count exceeded (10 or 100 modes only) or a late abort.
Frame Denied L2-GRE Loop	Packets where Ingress and Egress are same (Enabled for Mobility feature only).
Unknown Unicast	Unknown dest-mac counter.
IPv6 Unknown Unicast	Unknown Unicast for IPv6 ethtype.
IP Datagrams Fragmented	IP datagrams fragmented when packet-length is greater than Tunnel MTU (Tunnel can be between controllers or controller and AP).
WIFI AMSDU	Wi-Fi A-MSDU frames received from Wi-Fi clients.
WIFI AMSDU Aggregated	A-MSDU frames sent by controller to Wi-Fi clients.
Runts Received	Packet length is less than minimum header length.
Station Not Data Ready	Packets received by a controller from the APs or Stations before they got provisioned.
Station Inactive	Packets received by a controller from the APs or Stations after they were inactive.
Association Throttle	Drops of APs or Stations Associate coming at high rate (e.g., during failover).

Output Parameter	Description
IKE Throttle	Drops of IKE packets coming at high rate.
IPv6 NA Spoofs	IPv6 Network Advertisement spoofs.
IPv6 NS Spoofs	IPv6 Network Solicitation spoofs.
EOP zero frames	Zero length frames.
CP Policed Frames	Packets bound to Control plane from Data plane dropped.
Seqno request failure	Wi-Fi Sequence no. request failed.
Heartbeats sent to SP	Tunnel Heartbeats punted to Slowpath (due to route-cache miss, etc.)
Heartbeats dropped by FP	Tunnel Heartbeats dropped in data plane.
POE descriptor freed	Internal counter
CP Enqueue Buffer Alloc Failure	Buffer allocation failures while sending packets to Control plane.
VOQ retries	Virtual Output Queues are packet exchanges between any two entities (CPU or Hardware offload engines) that have failed due to there not being any available credits. Packets are scheduled to be retried at a later point in time.
Seqno responses sent	The sequence number sent in response to sequence number requests used in Wi-Fi frames.
Dot1Q Discards	The Dot1Q discard counter may increase as a result of the following: 1. An incoming frame's VLAN does not match a port's configured VLAN. 2. A trunk port is not a member of the received frames's VLAN and the received frame is not an STP BPDU, CISCO BPDU or an LACP PDU. 3. A received frame has three or more stacked (QnQ tagged) VLANs. 4. A received frame contains more than one VLAN tag, however the expected number of VLAN tags is one. 5. An untagged access port is not a member of the VLAN in the received frame. 6. A station has sent a tagged VLAN frame. 7. A received LLDP frame has no multicast destination. 8. A received frame has no multicast destination in the VLAN group.
Dot1D Discards	The Dot1d discard counter may increase as a result of the following: 1. If a port is in STP blocking state, then received frames are dropped. 2. The tagged frame received on untagged port and dropped. 3. Received frame length is less than (Ethernet + VLAN) header length. 4. Frames that have been dropped due to bridge filtering. 5. Port has MUX flag set but NULL egress destination. 6. Frame drop either if destined for non-tunnel or to port channel or destination tunnel with no multicast configured. 7. Dropped frames addressed to BPDU MACs but not configured in the bridge table. 8. Dropped unexpected frames.

When the counter value is zero, the output parameter line is not displayed.

Some of the other output parameters that could be part of the **show datapath frame** command are as follows:

- IP Fragmentation Failures
- IP Jumbo Fragmentation Failures
- IP Jumbo IPSec Encrption Failures
- IP Reassembled Datagrams
- IP Reassembly overlaps
- IP Reassembly PAPI Failures
- IP Reassembly PAPI
- IP Reassembly Failures
- IPv6 Datagrams Fragmented
- IPv6 Fragmentation Failures
- IPv6 Reassembled Datagrams
- IPv6 Reassembly overlaps
- Invalid IP headers Received
- Invalid IPv6 headers Received
- Too Many IPv6 Ext. Hdrs Received
- xSec Frames Re-Assembled
- xSec Re-Assembly Failures
- Flood Frames
- Flood Frames Peak Value
- ARP Request Spoofs
- ARP Reply Spoofs
- Gratuitous ARP Spoofs
- IP spoofs
- CPU based seqno resp
- Frame Length Failure
- Packet send failed and will be retried later
- Invalid Tail Room DDMO
- Invalid mcast entry
- Jumbo Wi-Fi Frames
- Invalid ingress frames
- Invalid egress frames
- Invalid opcode
- Invalid Port
- Invalid Slot
- Invalid ACL
- Jumbo discards
- Jumbo recvd
- Jumbo xmits
- Jumbo drops
- Jumbo wire to wireless drops
- Jumbo xmits Failures
- Jumbo drops [Non Jumbo Port]
- Jumbo drops [Wireless client]
- Flooded Jumbo Frames
- Buffer Alloc Failure
- NAE Transmit Failure
- Total queued BWM packets
- Excessive ARP Requests
- Drops - DPI enforcement
- Drops - WEB CC enforcement
- IPv6 Vlan Discards
- Drops - Wireless client garps

The following is an example of the **show datapath compression** command output:

```
+----+------+-----------------------------------------------------+
|SUM/|      |                                     |               |
|CPU | Addr | Description                                   Value |
+----+------+-----------------------------------------------------+
|    | [00] | Compression Engine Present                     True |
|    | [01] | Comp Response received                          150 |
|    | [02] | Comp Response failed                              0 |
|    | [03] | Decomp Requests                                  80 |
|    | [04] | Decomp Response received                         80 |
|    | [05] | Decomp Requests queued                           75 |
| G  | [06] | Compression Engine Total                          4 |
+----+------+-----------------------------------------------------+
```

When the counter value is zero, the output parameter line is not displayed.

The following example displays the output of the **show datapath bwm table** command:

```
(host) [mynode] #show datapath bwm table
Datapath Bandwidth Management Table Entries
-------------------------------------------
Contract Types :
0 - CP Dos 1 - Configured contracts 2 - Internal contracts
----------------------------------------------
Flags: Q - No drop, P - No shape(Only Policed),
T - Auto tuned
-----------------------------------------------------------------------
Rate: pps - Packets-per-second (256 byte packets), bps - Bits-per-second
-----------------------------------------------------------------------
Cont                          Avail     Queued/Pkts
Type   Id    Rate      Policed      Credits    Bytes      Flags   CPU     Status
----  ----  ---------  ----------  -------  -----------   ------- -------  ------
0     1     9792 pps             0      306        0/0            9        ALLOCATED
0     2     3936 pps             0      123        0/0            9        ALLOCATED
0     3     65536 pps            0     2047        0/0            9        ALLOCATED
0     4     3936 pps             0      123        0/0            9        ALLOCATED
0     5     992 pps              0       31        0/0            9        ALLOCATED
0     6     992 pps              0       31        0/0            9        ALLOCATED
0     7     992 pps              0       31        0/0            9        ALLOCATED
```

```
0     8     512 pps          0       16       0/0          9       ALLOCATED
0     9     3936 pps         0      123       0/0          9       ALLOCATED
0     10    1984 pps         0       62       0/0          9       ALLOCATED
1     1     5 Mbps           0    19532       0/0          17      ALLOCATED
```

If the policed counter is a non-zero value, it means excessive traffic of that type that has been dropped to avoid saturating the Control Plane, resulting in potential DoS.

The following table provides description for the contract IDs 1-10 as well as the corresponding firewall parameters:

Contract ID	Contract Description	Firewall Parameter
1	Rate limit Control-Plane-bound untrusted unicast packets. It is used to limit Web CC traffic to CP.	untrusted-ucast
2	Rate limit Control-Plane-bound untrusted multicast packets. It limits ACL logging, packet capture traffic.	untrusted-mcast
3	Rate limit Control-Plane-bound trusted unicast packets.	trusted-ucast
4	Rate limit Control-Plane-bound trusted multicast packets.	trusted-mcast
5	Rate limit Control-Plane-bound routed packets.	route
6	Rate limit Control-Plane-bound GRE control-plane session mirrored packets.	sessmir
7	Rate limit Control-Plane-bound authentication-related packets.	auth
8	Rate limit Control-Plane-bound VRRP protocol packets.	vrrp
9	Rate limit Control-Plane-bound ARP protocol packets	arp-traffic
10	Rate limit Control-Plane-bound other Layer-2 or bridging packets - Non-ARP traffic.	l2-other

Command History

Release	Modification
ArubaOS 8.2.0.0	The **netdest-id**, and **remote-device-table** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show dds debug

```
show dds debug
global_object_db [peer <A.B.C.D> [rkey <rkey-id>]|peerv6 <X:X:X:X::X>]
message-stats
peers
rkey
replicaton <sources>
stats
```

Description

This command shows the dds debug information.

Syntax

Parameter	Description
`global_object_db`	DDS global object database.
`peer <A.B.C.D>`	Peer for the global object database.
`rkey <rkey-id>`	Replication key for the global object database.
`peerv6 <X:X:X:X::X>`	Set peer ipv6 address.
`message-stats`	Message statistics.
`peers`	Remote peers.
`replication`	Object replication.
`rkey <rkey-id>`	Replication keys
`stats`	Statistics of the DDS log

Command History

Release	Modification
ArubaOS 8.2.0.0	The **peerv6** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show debug

```
show debug
```

Description

This command shows the debug information for debug logging levels.

Syntax

No Parameters

Example

```
(host) [mynode] (config) #show debug
DEBUG LEVELS
------------
Facility    Level      Debug Value         Sub Category  Process
--------    -----      -----------         ------------  -------
user-debug  debugging  12:12:12:12:12:12   N/A           N/A
```

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, facility, severity, and the type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show dialer group

```
show dialer group
```

Description

Display dialer group information.

Syntax

No parameters.

Usage Guidelines

Displays the Dialer Group Table with the current dialing parameters.

Example

```
(host) #show dialer group
Dialer Group Table
------------------
Name      Init String                       Dial String
----      -----------                       -----------
evdo_us   ATQ0V1E0                          ATDT#777
gsm_us    AT+CGDCONT=1,"IP","ISP.CINGULAR"  ATD*99#
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show dot1x ap-table

```
show dot1x ap-table
```

Description

Shows the 802.1X AP table.

Syntax

No parameters.

Example

Issue this command to display details from the AP table.

```
AP Table
--------
MAC                IP          Essid       Type AP name           Vlan Enc           Stations
Forwarding-Mode        Profile          Acl
---                --          -----       ---- -------           ---- ---           -------- ---
------------        -------          ---
00:1a:1e:87:ff:c0 10.3.9.242             AP   00:1a:1e:c0:7f:fc 0    -             0
FORWARD_TUNNEL_80211  default/        1
00:1a:1e:87:ff:d0 10.3.9.242 sw-pn-nokia AP   00:1a:1e:c0:7f:fc 0    WPA2-AES      0
FORWARD_TUNNEL_80211  default/default 1
00:1a:1e:82:ab:a0 10.3.9.220             AP   monitor-124       0    -             0
FORWARD_TUNNEL_80211  default/        1
00:1a:1e:82:ab:b0 10.3.9.220             AP   monitor-124       0    -             0
FORWARD_TUNNEL_80211  default/        1
00:1a:1e:87:ff:d1 10.3.9.242 sw-pn-t2    AP   00:1a:1e:c0:7f:fc 0    WPA2-PSK-AES  0
FORWARD_TUNNEL_80211  default/default 1
Num APs: 5
```

The output of this command includes the following parameters:

Parameter	Description
MAC	The MAC address of the AP
IP	The IP address of the AP
Essid	The AP's ESSID
Type	Device type
AP name	Name of the AP
Vlan	Number of VLANs associated with the specified AP
Enc	AP's encryption method
Stations	Number of stations associated with the specified AP
Forwarding Mode	Forwarding mode used by the specified AP
Profile	AP profile
Acl	Number of ACLs this AP belongs to

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show dot1x ap-table aes

```
show dot1x ap-table aes
```

Description

Shows the AES keys of all APs.

Syntax

No parameters.

Example

Issue this command to display AES keys of all APs.

```
AP Table Showing AES Keys
-------------------------
AP-MAC              GTK/Size/Slot
------              -------------
00:1a:1e:87:ff:d0   * * * * * * * */128-Bit/1
00:1a:1e:87:ff:d1   * * * * * * * */128-Bit/1
```

The output of this command includes the following parameters:

Parameter	Description
`AP-MAC`	AP MAC address
`GTK/Size/Slot`	GTK: The group temporal key Size: Size of the AES key Slot: Slot number

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x ap-table dynamic-wep

```
show dot1x ap-table dynamic-wep
```

Description

Shows the dynamic WEP keys of all APs.

Syntax

No parameters.

Example

Issue this command to display dynamic keys of all APs.

```
Dynamic-WEP Key Information
---------------------------
AP-MAC  Key1/Size/Slot  Key2/Size/Slot
------  --------------  --------------
Num APs: 0
```

The output of this command includes the following parameters:

Parameter	Description
`AP-MAC`	AP MAC address
`Key1/Size/Slot`	Key1: The WEP key Size: Size of the WEP key Slot: Slot number
`Key12/Size/Slot`	Key2: The WEP key Size: Size of the WEP key Slot: Slot number

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x ap-table static-wep

```
show dot1x ap-table static-wep
```

Description

Shows the static WEP keys of all APs.

Syntax

No parameters.

Example

Issue this command to display the static WEP keys of all APs.

```
Static-WEP Key Information
--------------------------
AP-MAC  Key1/Size  Key2/Size  Key3/Size  Key3/Size
------  ---------  ---------  ---------  ---------
Num APs: 0
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP's MAC address
Key1/Size	WEP key 1 and its size
Key2/Size	WEP key 2 and its size
Key3/Size	WEP key 3 and its size
Key3/Size	WEP key 3 and its size

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x ap-table tkip

```
show dot1x ap-table tkip
```

Description

Displays a table of TKIP keys on the managed devices.

Syntax

No parameters.

Example

Issue this command to display all TKIP keys.

```
AP Table Showing TKIP Keys
--------------------------
AP-MAC             GTK/Size/Slot
------             -------------
00:1a:1e:6f:e5:10  * * * * * * * */256-Bit/1
Num APs: 1
```

The output of this command includes the following parameters:

Parameter	Description
AP-MAC	AP MAC Address
GTK/Size/Slot	GTK: The group temporal key Size: Size of the AES key Slot: Slot number

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x ap-hash-table

```
show dot1x ap-hash-table
```

Description

Shows the 802.1X ap hash table.

Syntax

No parameters.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x certificate details

```
show dot1x certificates details
```

Description

Displays a detailed 802.1X certificate usage.

Example

```
(host) [mynode] (config) #show dot1x certificates details

Certficate Hash table entries
-----------------------------
Certificate Name: default-self-signed
Usage Count: 3, Dot1x:Yes, Captive portal:No, Ldap:No
Dot1x certificate table entries
-------------------------------
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show dot1x counters

```
show dot1x counters
```

Description

Displays a table of dot1x counters.

Example

Issue this command to display all 802.1X counter information.

```
802.1X Counters

AP
 Sync Request...................4
 Sync Response..................3
 Up.............................4
 Down...........................1
 Resps..........................4
 Acl............................53
Station
 Sync Request...................9
 Sync Response..................9
 Up.............................2321
 Down...........................2272
 Unknown........................72
EAP
 RX Pkts........................4811
 Dropped Pkts...................4497
 TX Pkts........................5253
WPA
 Message-1......................2484
 Message-2......................63
 Message-3......................63
 Message-4......................63
 Group Message-1................63
 Group Message-2................63
 Rx Failed......................2418
 IE Mismatches..................4836
 Key Exchange Failures..........602
WPA2
 Message-1......................2630
 Message-2......................13
 Message-3......................13
 Message-4......................13
 Rx Failed......................2079
 IE Mismatches..................4158
 Key Exchange Failures..........549
Radius
 Accept.........................1217
Station Deauths.................1151
```

The output of this command includes the following parameters:

Parameter	Description
AP ■ Sync Request ■ Sync Response ■ Up ■ Down ■ Resps ■ Acl	■ Number of sync requests sent ■ Number of sync responses sent ■ Number of times an AP has come up ■ Number of times an has gone down ■ Number of response messages sent to the AP due to an AP up message ■ Number of ACLs
Station ■ Sync Request ■ Sync Response ■ Up ■ Down ■ Unknown	■ Number of sync requests sent to find all APs and stations that are connected ■ Number of sync responses received ■ Number of times a station (any station) connected to the AP ■ Number of times a station (any station) disconnected from the AP ■ Number of times a station attempted to start an EAP exchange before associating to an AP. In other words, the number of times the auth module saw the start of an EAP exchange before auth was notified that a station has associated an AP
EAP ■ RX Pkts ■ Dropped Pkts ■ TX Pkts	■ Number of EAP packets received ■ Number of EAP packets dropped (ignored) for any reason, such as bad packet, length, EAP ID mismatch, etc. ■ Number of EAP packets sent
WPA ■ Message-1 ■ Message-2 ■ Message-3 ■ Message-4 ■ Group Message-1 ■ Group Message-2 ■ Rx Failed ■ IE Mismatches ■ Key Exchange Failures	■ Number of WPA message-1s sent ■ Number of WPA message-2s sent ■ Number of WPA message-3s sent ■ Number of WPA message-4s sent ■ Number of WPA group message-1s sent ■ Number of WPA group message-2s sent ■ Number of WPA related EAP packets dropped for any reason ■ Number of WPA related EAP packets dropped because the station and controller have a different perception of what the connection details are ■ Number of key exchange failures
WPA2 ■ Message-1 ■ Message-2 ■ Message-3 ■ Message-4 ■ Rx Failed ■ IE Mismatches ■ Key Exchange Failures	■ Number of WPA2 message-1s sent ■ Number of WPA2 message-2s sent ■ Number of WPA2 message-3s sent ■ Number of WPA2 message-4s sent ■ Number of WPA2 related EAP packets dropped for any reason ■ Number of WPA2 related EAP packets dropped because the station and controller have a different perception of what the connection details are ■ Number of key exchange failures
Radius Accept	Number of RADIUS accepts
Station Deauths	Number of stations deaths

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show dot1x supplicant-info

```
show dot1x machine-auth-cache <supplicant-mac>
```

Description

Shows the machine authentication cache.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x supplicant-info

```
show dot1x supplicant-info <supplicant-mac> <ap-mac>
```

Description

Shows the details about a specific supplicant.

Example

Issue this command to display the details about a supplicant.

```
Name                                MYCORPNETWORKS\ccutler
MAC Address                         00:19:7e:a9:8e:b0
AP MAC Address                      00:1a:1e:11:5f:11
Status                              Authentication Success
Unicast Cipher                      WPA2-AES
Multicast Cipher                    WPA2-AES
EAP-Type                            EAP-PEAP
Packet Statistics:
EAPOL Starts                        0
EAP ID Requests                     0
EAP ID Responses                    0
EAPOL Logoffs from station          0
EAP pkts to the station             2
EAP pkts from station               2
Unknown EAP pkts from station       0
EAP Successes sent                  0
EAP Failures sent                   0
Station failed to respond           0
Station NAKs                        0
Radius pkts to the server           0
Radius pkts from the server         0
Server failed to respond            0
Server rejects                      0
WPA/WPA2-Key Message1               1
WPA/WPA2-Key Message2               1
WPA/WPA2-Key Message3               1
WPA/WPA2-Key Message4               1
WPA-GKey Message1                   0
WPA-GKey Message2                   0
ID of the last EAP request          0
Length of the last EAP request      151
ID of the last EAP response         0
Length of the last EAP response     0
ID of the last radius request       0
Length of the last radius request   0
ID of the last radius response      0
```

The output of this command includes the following parameters:

Parameter	Description
Name	Supplicant name.
MAC Address	Supplicant MAC address.
AP MAC Address	AP MAC address.
Status	Supplicant's status.
Unicast Cipher	Supplicant's unicast cipher.
Multicast Cipher	Supplicant's multicast cipher.
EAP-Type	Supplicant's EAP-Type.
EAPOL Starts	Number of EAPOL starts.
EAP ID Requests	Number of EAP ID requests.
EAP ID Responses	Number of EAP ID responses.
EAPOL Logoffs from station	Number of EAPOL logoffs from the station.
EAP pkts to the station	Number of EAP packets sent to the station.
EAP pkts from station	Number of EAP packets sent from the station.
Unknown EAP pkts from station	Number of unknown EAP packets sent from the station.
EAP Successes sent	Number of EAP successes sent.
EAP Failures sent	Number of EAP failures sent.
Station failed to respond	Number of times the station failed to respond.
Station NAKs	Number of station negative-acknowledgement characters.
Radius pkts to the server	Number of RADIUS packets set to the server.
Radius pkts from the server	Number of RADIUS packets sent from the server.
Server failed to respond	Number of times the server failed to respond.
Server rejects	Number of times ac connection was rejected by the server.
WPA/WPA2-Key Message1	Number of WPA message-1s sent
WPA/WPA2-Key Message2	Number of WPA message-2s sent.
WPA/WPA2-Key Message3	Number of WPA message-3s sent.
WPA/WPA2-Key Message4	Number of WPA message-4s sent.
WPA-GKey Message1	Number of WPA group message-1s sent.
WPA-GKey Message2	Number of WPA group message-2s sent.
ID of the last EAP request	The ID of the last EAP request.

Parameter	Description
`Length of the last EAP request`	The length of the last EAP request.
`ID of the last EAP response`	The ID of the last EAP response.
`Length of the last EAP response`	The length of the last EAP response.
`ID of the last radius request`	The ID of the last RADIUS request.
`Length of the last radius request`	The length of the last RADIUS request.
`ID of the last radius response`	The ID of the last RADIUS response.
`Length of the last radius response`	The length of the last RADIUS response.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x supplicant-info list-all

```
show dot1x supplicant-info list all
```

Description

Shows all 802.1X supplicants.

Syntax

No parameters.

Example

Issue this command to display all 802.1X supplicants as well as additional relevant information.

```
802.1X User Information
-----------------------
     MAC              Name     Auth  AP-MAC                Enc-Key/Type              Auth-Mode
 EAP-Type  Remote
------------       --------  ----  ------             -------------------       ------------
---------  ------
00:15:00:26:f8:f5  user1     Yes   00:0b:86:8b:68:68  * * * * * * * */WPA2-AES  Explicit Mode
EAP-PEAP   No

Station Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address
Name	Supplicant name
Auth	Shows if the supplicant authenticated successfully
AP-MAC	AP MAC address
Enc-Key/Type	Enc-Key: Supplicant's encryption key Type: Encryption type used by the supplicant
Auth-Mode	Authentication mode
EAP-Type	EAP type
Remote	Is the supplicant remote

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x supplicant-info pmkid

```
show dot1x supplicant-info pmkid <supplicant-mac>
```

Description

Shows the PMKIDs of the various stations on the controller.

Syntax

No parameters.

Example

Issue this command to display the PMKIDs of the various stations on the controller.

```
PMKID Table
  -----------
  Mac                Name            AP                PMKID
  ---                ----            --                -----
  00:03:7f:bf:12:ac  zoobar22  00:0b:86:a0:57:60
c2:7d:12:1a:1c:5b:40:f8:89:46:22:a5:ec:9b:fb:a6
  00:03:7f:bf:12:ac  zoobar22  00:0b:86:c0:04:88
bb:2d:e1:57:e1:b8:9b:a2:71:f5:98:ad:61:db:47:e7
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address
Name	Supplicant name
AP	AP MAC address
PMKID	Station PMKID

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x supplicant-info statistics

```
show dot1x supplicant-info statistics
```

Description

Shows the 802.1X statistics of the users.

Syntax

No parameters.

Example

Issue this command to display the 802.1X statistics of the users.

```
802.1X Statistics
-----------------
Mac                 Name    AP                 Auth-Succs  Auth-Fails  Auth-Tmout  Re-Auths
Supp-Naks  UKeyRotations  MKeyRotations
---                 ----    --                 ----------  ----------  ----------  --------  ---
------  -------------  -------------
00:15:00:26:f8:f5  user1   00:0b:86:8b:68:68  1           0           0           0         0
       0              0
Total:                                         2           0           0           0         0
       0              0

Station Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
MAC	Supplicant MAC address.
Name	Supplicant name.
AP	AP MAC address.
Auth-Succs	Number of successful authentications.
Auth-Fails	Number of authentication failures.
Auth-Tmout	Number of authentication timeouts.
Re-Auths	Number of reauthentications.
Supp-Naks	Number of negative-acknowledgement characters sent by the supplicant.
UKeyRotations	Number of unicast key rotations.
MKeyRotations	Number of multicast key rotations.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x supplicant-info reauth-table

```
show dot1x supplicant-info reauth-table [all|history|mac]
```

Description

Shows the reauthentication related information.

Syntax

Parameter	Description
`all`	All entries in reauth-table.
history	Information about last few reauth sweeps.
mac	Supplicant MAC address.

Command History

Version	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dot1x watermark

```
crypto-local
show dot1x watermark
   history
   table {active|pending}
```

Description

Use this command under the guidance of Aruba support to view information about the table that contains 802.1X sessions being processed.

Syntax

Parameter	Description	Range	Default
`history`	Displays all historical sessions in the 802.1X session queue.	—	—
`table {active|pending}`	Table types: ■ **active**: Displays all current active sessions in the 802.1X queue and the corresponding user-age. ■ **pending**: Displays all pending sessions in the 802.1X queue, the duration for which the user is pending in the queue, and the corresponding user-age.	—	—

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show dot1x wired-ap-table

```
show dot1x wired-ap-table
```

Description

Shows the 802.1X Wired AP table.

Syntax

No parameters.

Command History

Version	Description
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show dpi

```
show dpi
application
   name
   all
   category <name>
   custom-app <name>
global-bandwidth-contract
   all
   category <name>
   custom-app <name>
custom-app
   all
   string
```

Description

Shows applications and application categories that are configured for DPI. It also shows DPI global bandwidth contracts by application or application category.

Syntax

Parameter	Description
`name`	Name of the application.
`all`	Shows all applications.
`category <name>`	Shows all applications within a category.
`custom-app <name>`	Shows all custom applications.
`global-bandwidth-contract`	Shows the DPI global bandwidth contracts.
`all`	Shows all bandwidth contracts.
`app <name>`	Shows bandwidth contracts by application name.
`appcategory <name>`	Shows bandwidth contracts by application category name.
`custom-app`	Show custom applications.
`all`	Show all applications.
`string`	Name of the application to show.

Example

The output of the following command shows custom applications by name, ID, application category, and default ports that are configured for DPI.

```
(host) (config) #show dpi application all
Applications
------------
Name                App ID  App Category         Default Ports              Applied
----                ------  ------------         -------------              -------
01net               948     web                  tcp 80                     0
050plus             1123    audio-video          tcp 80 443                 0
0zz0                584     web                  tcp 80                     0
```

```
10050net            1339    web                 tcp 80                  0
10086cn             949     web                 tcp 80 443              0
104com              1336    web                 tcp 80                  0
1111tw              1338    web                 tcp 80                  0
1141a               950     web                 tcp 80                  0
115com              951     web                 tcp 80 443              0
118114cn            952     web                 tcp 80                  0
11st                1191    web                 tcp 80                  0
```

Related Commands

Command	Description	Mode
dpi	Use this command to configures DPI and the global bandwidth contract for an application or application categories for the AppRF feature.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show esi groups

```
show esi groups [{group-name <groupname>|{ping-name <ping-name>}]
```

Description

Show ESI group information.

Syntax

Parameter	Description
group-name <groupname>	View the facility used when logging messages into the remote syslog server.
ping-name <ping-name>	Enter the name of a set of ping values to how the names of ESI groups using that set of ping attributes. Define a set of ESI ping values using the command esi ping.

Usage Guidelines

The ESI parser is a mechanism for interpreting syslog messages from third party appliances such as anti-virus gateways. Use this command to view configured ESI server groups.

Example

This example below displays the name of each configured ESI group, including its ping definitions and ESI server.

```
(host) #show esi groups

ESI Group Table
---------------
Name        Tunnel ID  Ping      Flags  Servers
----        ---------  ----      -----  -------
anything    0x1042     pingset_1 C      0
cupertino   0x1043     -         C      0
Flags:
  C:Datapath Download complete
```

Related Commands

Platforms	Licensing	Command Mode
esi parser domain	This command configures an ESI syslog parser domain.	Config mode on Mobility Master
esi parser rule	This command creates or changes an ESI syslog parser rule.	Config mode on Mobility Master

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show esi parser

```
show esi parser domains|rules|stats
```

Description

Show ESI parser information.

Syntax

Parameter	Description
`domains`	Show ESI parser domain information.
`rules`	Show ESI parser rule information.
`stats`	Show ESI parser rule stats.

Usage Guidelines

The ESI parser is a generic syslog parser on the controller that accepts syslog messages from external third-party appliances such as anti-virus gateways, content filters, and IDS. It processes syslog messages according to user-defined rules and takes configurable actions on the corresponding system users.

ESI servers are configured into domains to which ESI syslog parser rules are applied.

Use the **`show esi parser domains`** command to show ESI parser domain information.

Example

The ESI Parser Domain table in the example below shows that the controller has two ESI domains and two ESI servers.

```
(host) [mynode] (config) #show esi parser domains

ESI Parser Domain Table
-----------------------
Domain          ESI Servers    Peer Controllers
------          -----------    ----------------
corp_domain     172.21.5.50    10.3.132.14
remote_domain   192.84.66.30

Total number of servers configured: 2
```

Related Commands

Platforms	Licensing	Command Mode
esi parser domain	This command configures an ESI syslog parser domain.	Config mode on Mobility Master
esi parser rule	This command creates or changes an ESI syslog parser rule.	Config mode on Mobility Master

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show esi ping

```
show esi ping [ping-name <ping-name>]
```

Description

Show settings for ESI ping health check attributes.

Syntax

Parameter	Description
`ping-name <ping-name>`	Include the optional **ping-name <ping-name>** parameters to display settings for one specified set of ping settings.

Example

This example below shows that the controller has three defined sets of ping attributes.

```
(host) #show esi groups

ESI Ping Table
--------------
Name        Frequency (sec)  Timeout (sec)  Retry Count  ID  Num Groups
----        ---------------  -------------  -----------  --  ----------
ping_att1                        5                2              2            0   1
ESIping                                  5                2              2            1   0
ESIping2                                 50000            2              2            2   2
```

The output of this command includes the following information:

Column	Description
`Name`	Name of a group of ping settings.
`frequency`	Specifies the ping frequency in seconds.
`timeout`	Specifies the ping timeout in seconds.
`retry-count`	Specifies the ping retry count
`ID`	ID number assigned to the ping attributes when that set of attributes was defined.
`Num Groups`	Number of ESI groups to which this set of ping attributes is assigned.

Related Commands

Platforms	Licensing	Command Mode
esi ping	This command specifies the ESI ping health check configuration.	Config mode on Mobility Master

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show esi servers

```
show esi servers [{group-name <groupname>|{server-name <server-name>}]
```

Description

Show configuration information for ESI servers.

Syntax

Parameter	Description
group-name <groupname>	Include this optional parameter to display information for all ESI servers assigned to a specific ESI group.
server-name <server-name>	Specify an ESI server name to view configuration information for just that server.

Usage Guidelines

By default, this command displays configuration settings for all ESI servers. You can include the name of an ESI group to view servers assigned to just that group, or specify a server name to view information for that server only.

Example

This example below displays configuration details for the ESI server name **forti_1**.

```
(host) #show esi servers server-name forti_1

ESI Server Table
----------------
Name     Trusted IP    Untrusted IP  Trusted Port Untrusted Port Group  Mode   NAT Port  ID
----     ----------    ------------  ------------ -------------- -----  ----   --------  --
forti_1  10.168.173.2  10.168.171.3  -/-/-          -/-/-        default route  0         4

Flags
-----
U

Flags:
  C :Datapath Download complete
  U :Server Up
  D :Server Down
  PT:Trusted Ping response outstanding
  PU:Untrusted Ping response outstanding
  HT:Health Check Trusted IP
  HU:Health Check Untrusted IP
  FT:Trusted Ping failed
  FU:Untrusted Ping failed
```

The output of this command includes the following information:

Column	Description
Name	Name of the ESI server.
Trusted IP	Displays the server IP address on the trusted network. As an option, you can also enable a health check on the specified address
Untrusted IP	Displays the server IP address on the untrusted network. As an option, you can also enable a health check on the specified address
Trusted Port	Shows the slot and port connected to the trusted side of the ESI server in the format <slot>/<module>/<port>.
Untrusted Port	Shows the slot and port connected to the untrusted side of the ESI server in the format <slot>/<module>/<port>.
Group	Name of the ESI group to which this server is assigned. If the server has not yet been assigned to a group, this column will be blank.
Mode	Specifies the ESI server mode of operation: bridge, nat, or route
Nat Port	Displays the NAT destination TCP or UDP port.
ID	ID number assigned to the server when it was first defined.
Flags	This data column displays any flags associated with this server. The flag key appears below the ESI Server Table.

Related Commands

Platforms	Licensing	Command Mode
esi server	This command configures an ESI server.	Config mode on Mobility Master

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices

show est profile

```
show est profile {default|<profile-name>}
```

Description

Displays the information of the activated EST profiles on the device.

Syntax

Parameter	Description
`<profile-name>`	Name of this instance of the profile.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command shows the default EST profile of a single managed device:

```
(host) [mynode] # show est profile default
EST Profile "default"
---------------------
Parameter              Value
---------              -----
Server Host            N/A
Server Port            443
Challenge password     N/A
Arbitrary label        N/A
Server's CA Cert Name  N/A
```

Command History

Version	Description
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show est status

```
show est status [all]
```

Description

Displays the information of the activated EST profiles along with the current status of the EST information on the device.

Syntax

Parameter	Description
`all`	Displays the activated EST profiles and the current status of the EST related information of the all switches.

Usage Guidelines

show est status—Use this command to view the current status of the EST related information on the device.

show est status all—Use this command to view the current status of the EST related information of all the switches.

Example

The output of this command shows the current EST status of a single managed device:

```
(host) [mynode] # show est status
EST STATUS
----------
Profile Name       : ssetty26_new
Server Host        : 10.20.21.26
Server Port        : 8443
Enrollment status  : Re-enrolled
Expiry status      : EXPIRING SOON
Valid from         : 2017-08-01 06:02:30
Valid till         : 2017-08-02 06:02:30
Re-enrollment due  : 2017-08-02 00:02:30
```

The output of this command shows the current EST status of all the switches:

```
(host) [mynode] # show est status all
EST Status for All Switches
---------------------------
IP Address    Name            Type     Version              Profile       Status      Expiry
time          Expiry status
----------    ----            ----     -------              -------       ------      --------
---           -------------
10.17.65.115  sree_sc_65_115  master   8.2.0.0-mm-dev_0000  ssetty26_new  REENROLLED  2017-08-
02 06:02:30  EXPIRING SOON
10.17.65.116  sree_vmc        MD       8.2.0.0-mm-dev_0000  ssetty26      REENROLLED  2017-08-
02 09:54:34  EXPIRING SOON
10.17.41.82   sree_41_82      MD       8.2.0.0-mm-dev_0000  ssetty26      REENROLLED  2017-08-
02 08:26:00  EXPIRING SOON
10.17.65.117  sree_65_117     standby  8.2.0.0-mm-dev_0000  ssetty26_new  REENROLLED  2017-08-
02 12:57:05  EXPIRING SOON
10.17.60.120  midhavmc60.120  MD       8.2.0.0-mm-dev_0000  N/A           N/A         N/A
           N/A
Total Switches:5
```

The output of this command includes the following information:

Column	Description
`IP Address`	IP address of the managed device.
`Name`	Name of the managed device or switch.
`Type`	Type of device
`Version`	Version of the ArubaOS software running on the device.
`Profile`	Denotes the EST profile configured on the device.
`Status`	The status of the EST profile
`Expiry Time`	Denotes the date and time of the expiry of the certificate enrollment.
`Expiry Status`	Denotes the current expiry status such as Certificate is Expiring Soon, Expired, or Not Expired.

Command History

Version	Description
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show fake-ade-cnt

```
show fake-ade-cnt
```

Description

Display the global and current fake ade counters

Syntax

None.

Example (TBD)

The following example shows the output of **show fake-ade-cnt**.

```
(host) [mynode] (config) #show fake-ade-cnt
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on Mobility Master8

show faults

```
show fault [history]
```

Description

Display a list of faults, which are any problematic conditions of the ArubaOS software or hardware.

Syntax

Parameter	Description
history	Include this parameter to display a history of faults cleared by the managed device or the operator.

Usage Guidelines

A managed device can maintain a list of up to 100 faults. Once 100 faults have been logged, any faults arising after that are dropped. The managed device maintains a history of the last 100 faults that have cleared. Every time a new fault clears clear, the oldest fault in the fault history is purged from the list.

Example

This example below shows all active faults the managed device, including the time the fault occurred, the fault ID number, and a description of the problem.

```
(host) [mynode] (config) #show faults

Active Faults
-------------
Time                 Number  Description
----                 ------  -----------
2009-03-02 18:13:08  93      Authentication Server vortex is down.
2009-03-02 18:13:08  94      Authentication Server vortex is down.
2009-03-02 18:13:08  95      Authentication Server vortex is down.
2009-03-02 18:13:08  96      Authentication Server vortex is down.
2009-03-02 18:13:08  97      Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  98      All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:08  99      Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  100     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:08  101     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  102     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:08  103     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  104     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:08  105     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:08  106     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:09  107     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  108     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:09  109     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  110     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:09  111     Authentication Server corp1-supersvr is down.
```

```
2009-03-02 18:13:09  112     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:09  113     Authentication Server corp1-supersvr is down.
2009-03-02 18:13:09  114     All authentication servers in server group sg-auth2 are brought
back in service.
2009-03-02 18:13:09  115     Authentication Server corp1-supersvr is down.
Total number of entries in the queue    :23
```

Related Commands

Command	Description	Mode
`clear fault <id>|all`	Manually clear a single fault by specifying the fault ID number, or clear all faults by including the **all** parameter.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on managed devices.

show file syncing profile

```
show file syncing profile
```

Description

This command displays the configuration the file syncing profile.

Syntax

None.

Usage Guidelines

Execute this command to view the file syncing profile.

Example

The following example shows the output of **show file syncing profile**.

```
(host) [mynode] (config) #show file syncing profile
File syncing profile
--------------------
Parameter      Value
---------      -----
File syncing   Enabled
sync time      30
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licenses	Command Mode
Available on all platforms	Available in the base operating system	Enable mode on Mobility Master

show fips

```
show fips
```

This command applies only to the FIPS version of ArubaOS.

Description

Displays FIPS mode of operation status as enabled or disabled.

Syntax

No parameters.

Example

The output of this command shows that the FIPS mode of operation is currently enabled.

```
(host) [mynode] (config) # show fips

FIPS Settings:
--------------
Mode  Enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master and managed devices

show firewall

```
show firewall [debug-route][dns-names]
```

Description

Display a list of global firewall policies and policy details.

Syntax

Parameter	Description
`debug-route`	Show global route debug settings, including the route protocol (IPv4/IPv6) and IP address.
dns-names	Display a list of DNS names and IP addresses used in firewall commands.

Examples

Include the optional **dns-names** parameter to list the DNS names used in firewall policies currently configured on the controller.

```
(host) [mynode] #show firewall dns-names
FW DNS names
------------
Name                       Id  InUse  List
----                       --  -----  ----
*.google.                  13  1      216.58.213.174 216.58.213.163 74.125.24.94 216.58.210.131
youtube.googleapis.com     9   1
m.youtube.com              7   1
accounts.google.com        1   1
www.youtube.com            6   1      64.233.167.91 64.233.167.93 64.233.167.190 216.58.198.110
graph.facebook.com         3   1
www.bing.com               12  1      204.79.197.200
www.youtube-nocookie.com   10  1
ssl.gstatic.com            2   1      216.58.213.163 216.58.198.99
youtubei.googleapis.com    8   1
www.googleapis.com         11  1      216.58.213.138 64.233.184.95
facebook.com               5   1
fbstatic-a.akamaihd.net    4   1
```

This example below shows all firewall policies currently configured on the controller.

```
(host) [mynode] (config) #show firewall
Global firewall policies
------------------------
Policy                                      Action          Rate       Port
------                                      ------          ----       ----
Enforce TCP handshake before allowing data  Disabled
Prohibit RST replay attack                  Disabled
Deny all IP fragments                       Disabled
Prohibit IP Spoofing                        Enabled
Monitor ping attack                         Disabled
Monitor TCP SYN attack                      Disabled
Monitor IP sessions attack                  Disabled
Deny inter user bridging                    Disabled
Log all received ICMP errors                Disabled
Per-packet logging                          Disabled
Blacklist Grat ARP attack client            Disabled
```

```
Allow tri-session with DNAT                 Disabled
Disable FTP server                          No
Blacklist ARP attack client                 Disabled
Monitor ARP attack                          Disabled
Monitor Gratuitous ARP attack               Enabled          50/sec
GRE call id processing                      Disabled
Session Idle Timeout                        Disabled
WMM content enforcement                     Disabled
Session VOIP Timeout                        Disabled
Only allow local subnets in user table      Disabled
Monitor/police CP attacks                   Disabled
Rate limit CP untrusted ucast traffic       Enabled           9765 pps
Rate limit CP untrusted mcast traffic       Enabled           1953 pps
Rate limit CP trusted ucast traffic         Enabled           65535 ps
Rate limit CP trusted mcast traffic         Enabled           1953 pps
Rate limit CP route traffic                 Enabled           976 pps
Rate limit CP session mirror traffic        Enabled           976 pps
Rate limit CP auth process traffic          Enabled           976 pps
Deny inter user traffic                     Disabled
Prohibit ARP Spoofing                       Disabled
Enforce bw contracts for broadcast traffic  Disabled
Multicast automatic shaping                 Disabled
Stall Detection                             Enabled
Enforce TCP Sequence numbers                Disabled
AMSDU Rx                                    Enabled
Jumbo Frames                                Disabled
Session-tunnel FIB                          Enabled
Prevent DHCP exhaustion                     Disabled
Deny source routing                         Disabled
Immediate Freeback                          Disabled
DPI Classification                          Enabled [Cfg: enabled, PEF license: installed]
Web Content Classification                  Enabled
Web Content Cache Miss Drop                 Disabled
Optimize Duplicate Address Detection frames Enabled
```

The output of this command includes the following information:

Parameter	Description
`Enforce TCP handshake before allowing data`	If enabled, this feature prevents data from passing between two clients until the three-way TCP handshake has been performed. This option should be disabled when you have mobile clients on the network as enabling this option will cause mobility to fail. You can enable this option if there are no mobile clients on the network.
`Prohibit RST replay attack`	If enabled, this setting closes a TCP connection in both directions if a TCP RST is received from either direction.
`Deny all IP Fragments`	If enabled, all IP fragments are dropped.
`Prohibit IP Spoofing`	When this option is enabled, source and destination IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.

Parameter	Description
Monitor ping attack	If enabled, the controller monitors the number of ICMP pings per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack.
Monitor TCP SYN attack	If enabled, the controller monitors the number of TCP SYN messages per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack.
Monitor IP sessions attack	If enabled, the controller monitors the number of TCP sessions requests per second. If this value exceeds the maximum configured rate, the controller will register a denial of service attack sessions.
Deny inter user bridging	If enabled this setting prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
Log all received ICMP errors	Shows if the controller will log received ICMP errors.
Per-packet logging	If active, and logging is enabled for the corresponding session rule, this feature logs every packet.
Blacklist Grat ARP attack client	If enabled, blacklist clients exceeding the Gratuitous ARP attack rate.
Allow tri-session with DNAT	Shows if the controller allows three-way session when performing destination NAT.
Disable FTP server	If active, this feature disables the FTP server on the controller.
Blacklist ARP attack client	If enabled, blacklist clients exceeding the ARP attack rate.
Monitor ARP attack	Shows the status of the ARP attack monitor.
Monitor Gratuitous ARP attack	Shows the status of the Gratuitous ARP attack monitor.
GRE call id processing	If active the controller creates a unique state for each PPTP tunnel.
Session Idle Timeout	Shows if a session idle timeout interval has been defined.
WMM content enforcement	If traffic to or from the user is inconsistent with the associated QoS policy for voice, this feature reclassifies traffic to best effort and data path counters are incremented.
Session VOIP Timeout	If enabled, a idle session timeout is defined for sessions that are marked as voice sessions.

Parameter	Description
Only allow local subnets in user table	If enabled, the controller only adds IP addresses which belong to a local subnet to the user table.
Monitor/police CP attacks	If enabled, the controller monitors a misbehaving user's inbound traffic rate. If this rate is exceeded, the controller can register a denial of service attack.
Rate limit CP untrusted ucast traffic	Shows the inbound traffic rate
Rate limit CP untrusted mcast traffic	Displays the untrusted multicast traffic rate limit.
Rate limit CP trusted ucast traffic	Displays the trusted unicast traffic rate limit.
Rate limit CP trusted mcast traffic	Displays the trusted multicast traffic rate limit.
Rate limit CP route traffic	Displays the traffic rate limit for traffic that needs generated ARP requests.
Rate limit CP session mirror traffic	Displays the traffic rate limit for session mirrored traffic forwarded to the controller.
Rate limit CP auth process traffic	Displays the traffic rate limit for traffic forwarded to the authentication process.
Deny inter user traffic	If enabled, this setting disables traffic between all untrused users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
Prohibit ARP Spoofing	When this option is enabled, possible arp spoofing attacks are logged and an SNMP trap is sent.
Enforce bw contracts for broadcast traffic	If enabled, bw contracts are applied ot local subnet broadcast traffic.
Multicast automatic shaping	If enabled, enables multicast optimization and provides excellent streaming quality regardless of the amount of VLANs or IP IGMP groups that are used.
Stall Detection	If enabled, triggers datapath crash on stall detection. Applies to the to 7200 Seriescontrollers only.
Enforce TCP Sequence numbers	If enabled, prevents data from passing between two clients until the three-way TCP handshake has been performed.
AMSDU Rx	AMSDU packets are dropped if this option is enabled.
Jumbo Frames	If enabled, supports up to 9216 bytes of payload on the controller.
Session-tunnel FIB	Enables session tunnel based forwarding.

Parameter	Description
`Prevent DHCP Exhaustion`	If enabled, this option checks for DHCP client hardware address against the packet source MAC address. This command checks the frame's source-MAC against the DHCPv4 client hardware address and drops the packet if it does not match. This feature prevents a client from submitting multiple DHCP requests with different hardware addresses, thereby preventing DHCP pool depletion.
`Deny Source Routing`	If enabled, forwarding of IP frames with source routing with the source routing options set is disallowed.
`Immediate Freeback`	If enabled, immediately frees buffers on 7200 Series controllers. Do not enable this option unless instructed to do so by a technical support representative.
`DPI Classification`	If enabled, performs deep packet inspection.
`Web Content Classification`	If enabled, allows web content classification for all HTTP traffic. Default: disabled
`Web Content Cache Miss Drop`	If enabled, allows the controller to drop any packets that do not match any web content category or reputation levels in the controller's internal web content cache. Default: disabled
`Optimize Duplicate Address Detection frames`	Reduce flooding of IPv4 Gratuitous ARPs/IPv6 Duplicate Address Detection frames onto wireless clients. Default: enabled

Related Commands

Command	Description
firewall	This command configures firewall options on the controller.
firewall cp	This command creates whitelist session ACLs
firewall cp-bandwidth-contract	This command configures bandwidth contract traffic rate limits to prevent denial of service attacks.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show firewall-cp

```
show firewall-cp [internal]
```

Description

Displays the Captive-Portal firewall policies on the controller.

Syntax

No Parameters

Example

The output of this command shows the CP firewall policies.

```
(host) [mynode] #show firewall-cp

CP firewall policies
--------------------
IP Version  Source IP    Source Mask  Protocol  Start Port  End Port  Permit/Deny  hits
contract
----------  ---------    -----------  --------  ----------  --------  -----------  ----  -----
---
ipv4        any                       6         21          21        Permit       0     test
ipv4        10.10.10.10  2.2.2.2      6         8           9         Permit       0
ipv4        2:2:2:2::2                1         1           2         Permit       0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show firewall-visibility

```
show firewall-visibility {debug|status}
```

Description

Displays the policy enforcement firewall visibility process state and status information.

Syntax

Parameter	Description
`debug`	Displays process state information for debugging firewall visibility.
`status`	Displays the status of firewall visibility as enabled or disabled.

Example

The output of this command shows the status of firewall visibility.

```
(host)[mynod] #show firewall-visibility status

enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	This command requires the PEFNG license	Config or Enable mode on Mobility Master.

show flush-r1-on-new-r0

```
ap·flush-r1-on-new-r0 {enable|disable}
```

Description

Use this command to view the status of flushing r1 keys on new r0.

Syntax

No parameters.

Example

The following example displays the status of flushing r1 keys on new r0:

```
(host) [mynode] (config) #show flush-r1-on-new-r0
Fast Roaming flush-r1-on-new-r0:enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Enable mode or Config mode

show gap-debug

```
show gap-debug
```

Description

Displays the troubleshooting information for the global AP database.

Usage Guidelines

Use this command to identify any issues with the global AP database. This command displays the troubleshooting information for the global AP database.

Example

The following is a sample output of this command:

```
(host) [mynode] (6000-202) #show gap-debug
GAP Master LMS Table
--------------------
IP            Master Cookie          Master Seq  LMS Cookie             LMS Seq  Activity
Status  Msg In Prog  Msg Len  Attempts  Last Reset Reason
--            -------------          ----------  ----------             -------  --------  ---
---  -----------  -------  --------  -----------------
172.20.1.101  172.20.1.102,521bbce7  0           0.0.0.0,00000000       0        --        up
    no           -        -         down notification
172.20.1.102  172.20.1.102,521ba3b1  0           0.0.0.0,00000000       0        --        up
    no           -        -         switched to backup
192.168.2.2   172.20.1.102,521ba5e6  0           192.168.2.2,521ba6fd   170      30        up
    no           -        -         down notification
192.168.3.2   172.20.1.102,521ba67e  0           192.168.3.2,521ba71b   172      34        up
    no           -        -         down notification
192.168.4.2   172.20.1.102,521ba6af  0           192.168.4.2,521ba724   163      58        up
    no           -        -         down notification
192.168.5.2   172.20.1.102,521ba6be  0           192.168.5.2,521ba794   169      19        up
    no           -        -         down notification
192.168.6.2   172.20.1.102,521ba694  0           192.168.6.2,521ba730   163      40        up
    no           -        -         down notification
192.168.7.2   172.20.1.102,521ba677  0           192.168.7.2,521ba6fd   170      29        up
    no           -        -         down notification
```

The output of this command includes the following information:

Parameter	Description
`IP`	The IP address of the managed device
`Master Cookie`	The cookie information on Mobility Master that is used to communicate with the LMS.
`Master Seq`	The sequence number used by Mobility Master to sync up with the LMS. This tracks the number of times Mobility Master has communicated with the LMS.
`LMS Cookies`	The cookie information on the LMS that is used to communicate with Mobility Master.
`LMS Seq`	The sequence number used by the LMS to sync up with Mobility Master.This tracks the number of times the LMS has communicated with Mobility Master.

Parameter	Description
`Activity`	The time at which the last activity happened on the LMS.
`Status`	Indicates if the status of the LMS is up or down.
`Msg in Prog`	Indicates if an active communication is happening between the LMS andMobility Master. It can be Yes or No. If it is yes, then the Msg Len and Attempt fields are set.
`Msg Len`	The length of the message that Mobility Master is syncing with the LMS.
`Attempts`	Number of times Mobility Master has attempted to sync with the LMS.
`Last Reset Reason`	Indicates the reason for last reset.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show gateway health-check

```
show gateway health-check
```

Description

Display the current status of the gateway health-check feature.

Syntax

No parameters.

Usage Guidelines

The gateway health check feature can only be enabled by Aruba Technical Support.

Example

This example below shows that the gateway health-check feature has not been enabled on the managed device.

```
(host) [mynode] (config) #show gateway health-check
Gateway health check not enabled
```

Related Commands

Command	Description	Mode
gateway health-check	Disable the gateway health check	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show global-user-table

```
show global-user-table count|list
```

Description

This command displays a count of global user based on the specified criteria or displays the list of users matching the given criteria.

Syntax

Parameter	Description
`count`	Show the number of users matching the given criteria
`current-switch`	Match IP address of the switch where the user is currently associated
`authentication-method`	Count users matching the specified authentication method
`role`	Count users matching the specified role
`bssid`	Count users matching the specified BSSID
`essid`	Count users matching the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
`ap-name`	Count users matching the specified AP name
`phy-type`	Count users matching the specified Phy type
`age`	Count users matching the specified age
`list`	Show users matching the given criteria
`ap-name`	Lists users matching the specified AP name
`authentication-method`	Lists the users matching the specified authentication method
`bssid`	Lists the users matching the specified BSSID
`current-switch`	Match IP address of the switch where the user is currently associated
`devtype`	Lists the users matching device type
`essid`	Lists the users matching the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
`ip`	Match IP address
`mac-addr`	Match MAC address
`name`	Match name
`not`	Show users that do not satisfy the given criteria
`or`	Show users that satisfy any of the given condition

Parameter	Description
`phy-type`	Match PHY type
`role`	Match role
`rows`	Show certain rows
`start`	Show user table starting from the specific row

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show gsm application

```
show gsm application <application_name> status
```

Description

Displays the status of the GSM application, for example, stm, auth, and so on.

Syntax

Parameter	Description
`application_name`	GSM application name like stm, auth, and so on

Example

The following is a sample output of this command:

```
(host) [mynode] (config) #show gsm application stm status
GSM Tick(500 us/tick, gsm_tick=2932440723368, gsm_ticktime=1466220361684074)
Application Histogram:stm

+------------------+-----------+-------------+-------------+-------------+-------------+
|          Histogram| GSM Thread|    GSM Thread|    GSM Thread|   Main Thread|   Main Thread|
|Time Range (in ms)| Cycle Time|API Mutex Wait|API Mutex Hold|API Mutex Wait|API Mutex Hold|
+------------------+-----------+-------------+-------------+-------------+-------------+
| 0.000 ..    0.500|         14|           14|           14|      2477350|      2477266|
| 0.500 ..    1.000|          0|            0|            0|            0|           25|
|   1.0 ..      2.0|          1|            0|            0|            0|           43|
|   2.0 ..      4.0|          0|            0|            0|            0|           14|
|   4.0 ..      8.0|          0|            0|            0|            0|            1|
|   8.0 ..     16.0|          0|            0|            0|            0|            1|
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show gsm channel-matrix

```
show gsm channel-matrix
```

Description

Displays the channels with Publisher and Subscriber Information.

Example

The following is a sample output of this command:

```
(host) [mynode] (config) #show gsm channel-matrix
GSM Channel Matrix
------------------
Channel              Publishers                    Subscribers
-------              ----------                    -----------



ap                                                  air_group arm dds ucm nbapi

bss                                                 auth air_group arm dds ucm


radio                                               air_group arm dds ucm nbapi


sta                                                 auth arm dds ucm nbapi_help


mac_user                                            auth air_group dds ucm nbapi_helper_proc
ip_user                                             auth air_group dds ucm nbapi_helper_proc
user                                                auth air_group dds ucm nbapi_helper_proc
wired_ap                                            dds
ag_user
dev_id_cache                                        arm dds nbapi_helper_proc
sectun              ha_mgr cfgm sc_replication_mgr  dds ipstm appRF
key_cache                                           air_group dds
pmk_cache
rep_key             ipstm ha_mgr sc_replication_mgr dds
port_info           fpapps                          dds
lldp_info           fpapps
lldp_chassis_info fpapps
dds_peer            dds                             auth ucm
ucc_client          ucm                             stm
ucc_session         ucm                             stm arm
vlan_info           fpapps                          air_group dds


Multi                   writer Is Replicated
helper_proc mcell       No
nbapi_helper_procmcell No
helper_proc mcell       Yes
er_proc     mcell       Yes
No                      No
No                      No
No                      No
No                      No
No                      No
No                      No
Yes                     No
```

No	No
No	No
Yes	No
No	No
No	No
No	No
No	No
No	No
No	No
Yes	No

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show gsm debug

```
show gsm debug
 channel
   ag_user
   ale_sta
   all
   amon_registration
   ap
   application_status
   blacklist
   bss
   bucket_map
   cac_usage
   cluster
   cluster_aac
   cluster_ap
   cluster_bss
   cluster_sta
   cluster_tunneled_node
   dds_peer
   dev_id_cache
   device_config
   device_lclist
   ha_info
   ip_probe
   ip_user
   ipsec_tunnel_info
   key_cache
   license_keys
   lldp_chassis_info
   lldp_info
   mac_user
   mip_proxy
   mip_tunnel
   named_vlan_info
   pmk_cache
   port_info
   radio
   rap_whitelist
   rep_key
   sectun
   service_ctrl_info
   sta
   sys_racl
   tunneled_node
   tunneled_user
   ucc_client
   ucc_session
   user
   v4_dhcp_pool
   vlan_info
   web_cc_info
   wired_ap
 rkey
   assignment
```

Description

This command displays status, event ring channel information, and trace events for channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on.

Syntax

Parameter	Description
Channel	Channel Name
ag_user	AirGroup User Channel
ale_sta	Analytics and Location Engine Data
all	All GSM Channels
amon_registration	AMON messages Registration Data
ap	AP Channel
application_status	Application Status Data
blacklist	Blacklist Channel
bss	BSS Channel
bucket_map	STA Hash Bucket to UAC map
cac_usage	Call Admission Control Usage Data
cluster	Controller Cluster Info
cluster_aac	Cluster AAC Assignment Data
cluster_ap	Cluster AP Data
cluster_bss	Cluster BSS Data
cluster_sta	Cluster STA Data
cluster_tunneled_node	Cluster Tunneled Node Channel.
dds_peer	DDS Peer Info
dev_id_cache	Device Id Cache Channel
device_config	Device Config
device_lclist	Device Lclist
ha_info	HA Info Channel
ip_probe	MIP Proxy Info
ip_user	IP User Channel
ipsec_tunnel_info	ipsec_tunnel_info Channel
key_cache	Key Cache Channel
license_keys	License Keys Channel
lldp_chassis_info	LLDP Chassis Info Channel

Parameter	Description
lldp_info	LLDP Info Channel
mac_user	Layer 2 MAC user Channel
mip_proxy	MIP Proxy Info
mip_tunnel	Mobileip tunnel control information.
named_vlan_info	Named vlans information.
pmk_cache	PMK Cache Channel
port_info	Port Info Channel
radio	Radio Channel
rap_whitelist	RAP Whitelist Channel
rep_key	Replication Key Channel
sectun	Secured Tunnel Channel
service_ctrl_info	Service Control Info
sta	STA Channel
sys_racl	sys_racl Data
tunneled_node	Tunneled Node Channel.
tunneled_user	Tunneled User Channel.
ucc_client	UCC Client Channel
ucc_session	UCC Session Channel
user	User Channel
v4_dhcp_pool	v4 DHCP Pool Info
vlan_info	VLAN Info Channel
web_cc_info	Web content classification Info Channel
wired_ap	Wired AP Channel
rkey	replication key
assignment	current Replication Key assignment

Example

You can use the following show command to check the status of the tunneled node:

```
(host) [mynode] #show gsm debug channel tunneled_node status
   GSM Channel status for Channel:TUNNELED_NODE
   CSM:: Key = 0X1BB7, Size = 357612 B
   DSM:: Base Key = 0X1BB8, Size = 524288 B Max number of segments = 1 Segments created = 1
   DSM:: In current segment: free_slots = 3040
```

```
Object Size = 165 B, Key Size = 6 B
Max number of Objects = 2048
Number of Allocated Objects = 0
Number of Objects in use = 0
Producers of TUNNELED_NODE channel are
tunneled_node_mgr
Subscribers of TUNNELED_NODE channel are ---
stm
cluster_mgr
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **sectun** parameter accepts IPv6 addresses.
ArubaOS 8.1.0.0	The **tunneled_node** and **tunneled_user** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show gsm lookup

```
show gsm lookup
 channel
   ag_user
   ale_sta
   amon_registration
   ap
   application_status
   blacklist
   bss
   bucket_map
   ccm_state
   cluster
   cluster_aac
   cluster_ap
   cluster_bss
   cluster_sta
   cluster_tunneled_node
   dds_peer
   dev_id_cache
   device_config
   device_lclist
   device_unprov
   ha_info
   ip_probe
   ip_user
   ipsec_tunnel_info
   key_cache
   license_keys
   lldp_chassis_info
   lldp_info
   mac_user
   mip_proxy
   mip_tunnel
   named_vlan_info
   ofa_port
   pmk_cache
   port_info
   radio
   rap_whitelist
   rep_key
   sectun
   service_ctrl_info
   split_tunnel
   sta
   sys_racl
   tunneled_node
   tunneled_user
   ucc_client
   ucc_session
   user
   vlan_info
   vrrp_info
   web_cc_info
   wired_ap
```

Description

This command displays status, event ring channel information, and trace events for specific channel and assignment related features like cluster, LLDP, tunneled nodes, UCC, and so on.

Syntax

Parameter	Description
Channel	Channel Name
ag_user	AirGroup User Channel
ale_sta	Analytics and Location Engine Data
amon_registration	AMON messages Registration Data
ap	AP Channel
application_status	Application Status Data
blacklist	Blacklist Channel
bss	BSS Channel
bucket_map	STA Hash Bucket to UAC map
ccm_state	Centralized Configuration Module state
cluster	Controller Cluster Info
cluster_aac	Cluster AAC Assignment Data
cluster_ap	Cluster AP Data
cluster_bss	Cluster BSS Data
cluster_sta	Cluster STA Data
cluster_tunneled_node	Cluster Tunneled Node Channel.
dds_peer	DDS Peer Info
dev_id_cache	Device Id Cache Channel
device_config	Device Config
device_lclist	Device LC list
device_unprov	Unprovisioned device
ha_info	HA Info Channel
ip_probe	MIP Proxy Info
ip_user	IP User Channel
ipsec_tunnel_info	ipsec_tunnel_info Channel
key_cache	Key Cache Channel
license_keys	License Keys Channel
lldp_chassis_info	LLDP Chassis Info Channel

Parameter	Description
lldp_info	LLDP Info Channel
mac_user	Layer 2 MAC user Channel
mip_proxy	MIP Proxy Info
mip_tunnel	Mobileip tunnel control information.
named_vlan_info	Named vlans information.
ofa_port	OpenFlow Port Channel
pmk_cache	PMK Cache Channel
port_info	Port Info Channel
radio	Radio Channel
rap_whitelist	RAP Whitelist Channel
rep_key	Replication Key Channel
sectun	Secured Tunnel Channel
service_ctrl_info	Service Control Info
split_tunnel	Split Tunnel
sta	STA Channel
sys_racl	sys_racl Data
tunneled_node	Tunneled Node Channel.
tunneled_user	Tunneled User Channel.
ucc_client	UCC Client Channel
ucc_session	UCC Session Channel
user	User Channel
vlan_info	VLAN Info Channel
vrrp_info	Virtual Router Redundancy Protocol Information
web_cc_info	Web content classification Info Channel
wired_ap	Wired AP Channel

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show guest-access-email

```
show guest-access-email
```

Description

This command shows a guest access email profile configuration. The guest access email process sends email to either the guest or the sponsor whenever a guest user account is created or when the Guest Provisioning user manually sends email from the GPP.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the current guest access email profile parameters. The Parameter and **Value** columns show the configured SMTP server and SMTP ports. that process guest email.

```
(host) [mynode] (config) #show guest-access-email

Guest-access Email Profile
--------------------------
Parameter    Value
---------    -----
SMTP Server  10.1.1.4
SMTP Port    25
```

Related Commands

Command	Description	Mode
guest-access-email	This command shows a guest access email profile configuration.	Enable or Config modes
local-userdb-guest add	This command creates a guest user in a local user database.	Enable or Config modes

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ha ap

```
show ha ap
   information {ip-addr <ip-addr>|ip6-addr <ip6-addr>}
   table
```

Description

This command displays information about APs using the HA feature.

Syntax

Parameter	Description
`information ip-addr <ip-addr> ip6-addr <ip6-addr>`	Issue this command under the supervision of Aruba support to troubleshoot the HA feature.
`table`	Display the HA AP table to view information about APs configured to use the HA feature.

Usage Guidelines

The HA features work across Layer-3 networks, so there is no need for a direct Layer-2 connection between in a high-availability group When the AP first connects to its active , the active provides the IP address of a standby , and the AP attempts to establish a tunnel to the standby to the standby . If an AP fails to connect to the first standby , the active will select a new standby for that AP, and the AP will attempt to connect to that standby .

An AP will failover to its backup if it fails to contact its active through regular heartbeats and keepalive messages, or if the user manually triggers a failover using the WebUI or CLI.

Examples

The following command displays the HA table for the HA group **default**.

```
(host) [mynode] (config) #show ha ap table
HA AP Table
-----------
AP          IP-Address   MAC-Address        AP-flags  HA-flags
--          ----------   -----------        --------  --------
ard         10.3.31.245  6c:f3:7f:c6:72:c0  LU
arr         10.3.31.222  d8:c7:c8:c0:02:7c  LU
kalap105-2  10.3.31.253  00:24:6c:c0:22:6b  LU        S
Total Num APs::3
Active APs::2
Standby APs::1
AP Flags: R=RAP; S=Standby; s=Bridge Split VAP L=Licensed; M=Mesh, U=Up
HA Flags: S=Standby, C=Standby connected, L=LMS, F=Sent Failover Request to AP,
H=AP flagged for Inter Controller Heartbeat
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Enable mode on Mobility Master

show ha group

```
show ha
   group-membership
   group-profile [<profile>]}
```

Description

This command displays HA profile settings and shows the HA group to which the managed device is currently assigned.

Syntax

Parameter	Description
`group-membership <profile>`	Name of the HA group to which the managed device should be a member.
`group-profile [<profile>]`	Display a list of all HA groups, or include the optional <profile> parameter to display configuration settings for the specified profile.

Usage Guidelines

The HA feature supports redundancy models with an active managed device pair, or an active or standby deployment model with one backup managed device supporting one or more active managed device. Each of these clusters of active and backup managed device comprises a HA group. Note that all active and backup managed device within a single HA group must be deployed in a single Mobility Master - managed device topology. The HA feature works across Layer-3 networks, so there is no need for a direct Layer-2 connection between managed device in a HA group.

Examples

The following command shows that the managed device from which the command was issued is a member of the HA group ha-group2.

```
(host) [mynode] (config) #show ha-group-member
Member of HA group :ha-group2
```

The example below shows that the managed device has two configured HA group profiles. The **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
HA group information List
-------------------------
Name      Profile Status
----      --------------
default
new
Total:2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Enable mode on Mobility Master

show ha heartbeat counters

```
show ha heartbeat counters
```

Description

This command displays statistics for the HA extended managed device capacity feature.

Syntax

No parameters.

Usage Guidelines

The HA inter-managed device heartbeat feature allows for faster AP failover from an active managed device to a standby managed device, especially in situations where the active managed device reboots or loses connectivity to the network.

The inter-managed device heartbeat feature works independently from the AP mechanism that sends heartbeats from the AP to the managed device. If enabled, the inter-managed device heartbeat feature supersedes the AP's heartbeat to its managed device. As a result, if a standby managed device detects missed inter-managed device heartbeats from the active managed device, it triggers its standby APs to failover to the standby managed device, *even if those APs have not detected any missed heartbeats between the APs and their active managed device*. Use this feature with caution in deployments where the active and standby managed device are separated over high-latency WAN links.

When this feature is enabled, the standby managed device starts sending regular heartbeats to an AP's active managed device as soon as the AP has an UP status on the standby managed device. By default, the standby managed device sends heartbeat messages every 100ms. If the active managed device becomes unreachable for the number of heartbeats defined by the heartbeat threshold (by default, 5 missed heartbeats), the standby managed device immediately detects this error, and informs the APs using the standby managed device to fail over from the active managed device to the standby managed device .

This feature is disabled by default. It can be used in conjunction with the HA state synchronization feature only in topologies that use a single active and standby managed device, or a pair dual-mode active managed device that act as standby managed device for each other. HA inter-managed device heartbeats can be enabled and configured in the HA group profile using the WebUI or CLI.

Examples

The following command displays HA heartbeat statistics for the HA group **default**.

```
(host) [mynode] (HA group information "default") #show ha heartbeat counters

Heartbeat stats
---------------
Controller IP  Active Reference Count    Total Heartbeat Sent   Total Heartbeat Received
-------------  ----------------------    --------------------   ------------------------
172.14.0.2     1                         101                    101

Last Missed Heartbeat (Count) Time
----------------------------------
0
```

The output of this command includes the following parameters:

Parameter	Description
`IP`	IP address of the managed device from which this command was issued.
`Active Reference Count`	Number of APs that are using that standby managed device as their active managed device.
`Total HeartBeat Sent`	Total number of heartbeats sent by the managed device.
`Total Heartbeat REceived`	Total number of heartbeats received by the managed device.
`Last Missed Heartbeat (count) time`	Timestamp showing when the last heartbeat sent was not received, as well as the number of heartbeats that failed to be sent.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Enable mode on Mobility Master

show ha oversubscription statistics

```
show ha oversubscription statistics
```

Description

This command displays statistics for the HA extended managed device capacity feature

Syntax

No parameters.

Usage Guidelines

A managed device acting as a standby managed device can oversubscribe to standby APs by up to four times that managed device's rated AP capacity, as long as the tunnels consumed the standby APs do not exceed the maximum tunnel capacity for that standby managed device.

Feature Requirements

All managed device using this feature must be deployed in a master-local topology where centralized licensing is enabled on the active and standby managed device. If centralized licensing is disabled, the standby AP oversubscription feature are disabled also. Standby managed device oversubscription and the HA state synchronization features are mutually incompatible cannot be be enabled simultaneously. If your deployment uses the state synchronization feature, you must disable it before you enable standby managed device oversubscription.

Standby managed device Capacity

The following table describes the AP oversubscription capacity maximum supported tunnels and for managed device that support this feature.

Controller Model	Standby AP Capacity	Maximum Tunnels Supported
7210	4x rated AP capacity	16384 tunnels
7220	4x rated AP capacity	32768 tunnels
7240	4x rated AP capacity	65536 tunnels

To determine the number of standby tunnels consumed by APs on each active managed device, multiply the number of APs on the active managed device by the number of BSSIDs per AP. As an example, consider a deployment with four active 7210 managed device that each have 512 APs with 8 BSSIDs. The APs on each active managed device consume (512 * 8) tunnels, for a combined total of 16,384 tunnels. A single 7210 managed device using the standby managed device oversubscription feature can act as the standby managed device for all four active managed device in this example, because this topology is within the 4x rated AP capacity limit and maximum tunnel limit for the a 7210 managed device model.

If the network administrator later changed all the APs in this deployment to support 10 BSSIDs, each active managed device would use (512 * 10) tunnels, for a combined total of 20,480 tunnels on the four active managed device. The tunnels required by the APs on the active managed device would then exceed the maximum tunnel limit for the standby managed device, so the standby managed device can no longer support all APs on the active managed device.

AP Failover

If a standby managed device reaches its AP oversubscription capacity or exceeds its maximum BSSID limit, the standby managed device drops any subsequent standby AP connections. A dropped AP attempts to reconnect to the standby managed device, but after it exceeds the maximum number of request retries, the AP informs the active managed device that it is unable to connect to the standby managed device. The active managed device then prompts the AP to create a standby tunnel to another standby managed device, if one is configured.

If an active managed device fails, the APs on the active managed device fail over to the standby managed device. Once the standby managed device has reached its capacity for active APs,it terminates tunnels to any standby APs that controller can no longer serve. When these APs detect that there is no longer a heartbeat between the AP and the standby managed device, they notify their active managed device that they can no longer connect to the standby. The active managed device then prompts the APs to establish standby tunnels to another standby managed device, if one is configured.

Examples

The following command displays oversubscription statistics for APs and tunnels

```
(host) [mynode] (config) #show ha oversubscription statistics
Platform oversubscription factor :          4
APs Limits
------------------
APs                      Number
----                     ------
Platform Limit           512
Current Active           2
Current Standby          694
Active remaining         0
Standby remaining        1
Maximum allowed Standby  697

BSS Limits
--------------------
Tunnels                Limits
-------                ------
Maximum BSS tunnels    16384
Average BSS/AP         23
BSS tunnels in use     16360
BSS tunnels available  24
```

The output of this command includes the following parameters:

Parameter	Description
`Platform limit`	Maximum number of APs supported by the managed device platform.
`Current Active`	Number of active APs currently associated to the managed device.
`Current Standby`	Number of APs that are currently using the managed device as a standby managed device.
`Active Remaining`	Number of APs that can connect to this managed device in Active mode.
`Standby Remaining`	Number of APs that can connect to this managed device in Standby mode.
`Maximum allowed Standby`	Maximum number of Standby APs supported by the managed device.

Parameter	Description
`Maximum BSS tunnels`	The maximum number of BSS tunnels supported by the managed device.
`Average BSS/AP`	The average number of BSS tunnels per AP using the managed device as a standby managed device.
`BSS tunnels in use`	Number of BSS tunnels currently in use by the managed device.
`BSS tunnels available`	Number of BSS tunnels not currently in use by the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Enable mode on Mobility Master

show hash statistics

```
Show hash statistics
   aaa
   ads
   authmgr
   certmgr
   cfgm
   cpsec
   cts
   dbsync
   dhcp
   esi
   fpapps
   httpd
   ike
   l2tp
   licensemgr
   mobileip
   mon_serv
   ntp
   ospf
   pim
   pktfilter
   pptp
   profmgr
   publisher
   resolver
   sapm
   snmp
   stm
   stm-lopri
   syslogd
   userdb
   wms
```

Description

Displays the

Syntax

Parameter	Description
`aaa`	Administrator Authentication
`ads`	Anomaly Detection
`authmgr`	User Authentication
`certmgr`	Certificate Manager
`cfgm`	Config Manager
`cpsec`	Control-Plane Security Manager
`cts`	Transport Service
`dbsync`	Database Synchronization

Parameter	Description
dhcp	DHCP Server
esi	Server Load Balancing
fpapps	Layer 2,3 control
httpd	HTTPD
ike	IKE Daemon
l2tp	L2TP
licensemgr	License Manager
mobileip	Mobile IP
mon_serv	Mon Server
ntp	NTP Daemon
ospf	OSPF
pim	Protocol Independent Multicast
pktfilter	Packet Filter
pptp	PPTP
profmgr	Profile Manager
publisher	Publish subscribe service
resolver	Resolver
sapm	SAPM
snmp	SNMP agent
stm	Station Management
stm-lopri	Station Management Low Priority
syslogd	Syslog Manager
userdb	User Database Server
wms	Wireless Management

Example

This example shows the NTP Daemon statistics

```
(host) [mynode] (config) #show hash statistics app-name ntp
Received response from application
Hash Statistics
Size    Nodes Max-Coll Owner
23        0        0
23      266        0
23      272        0
```

```
23          272           0
23          272           0
997           0           0
23            4           0
23            0           0
23            0           0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters	Enable mode of Mobility Master and managed device

show hostname

```
show hostname
```

Description

Show the hostname of the Mobility Master and managed device.

Syntax

No parameters.

Example

The output of this command shows the hostname configured for the controller. A hostname can contain alphanumeric characters, spaces, punctuation, and symbol characters.

```
(host) [MyNode] # show hostname

hostname is SampleHost
```

Related Commands

Configure the Mobility Master's hostname using the command hostname.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available on Mobility Master and managed device.

show iap detailed-table

```
show iap detailed-table
   branch-key <brkey>
   long
```

Description

Displays the details of all the branches terminating at the managed device.

Syntax

Parameter	Description
`branch-key <brkey>`	Key for the branch, which is unique to each branch.
`long`	Displays the branches connected to the managed device in detailed view.

Example

This example shows the details of the branches connected to the controller:

```
(host) [mynode] (config) #show iap detailed-table long

Name              VC MAC Address     Status   Inner IP   Key
----              --------------     ------   --------   ------------------------------------
Instant-C0:8C:08 d8:c7:c8:c4:73:53  UP       1.1.1.1    2d15576901190269568c3d9837fc1b414e1b06
                                                         523282805aaa
Instant-C0:8C:08 d8:c7:c8:c4:73:53  UP       1.1.1.1    2d15576901190269568c3d9837fc1b414e1b06
                                                         523282805aaa
Instant-C0:8C:08 d8:c7:c8:c4:73:53  UP       1.1.1.1    2d15576901190269568c3d9837fc1b414e1b06
                                                         523282805aaa

Flags    Branch (Subnet / Vlan)    BID    IP Address Range      Client Count
-----    ----------------------    ---    ----------------      ------------
PD2      52                        0      52.1.1.2-52.1.1.100   5
PD3      53.1.1.8/29               0      53.1.1.1-53.1.1.100   5
PC2      51                        0

Flags: P = Primary Tunnel; B = Backup Tunnel; C = Centralized; U = Unassigned;
       D = Distributed; L = Local; 3 = Routed(L3); 2 = Bridged(L2);
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the branch
`VC MAC Address`	MAC address of the Virtual managed device of the branch
`Status`	Current status of the branch (UP or DOWN)
`Inner IP`	Internal VPN IP of the branch
`Key`	Key for the branch, which is unique to each branch

Parameter	Description
Flags	This column displays any flags for the branch subnet ■ P = Primary Tunnel ■ B = Backup Tunnel ■ C = Centralized ■ D = Distributed ■ L = Local ■ U = Unassigned ■ 3 = Routed(L3) ■ 2 = Bridged(L2)
`Branch (Subnet/Vlan)`	Subnet mask or VLAN assigned to the branch
`BID`	Branch ID
IP Address Range	Allocated branch subnet IP address range
`Client Count`	Number of client terminating on this managed device

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters	Enable or Configuration mode on managed devices

show iap subnet

```
show iap subnet <subnet-name>
```

Description

Displays the details of specific IAP subnet information.

Syntax

Parameter	Description
`subnet <subnet-name>`	Displays specific subnet information for an IAP.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following command displays a subnet details:

```
(host) [mynode] (config) #show iap subnet test
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters	Enable or Configuration mode on managed devices

show iap table

```
show iap table
   branch-key <brkey>
   long
   summary
```

Description

Displays the branch details connected to the managed device.

Syntax

Parameter	Description
`branch-key <brkey>`	Key for the branch, which is unique to each branch.
`long`	Displays the branches connected to the managed device in detailed view.
`summary`	Displays the summary of the IAP table.

Example

This example shows the details of the branches connected to the managed device:

```
(host) [mynode] (config) #show iap table long

IAP Branch Table
----------------
Name              VC MAC Address     Status   Inner IP       Assigned Subnet  Assigned Vlan
----              --------------     ------   --------       ---------------  -------------
Tokyo-CB:D3:16    6c:f3:7f:cc:42:f8  DOWN     0.0.0.0
Paris-CB:D3:16    6c:f3:7f:cc:3d:04  UP       10.15.207.140  10.15.206.99/29  2
LA                6c:f3:7f:cc:42:25  UP       10.15.207.111  10.15.206.24/29  2
Munich            d8:c7:c8:cb:d3:16  DOWN     0.0.0.0
London-c0:e1      6c:f3:7f:c0:e1:b1  UP       10.15.207.120  10.15.206.64/29  2
Instant-CB:D3     6c:f3:7f:cc:42:1e  DOWN     0.0.0.0
Delhi             6c:f3:7f:cc:42:ca  DOWN     0.0.0.0
Singapore         6c:f3:7f:cc:42:cb  UP       10.15.207.122  10.15.206.120/29 2


Key         Bid(Subnet Name)
---         ----------------
b3c65c...
b3c65c...
b3c65c...   2(10.15.205.0-10.15.205.250,5),1(10.15.206.1-10.15.206.252,5)
a2a65c...   0
b3c65c...   7(10.15.205.0-10.15.205.250,5),8(10.15.206.1-10.15.206.252,5)
b3c65c...
b3c65c...   1(10.15.205.0-10.15.205.250,5),2(10.15.206.1-10.15.206.252,5)
b3c65c...   14(10.15.205.0-10.15.205.250,5),15(10.15.206.1-10.15.206.252,5)
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the branch.

Parameter	Description
`VC MAC Address`	MAC address of the Virtual managed device of the branch.
`Status`	Current status of the branch (UP or DOWN).
`Inner IP`	Internal VPN IP of the branch.
`Assigned Subnet`	Subnet mask assigned to the branch.
`Assigned Vlan`	VLAN ID assigned to the branch.
`Key`	Key for the branch, which is unique to each branch.
`Bid(Subnet Name)`	Branch ID (BID) of the subnet. ■ In the example above, the managed device displays bid-per-subnet-per-branch i.e., for "LA" branch, BID "2" for the ip-range "10.15.205.0-10.15.205.250" with client count per branch "5"). If a branch has multiple subnets, it can have multiple BIDs. ■ Branches that are in **UP** state and do not have a **Bid(Subnet Name)** means that the IAP is connected to a managed device which did not assign any bid for any subnet. In the above example, "Paris-CB:D3:16" branch is **UP** and does not have a **Bid(Subnet Name)** information. This means that either the IAP is connected to a backup managed device or connected to a primary managed device without any distributed L2 or L3 subnets. For more information on bid-per-subnet-per-branch and distributed L2 and L3 subnets, see the *DHCP Configuration* chapter of the Aruba *Instant Access Point 6.2.1.0-3.3 User Guide*.

Related Commands

Command	Description
iap del branch-key	This command removes a branch from the managed device based on the branch key.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters	Enable or Configuration mode on managed devices

show iap trusted-branch-db

```
show iap trusted-branch-db
```

Description

Displays the details of IAP trusted branch database information.

Syntax

None

Example

This example shows the details of IAP trusted branch database information:

```
(host) [mynode] (config) #show iap trusted-branch-db

Trusted Branch Validation: Enabled
IAP Trusted Branch Table
------------------------
Branch MAC
----------
01:01:0e:3e:4c:33
```

Another example:

```
(host) #show iap trusted-branch-db

Trusted Branch Validation: Disabled
IAP Trusted Branch Table
------------------------
Branch MAC
----------
(allow all as trusted branch)
```

The output of this command includes the following parameters:

Parameter	Description
`Branch MAC`	MAC address of the trusted IAP branch

Related Commands

Command	Description
iap trusted-branch-db	This command configures an IAP-VPN branch as trusted

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system, except for noted parameters	Enable or Configuration mode on managed devices

show ids ap-classification-rule

```
id-classification-rule <rule-name>
```

Description

Display the IDS AP classification rule profile.

Syntax

Parameter	Description
`<rule-name>`	Enter the AP classification rule profile name.

Usage Guidelines

Issue this command without the **<rule-name>**option to view the AP Classification Rule Profile list. Add the rule name option to display values for the rule.

Example

Below is the show command *without* the rule name option:

```
(host) [mynode] (config) #show ids ap-classification-rule
IDS AP Classification Rule Profile List
---------------------------------------
Name               References  Profile Status
----               ----------  --------------
exclude-ssid-rule  1
rule1              1
rule2              1
Total:3
```

In the example above, the **Reference** column indicates the number of references to the rule named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined. Optionally, you can enter a rule name to view the parameters for that rule. For example:

```
(host) (config) # show ids ap-classification-rule rule1
IDS AP Classification Rule Profile "rule1"
------------------------------------------
Parameter                    Value
---------                    -----
SSID                         Aruba-ap
Match SSIDs                  true
Min SNR value                0
Max SNR value                255
Discovered APs count         2
Check for Min Discovered APs  true
Classify To AP Type          suspected-rogue
Confidence level increase    5
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master.

show ids ap-rule-matching

Description

Display the IDS active AP rules profile.

Example

```
(host) [mynode] (config) #show ids ap-rule-matching

IDS Active AP Rules Profile
---------------------------
Parameter     Value
---------     -----
AP Rule name  snr0
AP Rule name  rule1
AP Rule name  rule2
AP Rule name  exclude-ssid-rule
```

In the above example, the rule names in the *Value* column have been activated by the **ids ap-rule-matching** command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config or Enable mode on Mobility Master

show ids dos-profile

```
show ids dos-profile <profile-name>
```

Description

Show an IDS DoS Profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS DoS profile.

Usage Guidelines

Issue this command without the **<profile-name>**parameter to display an IDS DoS profile.

Examples

The example below shows that the controller has four configured DoS profiles.

```
(host) [mynode] (config) #show ids dos-profile

IDS Denial Of Service Profile List
----------------------------------
Name           References  Profile Status
----           ----------  --------------
default        4
test           0
test1          1
Wizard-test    1
Wizard-test2   1

Total:5
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The example below displays a partial output for the profile “test1”.

```
(host) (config) #show ids dos-profile test1
Parameter                                       Value
---------                                       -----
Detect Disconnect Station Attack                true
Disconnect STA Assoc Response Theshold          5
Disconnect STA Deauth and Disassoc Theshold     8
Disconnect STA Detection Quiet Time             900 sec
Spoofed Deauth Blacklist                        Disabled
Detect AP Flood Attack                          false
AP Flood Threshold                              50
AP Flood Increase Time                          3 sec
AP Flood Detection Quiet Time                   900 sec
Detect Client Flood Attack                      false
Client Flood Threshold                          150
Client Flood Increase Time                      3 sec
Client Flood Detection Quiet Time               900 sec
Detect EAP Rate Anomaly                         false
EAP Rate Threshold                              60
```

```
EAP Rate Time Interval                          3 sec
EAP Rate Quiet Time                             900 sec
Detect CTS Rate Anomaly                         false
CTS Rate Threshold                              5000
CTS Rate Time Interval                          5 sec
CTS Rate Quiet Time                             900 sec
Detect RTS Rate Anomaly                         false
RTS Rate Threshold                              5000
RTS Rate Time Interval                          5 sec
RTS Rate Quiet Time                             900 sec
Detect Rate Anomalies                           false
Rate Thresholds for Assoc Frames                default
Rate Thresholds for Disassoc Frames             default
Rate Thresholds for Deauth Frames               default
...
```

For a detailed explanation of the output shown above, see the ids dos-profile command.

Related Commands

Configure IDS DoS profiles using the command ids dos-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids general-profile

```
show ids general-profile <profile-name>
```

Description

Display an IDS General profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS General profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the IDS General profile list. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has four configured General profiles.

```
(host) [mynode] (config) # show ids general-profile
IDS General Profile List
------------------------
Name           References  Profile Status
----           ----------  --------------
default        2
helen          0
wired-lb       1
Wizard-test2   1
Total:4
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The example below displays the settings for the profile **Michael**.

```
(host) (config) #show ids general-profile Michael

IDS General Profile "Michael"
-----------------------------
Parameter                                 Value
---------                                 -----
Adhoc AP Max Unseen Timeout               180 sec
Adhoc (IBSS) AP Inactivity Timeout        5 sec
AP Inactivity Timeout                     20 sec
AP Max Unseen Timeout                     600 sec
Frame Types for RSSI calculation          ba pr dlow dnull mgmt ctrl
IDS Event Generation on AP                none
Max Monitored Stations                    1024
Max Unassociated Stations                 256
Min Potential AP Beacon Rate              25 %
Min Potential AP Monitor Time             2 sec
Mobility Manager RTLS                     false
Monitored Device Stats Update Interval    0 sec
Packet SNR Threshold                      0
Send Adhoc Info to Controller             true
```

```
Signature Quiet Time                        900 sec
STA Inactivity Timeout                      60 sec
STA Max Unseen Timeout                      600 sec
Stats Update Interval                       60 sec
Wired Containment                           true
Wired Containment of AP's Adj MACs          true
Wired Containment of Suspected L3 Rogue     false
Wireless Containment                        deauth-only
Debug Wireless Containment                  false
WMS Client Monitoring                       all
```

The output of this command includes the following parameters:

Parameter	Description
Adhoc AP Max Unseen Timeout	Ageout time in seconds since ad hoc (IBSS) AP was last seen.
Adhoc (IBSS) AP Inactivity Timeout	Ad hoc (IBSS) AP inactivity timeout in number of scans.
AP Inactivity Timeout	Time, in seconds, after which an AP is aged out.
AP Max Unseen Timeout	Ageout time, in seconds, since AP was last seen.
Frame Types for RSSI calculation	Frame types used in AM RSSI calculation.
IDS Event Generation on AP	Enable or disable IDS event generation from the AP. Event generation from the AP can be enabled for syslogs, traps, or both. This does not affect generation of IDS correlated events on the switch.
Max Monitored Stations	Maximum number of monitored stations.
Max Unassociated Stations	Maximum number of unassociated stations.
Min Potential AP Beacon Rate	Minimum beacon rate acceptable from a potential AP, in percentage of the advertised beacon interval.
Min Potential AP Monitor Time	Minimum time, in seconds, a potential AP has to be up before it is classified as a real AP.
Mobility Manager RTLS	Shows if RTLS communication with the configured mobility-manager is enabled or disabled.
Monitored Device Stats Update Interval	Time interval, in seconds, for AP to update the switch with stats for monitored devices. Minimum is 60.
Packet SNR Threshold	The packet Signal to Noise Ratio (SNR) threshold. All packets with SNR below this threshold is dropped from IDS and ARM processing. No packets are dropped if the threshold is set to 0.
Send Adhoc Info to Controller	Enable or disable sending ad hoc information to the managed device from the AP.
Signature Quiet Time	After a signature match is detected, the time to wait, in seconds, to resume checking.
STA Inactivity Timeout	Time, in seconds, after which a station is aged out.

Parameter	Description
`STA Max Unseen Timeout`	Time, in seconds, after which an AP is aged out.
`Stats Update Interval`	Interval, in seconds, for the AP to update the managed device with statistics. This setting takes effect only if the Aruba Mobility Manager is configured. Otherwise, statistics update to the managed device is disabled.
`Wired Containment`	Shows if the profile has enabled or disabled containment from the wired side.
`Wired Containment of AP's Adj MACs`	Shows if the profile has enabled or disabled wired containment of MACs offset by one from APs BSSID.
`Wired Containment of Suspected L3 Rogue`	Shows if the profile has enabled or disabled the feature to identify and contain an AP with a preset wired MAC address that is completely different from the AP's BSSID. where the MAC address that the AP provides to wireless clients as a 'gateway MAC' is offset by one character from its wired MAC address.
`Wireless Containment`	Shows if the profile has enabled or disabled containment from the wireless side.
`Debug Wireless Containment`	Shows if the profile has enabled or disable debugging of containment from the wireless side.
`Wired Containment of AP's Adj MACs`	Enable or disable wired containment of MACs offset by one from APs BSSID.

Related Commands

Configure IDS General profiles using the command ids general-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids impersonation-profile

```
show ids impersonation-profile <profile-name>
```

Description

Display an IDS Impersonation Profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS Impersonation profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the IDS Impersonation profile list. Include a profile name to display detailed configuration information for that profile.

Examples

The example below displays that the Mobility Master has five configured Impersonation profiles.

```
(host) [mynode] (config) #show ids impersonation-profile

IDS Impersonation Profile List
------------------------------
Name           References  Profile Status
----           ----------  --------------
default        4
test           0
test1          1
Wizard-test    1
Wizard-test2   1

Total:5
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

The example below displays the configuration settings for the profile **test1**.

```
(host) (config) #show ids impersonation-profile test1

IDS Impersonation Profile "test1"
---------------------------------
Parameter                                 Value
---------                                 -----
Detect AP Impersonation                   false
Protect from AP Impersonation             false
Beacon Diff Threshold                     50 %
Beacon Increase Wait Time                 3 sec
Detect AP Spoofing                        true
Detect Beacon Wrong Channel               false
Beacon Wrong Channel Detection Quiet Time 900 sec
Detect Hotspotter Attack                  true
Hotspotter Quiet Time                     900 sec
```

The output of this command includes the following parameters:

Parameter	Description
`Detect AP Impersonation`	Shows of the profile has enabled or disabled detection of AP impersonation.
`Protect from AP Impersonation`	Shows if AP impersonation is enabled or disabled for the profile. When AP impersonation is detected, both the legitimate and impersonating AP are disabled using a DoS attack.
`Beacon Diff Threshold`	Percentage increase in beacon rates that triggers an AP impersonation event.
`Beacon Increase Wait Time`	Time, in seconds, after the beacon difference threshold is crossed before an AP impersonation event is generated.
`Detect AP Spoofing`	AP Spoofing detection is enabled
`Detect Beacon Wrong Channel`	Disable detection of beacons advertising the incorrect channel
`Beacon Wrong Channel Detection Quiet Time`	Wait 90 seconds after detecting a beacon with the wrong channel after which the check can be resumed.
`Detect Hotspotter Attack`	Enable detection of the Hotspotter attack to lure away valid clients.
`Hotspotter Quiet Time`	Wait 90 seconds after detecting an attempt to Use the Hotspotter tool against clients.

Related Commands

Configure IDS impersonation profiles using the command ids impersonation-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids management-profile

Description

Displays the management event correlation for IDS event traps and sylogs (logs).

Example

The following example displays the current management status.

```
(host) [mynode] (config) #show ids management-profile

IDS Management Profile
----------------------
Parameter                     Value
---------                     -----
IDS Event Correlation         logs-and-traps
Event Correlation Quiet Time  900 sec
```

The display output of the above command includes:

Parameter	Description
`IDS Event Correlation`	Management profile is set for logs-and-traps.
`Event Correlation Quiet Time`	The time to wait, 900 seconds, before the event can be raised again.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids profile

```
show ids profile <profile-name>
```

Description

Display all ids profiles or display a specific profile name.

Syntax

Parameter	Description
<profile-name>	Name of an IDS profile.

Usage Guidelines

Issue this command without the **<profile-name>**parameter to display the list of IDS profiles. Include a profile name to display detailed information for that profile.

Examples

The example below shows that the controller has seven configured IDS Profiles.

```
(host) [mynode] (config) #show ids profile

IDS Profile List
----------------
Name            References  Profile Status
----            ----------  --------------
default         5
test            0
test-tarpit     1
test-wired-lb   0
test1           0
Wizard-test     0
Wizard-test2    0

Total:7
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

This example displays the configuration settings for the profile **test1**.

```
(host) [mynode] (config) #show ids profile test1

IDS Profile "test1"
-------------------
Parameter                       Value
---------                       -----
IDS General profile             test1
IDS Signature Matching profile  test1
IDS DOS profile                 test1
IDS Impersonation profile       test1
IDS Unauthorized Device profile test1
```

The output of this command includes the following parameters:

Parameter	Description
`IDS General profile`	Name of a IDS General profile to be applied to an AP or AP group.
`IDS Signature Matching profile`	Name of a IDS Signature Matching profile to be applied to an AP or AP group.
`IDS DOS profile`	Name of a IDS DoS profile to be applied to an AP or AP group.
`IDS Impersonation profile`	Name of a IDS Impersonation profile to be applied to an AP or AP group.
`IDS Unauthorized Device profile`	Name of a IDS Unauthorized Device profile to be applied to an AP or AP group.

Related Commands

Configure the IDS profile using the command ids profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master.

show ids rap wml server profile

```
show ids rap-wml-server-profile <server-name>
```

Description

Show an IDS Rate Thresholds profile.

Syntax

Parameter	Description
`<server-name>`	Name of an IDS Remote AP WML server profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the IDS Rate Threshold profile list. Include a profile name to display detailed configuration information for that profile.

Related Commands

Configure the IDS Rate Threshold profile using the command

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids rap wml table profile

```
show ids rap-wml-table-profile <table-name>
```

Description

Show an IDS Rate Thresholds profile.

Syntax

Parameter	Description
`<table-name>`	Name of an IDS RAP WML Table profile.

Examples (TBD)

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids rate-thresholds-profile

```
show ids rate-thresholds-profile <profile-name>
```

Description

Show an IDS Rate Thresholds profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS Rate Threshold profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the IDS Rate Threshold profile list. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured IDS Rate Threshold profiles.

```
(host) [mynode] (config) #show ids rate-thresholds-profile

IDS Rate Thresholds Profile List
--------------------------------
Name                               References  Profile Status
----                               ----------  --------------
default                            20
probe-request-response-thresholds  10          Predefined
test                               0

Total:3
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

This example displays the configuration settings for the profile **test**.\

```
(host) [mynode] (config) #show ids rate-thresholds-profile test

IDS Rate Thresholds Profile "test"
----------------------------------
Parameter              Value
---------              -----
Channel Increase Time  15 sec
Channel Quiet Time     900 sec
Channel Threshold      300
Node Time Interval     15 sec
Node Quiet Time        900 sec
Node Threshold         200
```

The output of this command includes the following parameters:.

Parameter	Description
`Channel Increase Time`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
`Channel Quiet Time`	The time that must elapse after a channel rate alarm before another identical alarm may be triggered. This option prevents excessive messages in the log file.
`Channel Threshold`	Number of a specific type of frame that must be exceeded within a specific interval in an entire channel to trigger an alarm.
`Node Time Interval`	Time, in seconds, in which the threshold must be exceeded in order to trigger an alarm.
`Node Quiet Time`	The time that must elapse after a node rate alarm before another identical alarm may be triggered. This option prevents excessive messages in the log file.
`Node Threshold`	Number of a specific type of frame that must be exceeded within a specific interval for a particular client MAC address to trigger an alarm.

Related Commands

Configure the IDS Rate Threshold profile using the command ids rate-thresholds-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids signature-matching-profile

```
show ids signature-matching-profile <profile-name>
```

Description

Show an IDS Signature Matching profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an IDS Signature Matching profile.

Usage Guidelines

Issue this command without the **<profile-name>**parameter to display the entire IDS Signature Matching profile list. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the Mobility Master has four configured Signature Matching profiles.

```
(host) [mynode] (config) #show ids signature-matching-profile

IDS Signature Matching Profile List
-----------------------------------
Name           References  Profile Status
----           ----------  --------------
default        4
test1          1
Wizard-test    1
Wizard-test2   1

Total:4
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

This example displays the configuration settings for the profile **test1**.

```
(host) [mynode] (config) #show ids signature-matching-profile test1

IDS Signature Matching Profile "test1"
--------------------------------------
Parameter      Value
---------      -----
IDS Signature  Deauth-Broadcast
IDS Signature  Disassoc-Broadcast
```

The output of this command includes the following parameters:

Parameter	Value
`IDS Signature`	Broadcast is not authorized
`IDS Signature`	Disassociate broadcast

Related Commands

Configure the Signature Matching profile using the command ids signature-matching-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master.

show ids signature-profile

```
show ids signature-profile <profile-name>
```

Description

Show an IDS signature profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS Signature profile.

Usage Guidelines

Issue this command without the **<profile>**parameter to display the entire IDS Signature profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has eight configured Signature profiles.

```
(host) [mynode] (config) #show ids signature-profile

IDS Signature Profile List
--------------------------
Name                        References  Profile Status
----                        ----------  --------------
AirJack                     1           Predefined
ASLEAP                      1           Predefined
Deauth-Broadcast            1           Predefined
default                     1
Netstumbler Generic         1           Predefined
Netstumbler Version 3.3.0x  1           Predefined
Null-Probe-Response         1           Predefined
sample                      0

Total:8
```

This example displays the configuration settings for the profile **AirJack**.

```
(host) [mynode] (config) # show ids signature-profile
IDS Signature Profile "AirJack" (predefined)
--------------------------------------------
Parameter   Value
---------   -----
Frame Type  beacon SSID = AirJack
```

The output of this command includes the following parameters:

Parameter	Description
`Frame Type`	Type of 802.11 frame. For each type of frame, further parameters may be included to filter and detect only the required frames. ■ **assoc**: Association frame type. ■ **auth**: Authentication frame type. ■ **beacon**: Beacon frame type. ■ **control**: All control frames. ■ **data**: All data frames. ■ **deauth**: Deauthentication frame type. ■ **disassoc**: Disassociation frame type. ■ **mgmt**: Management frame type. ■ **probe-reques**t: Probe request frame type. ■ **probe-response:** Probe response frame type. ■ **ssid**: For beacon, probe-request, and probe-response frame types, the SSID as either a string or hex pattern. ■ **ssid-length**: For beacon, probe-request, and probe-response frame types, the length, in bytes, of the SSID.
`payload`	Pattern at a fixed offset in the payload of an 802.11 frame.
`sequence number`	Sequence number of the frame.
`src- mac`	Source MAC address in the 802.11 frame header.
`dst- mac`	Source MAC address in the 802.11 frame header.
`bssid`	BSSID field in the 802.11 frame header.

Related Commands

Configure the Signature profile using the command ids signature-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Enable and Config mode on Mobility Master

show ids unauthorized-device-profile

```
show ids unauthorized-device-profile <profile-name>
```

Description

Show an IDS Unauthorized Device Profile.

Syntax

Parameter	Description
<profile-name>	Name of an IDS Unauthorized Device profile

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the IDS Unauthorized Device profile list. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the Mobility Master has five configured Unauthorized Device profiles.

```
(host) [mynode] (config) #show ids unauthorized-device-profile

IDS Unauthorized Device Profile List
------------------------------------
Name           References  Profile Status
----           ----------  --------------
default        4
test           0
test1          1
Wizard-test    1
Wizard-test2   1

Total:5
```

In the example above, the **Reference** column indicates the number of references to the profile named in the **Name** column. The **Profile Status** column is blank unless the rule is predefined.

This example displays the configuration settings for the profile **test1**.

```
(host) [mynode] (config) #show ids unauthorized-device-profile test1

IDS Unauthorized Device Profile "test1"
IDS Unauthorized Device Profile "default"
----------------------------------------
Parameter                                       Value
---------                                       -----
Protect 802.11n High Throughput Devices         false
Protect 40MHz 802.11n High Throughput Devices   false
Detect Active 802.11n Greenfield Mode           false
Detect Adhoc Networks                           false
Protect from Adhoc Networks                     false
Protect from Adhoc Networks - Enhanced          false
Detect Adhoc Network Using Valid SSID           true
Adhoc Network Using Valid SSID Quiet Time       900 sec
Allow Well Known MAC                            N/A
Detect Devices with an Invalid MAC OUI          false
MAC OUI detection Quiet Time                    900 sec
```

```
Detect Misconfigured AP                                 false
Protect Misconfigured AP                                false
Detect Bad WEP                                          false
Privacy                                                 false
Require WPA                                             false
Valid 802.11g channel for policy enforcement            N/A
Valid 802.11a channel for policy enforcement            N/A
Valid and Protected SSIDs                               N/A
Valid MAC OUIs                                          N/A
Rogue AP Classification                                 true
Overlay Rogue AP Classification                         true
OUI-based Rogue AP Classification                       true
Propagated Wired MAC based Rogue AP Classification      true
Rogue Containment                                       false
Suspected Rogue Containment                             false
Suspected Rogue Containment Confidence Level            60
Detect Station Association To Rogue AP                  true
Detect Unencrypted Valid Clients                        true
Unencrypted Valid Client Detection Quiet Time           900 sec
Detect Valid Client Misassociation                      true
Detect Valid SSID Misuse                                false
Protect SSID                                            false
Protect Valid Stations                                  false
Valid Wired MACs                                        N/A
Detect Windows Bridge                                   true
Protect Windows Bridge                                  false
Detect Wireless Bridge                                  false
Wireless Bridge detection Quiet Time                    900 sec
Detect Wireless Hosted Network                          true
Wireless Hosted Network Quiet Time                      900 sec
Protect From Wireless Hosted Networks                   false
```

The output of this command includes the following parameters:

Parameter	Description
`Protect 802.11n High Throughput Devices`	Shows if the profile enables or disables protection of HT (802.11n) devices.
`Protect 40MHz 802.11n High Throughput Devices`	Shows if the profile enables or disables protection of HT (802.11n) devices operating in 40 MHz mode.
`Detect Active 802.11n Greenfield Mode`	Shows if the profile enables or disables detection of HT devices advertising greenfield preamble capability.
`Detect AdHoc Networks`	Shows if the profile has enabled or disabled detection of ad hoc networks.
`Protect from Adhoc Networks`	Shows if the profile has enabled or disabled protection from WPA or WPA2 ad hoc networks.
`Protect from Adhoc Networks-Enhanced`	Shows if the profile has enabled or disabled protection from WEP or Open ad hoc networks.
`Detect Valid SSID Misuse`	Shows if the detect valid SSID minuse is enabled (true) or disabled (false).

Parameter	Description
Adhoc Network Using Valid SSID Quiet Time	Shows time to wait, in seconds, after detecting an ad hoc network using a valid SSID, after which the check can be resumed.
Allow Well Known MAC	Shows if the profile allows devices with known MAC addresses to classify rogue APs.
Detect Devices with an Invalid MAC OUI	Shows if the profile has enabled or disabled checking of the first three bytes of a MAC address, known as the OUI, assigned by the IEEE to known manufacturers.
MAC OUI detection Quiet Time	Time, in seconds, that must elapse after an invalid MAC OUI alarm has been triggered before another identical alarm may be triggered.
Detect Misconfigured AP	Shows if the profile has enabled or disabled detection of misconfigured APs.
Protect Misconfigured AP	Shows if the profile has enabled or disabled protection of misconfigured APs.
Detect Bad WEP	Shows if the profile has enabled or disabled detection of WEP initialization vectors that are known to be weak or repeating.
Privacy	Shows if the profile has enabled or disabled encryption as a valid AP configuration.
Require WPA	Shows if the Mobility Master will flag any valid AP not using WPA as a misconfigured AP.
Valid 802.11g channel for policy enforcement	A list of valid 802.1b or 802.1g channels that third-party APs are allowed to use.
Valid 802.11a channel for policy enforcement	A list of valid 802.11a channels that third-party APs are allowed to use.
Valid and Protected SSIDs	A list of valid and protected SSIDs.
Valid MAC OUIs	A list of valid MAC OUIs.
Rogue AP Classification	Shows if the profile has enabled or disabled rogue AP classification.
Overlay Rogue AP Classification	Shows if the Mobility Master allows APs that are plugged into the wired side of the network to be classified as “suspected rogue” instead of “rogue”.
OUI-based Rogue AP Classification	Shows if OUI-based rogue AP classification is enabled or disabled.

Parameter	Description
Propagated Wired MAC based Rogue AP Classification	Shows if rogue AP classification through propagated wired MACs is enabled or disabled.
Rogue Containment	Shows if the Mobility Master will automatically shut down rogue APs.
Suspected Rogue Containment	Shows if the Mobility Master will automatically treat suspected rogue APs as interfering APs.
Suspected Rogue Containment Confidence Level	Confidence level of suspected Rogue AP to trigger containment, expressed as a percentage.
Detect Station Association To Rogue AP	Shows if the profile has been configured to detect station association to a rogue AP.
Detect Unencrypted Valid Clients	Shows if the profile has enabled or disabled detection of unencrypted valid clients.
Unencrypted Valid Client Detection Quiet Time	Shows the time to wait, in seconds, after detecting an unencrypted valid client after which the check can be resumed.
Detect Valid Client Misassociation	Shows if the profile has enabled or disabled detection of a misassociation between a valid client and an unsafe AP.
Detect Valid SSID Misuse	Shows if the profile has enabled or disabled detection of Interfering or Neighbor APs using valid or protected SSIDs.
Protect SSID	Shows if the profile has enabled or disabled use of SSID by valid APs only.
Protect Valid Stations	Shows if the Mobility Master will allow valid stations to connect to a non-valid AP.
Valid Wired MACs	List of valid and protected SSIDs.
Detect Windows Bridge	Shows if the profile has enabled or disabled detection of Windows station bridging.
Protect Windows Bridge	Shows if the profile has enabled or disabled protection of Windows station bridging.
Detect Wireless Bridge	Shows if the profile has enabled or disabled detection of wireless bridging.
Wireless Bridge detection Quiet Time	Time, in seconds, that must elapse after a wireless bridge alarm has been triggered before another identical alarm may be triggered.

Parameter	Description
`Protect From Wireless Hosted Networks`	Shows if the profile has enabled or disabled detection of a wireless hosted network.
`Wireless Hosted Network Quiet Time`	The wireless hosted network detection feature sends a log message and trap when a wireless hosted network is detected. The quiet time displayed in this field displays the amount of time, in seconds, that must elapse after a wireless hosted network log message or trap has been triggered before an identical log message or trap can be sent again.
`Protect From Wireless Hosted Networks`	Shows if the profile has enabled or disabled containment on a wireless hosted network by launching a DoS attack to disrupt associations between a Windows 7 software-enabled Access Point (softAP) and a client, and disrupt associations between the client that is hosting the softAP and any access point to which the host connects.

Related Commands

Configure the Unauthorized Device profile using the command ids unauthorized-device-profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced

Command Information

Platforms	License	Command Mode
Available on all platforms	Requires the RFprotect license	Config mode on Mobility Master

show ids wms-general-profile

```
show ids wms-general-profile
```

Description

Display general statistics for the wms configuration.

Syntax

No parameters.

Example

```
This example shows per-channel statistics for all monitored APs.

(host) [mynode] (config) #show ids wms-general-profile

IDS WMS General Profile
-----------------------
Parameter                                   Value
---------                                   -----
AP poll interval                            60000 msec
AP poll retries                             3
AP ageout interval                          0 minutes
Adhoc AP ageout interval                    31 minutes
Station ageout interval                     100 minutes
Statistics update                           true
Persistent Neighbor APs                     true
Persistent Valid STAs                       false
AP learning                                 false
Propagate Wired Macs                        true
Collect Stats for Monitored APs and Clients false
Learn System Wired Macs                     false
```

Column	Description
AP poll interval	Interval, in milliseconds, for communication between the controller and AMs. The controller contacts the AM at this interval to download AP to station associations, update policy configuration changes, and download AP and station statistics.
AP poll retries	Maximum number of failed polling attempts before the polled AM is considered to be down.
AP ageout interval	Time, in minutes, that an AP must remain unseen by any probes before it is deleted from the database.
Adhoc AP ageout interval	Time, in minutes, that an ad hoc (IBSS) AP remains unseen before it is deleted (ageout) from the database.
Station ageout interval	Time, in minutes, that an client must unseen by any probes before it is deleted from the database.

Column	Description
`Statistics update`	Shows the status of the statistics updates in the database.
`Persistent Neighbor APs`	Shows the status of known AP neighbors.
`Persistent Valid STAs`	Shows the status of known AP neighbors.
`AP learning`	Shows the status of “learning” of non-Aruba APs.
`Propagate Wired Macs`	Shows if the controller has enabled or disabled the propagation of the gateway wired MACs.
`Collect Stats for Monitored APs and Clients`	Shows if the master controller will collect up to 25,000 statistic entries for monitored APs and clients.
`Learn System Wired Macs`	Shows the status of “learning” of wired MACs at the controller.

The output of this command includes the following information:

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show ids wms-local-system-profile

```
ids wms-local-system-profile
   max-ap-threshold <max-ap-threshold>
```

Description

Display statistics for the WMS local system profile settings.

Syntax

No Parameters

Usage Guidelines

The configuration parameters in IDS WMS local system profile enables local termination of the WMS service, sets maximum thresholds for the maximum number of managed APs and stations, and defines the intervals at which valid AP, rogue AP and station data is sent to the managed device. Issue this command to view the local WMS service profile settings .

Example

The following commands first set the interval time for repopulating the MAC table to 10 minutes and then sets the maximimum number of APs to 100.

```
(host) (config) #show ids wms-local-system-profile
   IDS WMS Local System Profile
   ----------------------------
   Parameter                          Value        Set
   ---------                          -----        ---
   Max AP Threshold                   100
   Max STA Threshold                  0
   Max RBTree Entries                 3
   Max System Wired MACs              1000
   Override Service Termination       false
   Periodic AP Snapshot Interval      180 minutes
   Periodic Rogue AP Snapshot Interval  30 minutes
   Periodic STA Snapshot Interval     180 minutes
   System Wired MAC Update Interval   8
```

The output of this command includes the following information:

Table 10: *IDS WMS Local System Profile Settings*

Parameter	Description
Max AP Threshold	The max threshold for the total number of APs
Max STA Threshold	The max threshold for the total number of stations.
Max RBTree Entries	The max threshold for the total number of AP and station RBTree entries.
Max System Wired MACs	The max number of system wired MAC table entries learned by the managed device.
Override Service Termination	If enabled, this feature overrides the system-determined termination mode, and terminates WMS service at the managed device to which the AP is associated.

Parameter	Description
Periodic AP Snapshot Interval	The interval in minutes at which to generate a periodic snapshot of monitored APs. The (AMON) messages comprising the snapshot will be spread over this interval.
Periodic Rogue AP Snapshot Interval	The interval in minutes at which to generate a periodic snapshot of monitored Rogue APs. The (AMON) messages comprising the snapshot will be spread over this interval.
Periodic STA Snapshot Interval	The interval in minutes at which to generate a periodic snapshot of monitored clients. The (AMON) messages comprising the snapshot will be spread over this interval.
System Wired MAC Update Interval	The interval, in minutes, for repopulating the system wired MAC table at the managed device.

Related Commands

Release	Modification
mgmt-server	Configures the management server profile.
ids management-profile	Manage the events correlation for IDS event traps and syslogs (logs).
ids wms-local-system-profile	This command configures the WMS service to terminate on individual managed devices instead of Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show ifmap

```
show ifmap
   cppm
   state cppm
   statistics cppm
```

Descriptions

Issue this command to show the ClearPass Policy Manager IF-MAP configuration profile and the IP-MAP connection state.

Syntax

Parameter	Description
`cppm`	Shows the ClearPass Policy Manager IF-MAP profile parameters and their values.
`state cppm`	Shows the ClearPass Policy Manager IF-MAP connection state including if it is enabled, and the servers and their state.
`statistics cppm`	Shows the statistics data.

Example

To configure this feature using the CLI:

```
(host) [mynode] (config) #ifmap
(host) [mynode] (config) #ifmap cppm
(host) [mynode] (CPPM IF-MAP Profile) #server host <host>
(host) [mynode] (CPPM IF-MAP Profile) #port <port>
(host) [mynode] (CPPM IF-MAP Profile) #passwd <psswd>
(host) [mynode] (CPPM IF-MAP Profile) #enable
```

This show command show if the CCPM interface is enable and the ClearPass Policy Manager server IP address, username and password.

```
(host)[mynode] (CPPM IF-MAP Profile) #show ifmap cppm
CPPM IF-MAP Profile
-------------------
Parameter              Value
---------              -----
CPPM IF-MAP Interface  Enabled
CPPM IF-MAP Server     10.10.10.10:443 admin/********
```

This show command shows if state of all enabled ClearPass Policy Manager servers.

```
(host)[mynode] (CPPM IF-MAP Profile) #show ifmap state cppm
CPPM IF-MAP Connection State [Interface: Enabled]
-------------------------------------------------
Server           State
------           -----
10.4.191.32:443  UP
```

Related Commands

Command	Description	Mode
ifmap	This command is used in conjunction with ClearPass Policy Manager. It sends HTTP User Agent Strings and mDNS broadcast information to ClearPass so that it can make more accurate decisions about what types of devices are connecting to the network	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode

show image version

```
show image version
type
```

Description

Display the current system image version on both partition 0 and 1.

Syntax

Parameter	Description
`type`	Displays the System image type.

Example

The following example shows that the managed device is running ArubaOS 8.0 and booting off partition 0:1.

```
(host)[mynode] #show image version
---------------------------------
Partition               : 0:0 (/mnt/disk1)
Software Version        : ArubaOS 8.0.0.0-svcs-ctrl (Digitally Signed - Developer/Internal
Build)
Build number            : 0000
Label                   : ssetty@ss_sc_new-ENG.0000
Built on                : Wed Jun 8 14:46:22 IST 2016
---------------------------------
Partition               : 0:1 (/mnt/disk2) **Default boot**
Software Version        : ArubaOS 8.0.0.0-svcs-ctrl (Digitally Signed - Developer/Internal
Build)
Build number            : 0000
Label                   : ssetty@ss_sc_new-ENG.0000
Built on                : Thu Jun 16 12:53:57 IST 2016
```

The output of this command includes the following parameters:

Parameter	Description
`Partition`	Partition number and name. The default boot partition will display a **Default boot** notice by the partition name.
`Software Version`	Version of ArubaOS software running on the partition.
`Build number`	Build number for the software version.
`Label`	The label parameter can display additional information for the build. By default, this value is the software build number.
`Built on`	Date the software build was created.

Following is an example of **show image version type** command:

```
(host) [mynode] #show image version type

This image is development build
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show interface cellular access-group

```
show interface cellular access-group
```

Description

List the access groups configured on the cellular interface.

Example

```
(host) [mynode] #show interface cellular access-group

 Cell Interface:
 session access list 3 is configured
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show interface counters

```
show interface counters
```

Description

Displays a table of L2 interfaces counters.

Syntax

No parameters

Example

The example below shows the output of the **show interface counters** command.

```
(host) [mynode] #show interface counters
Port            InOctets         InUcastPkts       InMcastPkts     InBcastPkts
GE0/0/0         87071474           45349             590754          112566
Port            OutOctets        OutUcastPkts      OutMcastPkts    OutBcastPkts
GE0/0/0         10646801           18727             581               2
```

The output of this command includes the following parameters:

Parameter	Description
`Port`	Port number.
`InOctets`	Number of octets received through the port.
`InUcastPkts`	Number of unicast packets received through the port.
`InMcastPkts`	Number of multicast packets received through the port.
`InBcastPkts`	Number of broadcast packets received through the port.
`OutOctets`	Number of octets sent through the port.
`OutUcastPkts`	Number of unicast packets sent through the port.
`OutMcastPkts`	Number of multicast packets sent through the port.
`OutBcastPkts`	Number of broadcast packets sent through the port.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show interface gigabitethernet

```
show interface gigabitethernet <slot/module/port>
```

Description

Displays information about a specified Gigabit Ethernet port.

Syntax

Parameter	Description
`access-group`	Displays the Access Groups configured on this interface.
`counters`	Displays L2 interface counters for the specified interface.
`switchport`	Displays L2 interface information.
`transceiver`	Displays the transceiver serial ID information.
`trusted-vlan`	Displays port member vlan trusted status.
`untrusted-vlan`	Displays port member vlan untrusted status.
`xsec`	Displays xsec configuration.

Examples

The example below shows the output of **show interface gigabitethernet 0/0/0**.

```
(host)[mynode] (config) #show interface gigabitethernet 0/0/0
GE 0/0/0 is up, line protocol is up
Hardware is 10 Gigabit Ethernet, address is 00:0C:29:37:AB:82 (bia 00:0C:29:37:AB:82)
Description: GE0/0/0
Encapsulation ARPA, loopback not set
speed (10 Gbps)
MTU 1500 bytes, BW is 10000 Mbit
Last clearing of "show interface" counters 5 day 4 hr 57 min 41 sec
link status last changed 5 day 4 hr 55 min 22 sec
1560452 packets input, 498781462 bytes
Received 240098 broadcasts, 0 runts, 0 giants, 0 throttles
0 input error bytes, 0 CRC, 0 frame
240098 multicast, 1320354 unicast
1149614 packets output, 158075706 bytes
0 output errors bytes, 0 deferred
0 collisions, 0 late collisions, 0 throttles
This port is TRUSTED
```

The output of this command includes the following parameters:

Parameter	Description
`GE 0/0/0 is...`	Displays the status of the specified port.

Parameter	Description
line protocol is...	Displays the status of the line protocol on the specified port.
Hardware is....	Describes the hardware interface type.
address is...	Displays the MAC address of the hardware interface.
Description	The port type, name, and connector type.
Encapsulation	Encapsulation method assigned to this port.
loopback...	Displays whether or not loopback is set.
Configured	Configured transfer operation and speed.
Jumbo support...	Jumbo frame support is enabled.
Negotiated	Negotiated transfer operation and speed.
MTU bytes	MTU size of the specified port in bytes.
BW is...	Bandwidth of the link.
Last clearing of "show interface counters"	Time since "show interface counters" was cleared.
link status last changed...	Time since "show interface counters" was cleared. Below the time, all current counters related to the specified port are listed.
This port is...	Whether or not this port is trusted.
POE status of the port is...	The POE status of the specified port.
BW-Contract List/ Application Exception List/ Application BW-Contract list	Information about the bandwidth contract applied to the interface. For details, see interface gigabitethernet.

```
(host)[mynode] (config) #show interface gigabitethernet 0/0/0 counters

Port            InOctets          InUcastPkts      InMcastPkts      InBcastPkts
GE0/0/0         498972448         1321416          240316                0
Port            OutOctets         OutUcastPkts     OutMcastPkts     OutBcastPkts
GE0/0/0         158234051         1150823               0                0
```

The output of this command includes the following parameters:

Parameter	Description
Port	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.

Parameter	Description
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

```
(host)[mynode] (config)#show interface gigabitethernet 0/0/0 switchport

Name:  GE0/0/0
Switchport:  Enabled
Administrative mode:  static access
Operational mode:  static access
Administrative Trunking Encapsulation:  dot1q
Operational Trunking Encapsulation:  dot1q
Access Mode VLAN: 1 (Default)
Trunking Native Mode VLAN: 1 (Default)
Trunking Vlans Enabled: NONE
Trunking Vlans Active: NONE
```

The output of this command includes the following parameters:

Parameter	Description
Name	Port name.
Switchport	Whether or not switchport is enabled.
Administrative mode	Administrative mode .
Operational mode	Operational mode.
Administrative Trunking Encapsulation	Encapsulation method used for administrative trunking.
Operational Trunking Encapsulation	Encapsulation method used for operational trunking.
Access Mode VLAN	The access mode VLAN for the specified port.
Trunking Native Mode VLAN	The trunking native mode VLAN for the specified port.
Trunking Vlans Enabled	Number of trunking VLANs currently enabled.
Trunking Vlans Active	Number of trunking VLANs currently active.

```
(host) [mynode] (config)#show interface gigabitethernet 0/0/0 untrusted-vlan

Name:  GE1/0
Untrusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the specified port.
`Untrusted Vlan(s)`	List of untrusted VLANs.

```
(host) [mynode] (config)# show interface gigabitethernet 0/0/1 xsec
xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
`xsec vlan 7 is ACTIVE`	This states that xsec is active on the specified port as well as the associated VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show interface loopback

```
show interface loopback
```

Description

Displays information about the loopback IP interface.

Syntax

No parameters

Example

The example below shows the output of the **show interface loopback** command.

```
(host) [mynode] #show interface loopback

loopback interface is up line protocol is up
Hardware is Ethernet, address is 00:0C:29:37:AB:81
IPv6 link-local address is fe80::c:290f:ff37:ab81/64
```

The output of this command includes the following parameters:

Parameter	Description
`loopback interface is...`	Status of the loopback interface.
`line protocol is...`	Status of the line protocol on the specified port.
`Hardware is...`	Hardware interface type.
`address is...`	MAC address of the loopback interface.
`IPv6 link-local address`	IP address and subnet mask of the loopback interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show interface mgmt

```
show interface mgmt
```

Description

Displays information about management Ethernet IP interfaces.

Syntax

No parameters

Example

The example below shows the output of show interface mgmt:

```
(host) [mynode] (config)# show interface mgmt

  mgmt is up line protocol is up
  Hardware is Ethernet, address is 00:0C:29:37:AB:77
```

The output of this command includes the following parameters:

Parameter	Description
`mgmt is...`	Status of the mgmt interface.
`line protocol is...`	Status of the line protocol on the specified port.
`Hardware is...`	Describes the hardware interface type.
`address is...`	Interface's MAC address.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show interface port-channel

```
show interface port-channel <id>
   access-group
   counters
   switchport
   trusted-vlan
   untusted-vlan
   xsec
      xsec point-to-point
```

Description

Displays information about a specified port-channel interface.

Syntax

Parameter	Description
`access-group`	Displays access groups configured on this interface.
`counters`	Displays L2 interface counters for the specified interface.
`switchport`	Displays L2 interface information for the specified interface.
`trusted-vlan`	Displays port member vlan trusted status.
`untrusted-vlan`	Displays port member vlan untrusted status.
`xsec`	Displays xsec configuration.
`xsec point-to-point`	Displays the point-to-point xsec tunnels for the specified interface.

Example

The example below shows the output of **show interface port-channel 7** on a managed device.

```
(host) [mynode] (config) #show interface port-channel 7
   Port-Channel 7 is administratively up, Link is up, Line protocol is down
   Hardware is Port-Channel, address is 00:0C:29:37:AB:81 (bia 00:0C:29:37:AB:81)
   Description: Link Aggregate
   Spanning Tree is Discarding
   Switchport priority: 0
   Member port(s):
   Speed :0 Mbps
   Interface index: 8200
   MTU: 1500 bytes
   Last clearing of "show interface" counters 0 day 8 hr 48 min 3 sec
   link status last changed 0 day 8 hr 48 min 3 sec
   0 packets input, 0 bytes
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input error bytes, 0 CRC, 0 frame
   0 multicast, 0 unicast
   0 packets output, 0 bytes
   0 output errors bytes, 0 deferred
   0 collisions, 0 late collisions, 0 throttles
   Port-Channel 7 is NOT TRUSTED
```

The output of this command includes the following parameters:

Parameter	Description
Port-Channel 7 is...	Status of the specified port.
line protocol is...	Status of the line protocol on the specified port.
Hardware is....	Hardware interface type.
address is...	MAC address of the hardware interface.
Description	The port type, name, and connector type. If the LAG is created by LACP, it is indicated as shown in the display output above. If the LAG is created by LACP, you can not statically add or delete any ports under that port channel. All other commands are allowed. If LACP is not shown, then the LAG is created by static configuration.
Spanning Tree is...	Spanning tree status on the specified port-channel.
VLAN membership	Number of VLANs the specified port-channel is associated with.
Switchport priority	Switchport priority of the specified port-channel.
Jumbo Support is...	Displays the status of jumbo frame on a port channel.
Last clearing of "show interface counters"	Time since "show interface counters" was cleared. Below the time, all current counters related to the specified port are listed.
Port-channel 7 is...	Whether or not this port-channel is trusted.

```
#show interface port-channel 7 access-group

Port-Channel 7:

Port-Vlan Session ACL
---------------------
SessionACL            Vlan     Status
----------          ----     ------
```

The output of this command includes the following parameters:

Parameter	Description
SessionACL	Session ACL name.
Vlan	VLAN number.
Status	ACL status.

```
#show interface port-channel 7 counters
Port          InOctets     InUcastPkts     InMcastPkts     InBcastPkts
PC 0:                0               0               0               0
Port         OutOctets    OutUcastPkts    OutMcastPkts    OutBcastPkts
PC 0:                0               0               0               0
```

The output of this command includes the following parameters:

Parameter	Description
PC	Port number.
InOctets	Number of octets received through the port.
InUcastPkts	Number of unicast packets received through the port.
InMcastPkts	Number of multicast packets received through the port.
InBcastPkts	Number of broadcast packets received through the port.
OutOctets	Number of octets sent through the port.
OutUcastPkts	Number of unicast packets sent through the port.
OutMcastPkts	Number of multicast packets sent through the port.
OutBcastPkts	Number of broadcast packets sent through the port.

```
#show interface port-channel 7 trusted-vlan

Name:  Port-channel 7
Switchport:  Enabled
Administrative mode:  static access
Operational mode:  static access
Administrative Trunking Encapsulation:  dot1q
Operational Trunking Encapsulation:  dot1q
Access Mode VLAN: 1 (Default)
Trunking Native Mode VLAN: 1 (Default)
Trunking Vlans Enabled: NONE
Trunking Vlans Active: NONE
```

The output of this command includes the following parameters:

Parameter	Description
Name	Port name.
Switchport	Whether or not switchport is enabled.
Administrative mode	Administrative mode .
Operational mode	Operational mode.
Administrative Trunking Encapsulation	Encapsulation method used for administrative trunking.
Operational Trunking Encapsulation	Encapsulation method used for operational trunking.
Access Mode VLAN	The access mode VLAN for the specified port.
Trunking Native Mode VLAN	The trunking native mode VLAN for the specified port.
Trunking Vlans Enabled	Number of trunking VLANs currently enabled.
Trunking Vlans Active	Number of trunking VLANs currently active.

```
#show interface port-channel 7 trusted-vlan

Name:  Port-Channel7
Trusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the specified port.
`trusted Vlan(s)`	List of trusted VLANs.

```
#show interface port-channel 7 untrusted-vlan

Name:  FE1/0
Untrusted Vlan(s)
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the specified port.
`Untrusted Vlan(s)`	List of untrusted VLANs.

```
#show interface port-channel 7 xsec

xsec vlan 7 is ACTIVE
```

The output of this command includes the following parameters:

Parameter	Description
`xsec vlan 7 is ACTIVE`	This states that xsec is active on the specified port as well as the associated VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show interface-profile voip-profile

```
show interface-profile voip-profile <profile-name>
```

Description

This command displays the specified VoIP profile configuration information.

Syntax

Parameter	Description
`<profile-name>`	Name of the VoIP profile.

Examples

The following example shows configuration details for the VoIP profile:

```
(host) #show interface-profile voip-profile profile1
VOIP profile "profile1"
-----------------------
Parameter  Value
---------  -----
VOIP VLAN  1
DSCP       0
802.1 UP   0
VOIP Mode  auto-discover
```

The output of this command includes the following information:

Parameter	Description
`VOIP VLAN`	The Voice VLAN ID.
`DSCP`	The DSCP value for the voice VLAN.
`802.1 UP`	The 802.11p priority level.
`VOIP Mode`	The mode of VoIP operation. It can be auto-discover or static.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show interface tunnel

```
show interface tunnel <id>
```

Description

Displays information about tunnel interfaces.

Syntax

Parameter	Description
`id`	Tunnel interface number.

Example

The example below shows the output of **show interface tunnel** for IPv4.

```
(host) [mynode] #show interface tunnel 2000
Tunnel 64001 is up line protocol is up
Description: Internal Tunnel created for managed device communication
Internet address is 14.14.14.2 255.255.255.252
Source  10.4.251.65
Destination 12.12.12.1
Tunnel mtu is set to 1100
Tunnel is an IP GRE TUNNEL
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Tunnel keepalive is disabled
ip access-group r1 in
```

The example below shows the output of **show interface tunnel** for IPv6.

```
(host) [mynode] #show interface tunnel 21
Tunnel 21 is up line protocol is up
Description: Tunnel Interface
Internet address is 2005:81::1:2
Source  2082::802:1(Vlan 802)
Destination 2082::802:2
Tunnel mtu is set to 1280
Tunnel is an IPv6 GRE TUNNEL
Tunnel is Trusted
Inter Tunnel Flooding is enabled
Tunnel keepalive is disabled
```

The output of this command includes the following parameters:

Parameter	Description
`Tunnel 2000 is...`	Status of the specified tunnel.
`line protocol is...`	Displays the status of the line protocol on the specified tunnel.
`Description`	Description of the specified interface.
`Internet address is...`	IP address of the specified interface.

Parameter	Description
`Source`	IP address of the tunnel's source.
`Destination`	IP address of the tunnel's destination.
`Tunnel mtu is set to...`	Size of the specified tunnel's MTU.
`Tunnel is an...`	Description of the specified tunnel.
`Tunnel is...`	Whether or not the specified tunnel is trusted.
`Inter tunnel flooding is...`	Status of inter tunnel flooding on the specified tunnel.
`Tunnel keepalive is...`	Status of tunnel keepalive on the specified tunnel.
`ip access-group`	Name of a routing ACL applied to inbound traffic on a managed device terminating an L3 GRE tunnel in an IPv4 network.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show interface vlan

```
show interface vlan <id> [access-group]
```

Description

Displays information about a specified VLAN interface.

Syntax

Parameter	Description
`<id>`	VLAN interface number.
`access-group`	Session ACL configured on this interface.

Example

The following example displays information about VLAN 90:

```
(host) [mynode] #show interface vlan 20

VLAN20 is up line protocol is up
Hardware is CPU Interface, Interface address is 00:0C:29:3C:F7:D3 (bia 00:0C:29:3C:F7:D3)
Description: 802.1Q VLAN
IPv6 is enabled, link-local address is fe80::c:2900:143c:f7d3
Global unicast address(es):
2017::1, subnet is 2017::/64
IPv6 Router Advertisements are disabled
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled, BCMC Optimization disabled ProxyARP disabled Suppress ARP
enable
Encapsulation 802, loopback not set
MTU 1500 bytes
Last clearing of "show interface" counters 1 day 2 hr 55 min 37 sec
link status last changed 1 day 0 hr 37 min 24 sec
Proxy Arp is disabled for the Interface
IPv6 Helper Addresses Configured on this Interface:
2017::2 with source ::
```

The output of this command includes the following parameters:

Parameter	Description
`VLAN1 is...`	Status of the specified VLAN.
`line protocol is...`	Displays the status of the line protocol on the specified port.
`Hardware is...`	Describes the hardware interface type.
`Interface address is...`	Displays the MAC address of the hardware interface.
`Description`	Description of the specified VLAN.
`Internet address is...`	IP address and subnet mask of the specified VLAN.

Parameter	Description
`IPv6 Router Advertisements...`	Status of IPv6 RA.
`Routing interface is...`	Status of the routing interface.
`Forwarding mode is...`	Status of the forwarding mode.
`Directed broadcast is...`	Displays whether or not directed broadcast is enabled.
`BCMC Optimization...`	Status of broadcast-multicast optimization.
`ProxyARP...`	Status of proxy ARP. Proxy ARP is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network.
`Supress ARP...`	Status of suppressed ARP. If enabled, the managed device prevents flooding of ARP broadcasts on all the untrusted interfaces.
`Encapsulation`	Encapsulation type.
`loopback...`	Loopback status.
`MTU`	MTU size of the specified port in bytes.
`Last clearing of "show interface counters"`	Time since **show interface counters** was cleared.
`link status last changed`	Time since link status last changed.
`Proxy ARP is...`	Status of proxy ARP on the specified interface.
`IPv6 Helper Addresses...`	Helper address configured for a vlan.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **IPv6 helper-address** is displayed in the output.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show inventory

```
show inventory
```

Description

This command displays the hardware inventory of Mobility Master or the managed device.

Syntax

No parameters.

Example

Execute this command to display the hardware component inventory of Mobility Master.

```
(host) [mynode] #show inventory

Mgmt Port HW MAC Addr           : 00:0C:29:71:10:0B
HW MAC Addr                     : 00:0C:29:71:10:15
System Serial#                  : DC0604083
Activate license                : Not applicable
Supported device type           : MM
Active device type              : MM
```

Issue this command to display the hardware component inventory of the managed device. The output of this command will vary depending on the controller platform type.

```
(host-md) #show inventory

Supervisor Card slot            : 0
System Serial#                  : BA0009743 (Date:12/26/14)
CPU Card Serial#                : AE51038711 (Date:12/25/14)
CPU Card Assembly#              : 2010216H
CPU Card Revision               : (Rev:01.00)
Interface Card Serial#          : AE51031572 (Date:12/25/14)
Interface Card Assembly#        : 2010085E
Interface Card Revision         : (Rev:04.00)
SC Model#                       : Aruba7210
HW MAC Addr                     : 00:1a:1e:01:b2:28 to 00:1a:1e:01:b2:2f
CPLD Version                    : (Rev: 1.4)
Power Supply 0                  : Present               : No
Power Supply 1                  : Present               : Yes
: 12V OK                : Yes
: Fan OK                : Yes
: Aruba Model No        : 2510057
: Vendor & Model No     : QCS DCJ3501-01P
: Serial No             : QCS142320YU
: MFG Date              : 6/5/14
: Output 1 Config       : 12V 350W
: Input Min             : 90V AC
: Input Max             : 264V AC
Main Board Temperatures         :
: U24 - Local Temp      30 C (shadow of XLP heatsink)
: Q1  - Remote 1 Temp   34 C (shadow of VRM, VDD_CPU)
: Q2  - Remote 2 Temp   33 C (shadow of VRM, VDD_SOC)
: U44 - Local Temp      25 C (shadow of DPI connector)
: U29  - Remote 1 Temp  31 C (XLP die temperature)
: Q36  - Remote 2 Temp  28 C (shadow of 98X1422)
: J2  - DDR A Temp      24 C (DDR3 A temp)
: J4  - DDR B Temp      26 C (DDR3 B temp)
```

```
: J1  - DDR C Temp      25 C (DDR3 C temp)
: J3  - DDR D Temp      27 C (DDR3 D temp)
: Port 0 Temp           148 C (1G PHY temp)
: Port 1 Temp           148 C (1G PHY temp)
Interface Board Temperatures    :
: U21 - Local Temp      27 C (shadow of port 1 RJ45)
: Q4 - Remote 1 Temp    28 C (shadow of 88E1543)
: Q3 - Remote 2 Temp    34 C (shadow of 88X2140)
Fan  0                          : 8916 rpm (5.495 V),Speed Low
Fan  1                          : 9029 rpm (5.495 V),Speed Low
Fan  2                          : 9029 rpm (5.450 V),Speed Low
Fan  3                          : 8998 rpm (5.630 V),Speed Low
Main Board Voltages             :
ispPAC_POWR1014A_A              :
: 1V2                   1.20V sense 1.232 V
: VDD SOC               0.937V sense 0.918 V
: VCC IOBD 1V5          1.50V sense 1.528 V
: DDR3BD_VTT            0.75V sense 0.750 V
: VCC 1A                1.00V sense 1.024 V
: IV8_DIGITAL           1.80V sense 1.848 V
: 3V3_MAIN              3.30V sense 3.366 V
: VCC1                  1.00V sense 1.018 V
: VCC25                 2.50V sense 2.556 V
: 3V3 SB                3.30V sense 3.360 V
ispPAC_POWR1014A_B              :
: VDD                   0.806V sense 0.786 V
: VCC IOAC 1V5          1.50V sense 1.528 V
: DDR3AC_VTT            0.75V sense 0.752 V
: VDD_SRAM              1.00V sense 1.042 V
: VCC1B                 1.00V sense 1.030 V
: 1V8_ANALOG            1.80V sense 1.854 V
: 1V8                   1.80V sense 1.866 V
: VDDIO12_XAUI          1.20V sense 1.224 V
: 5V                    5.00V sense 5.016 V
Interface Board Voltages        :
ispPAC_POWR6AT6                 :
: VCC33                 3.30V sense 3.366 V
: VCC 18                1.80V sense 1.856 V
: VCC1                  1.00V sense 1.026 V
: VCC12                 1.20V sense 1.224 V
: VCC12-DVDD            1.20V sense 1.212 V
: VCC9                  0.90V sense 0.928 V
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master and Enable mode on Managed Device

show iostat

```
show iostat
```

Description

Displays Input/Output statistics information. This command reports Central Processing Unit (CPU) statistics and Input/Output statistics for devices and partitions.

Syntax

No parameters.

Example

Execute this command to display the IO statistics.

```
(host) [mynode] #show iostat
cpu  14758445 156489 6454935 212748689 15245 1 144063 0 0 0
cpu0 4988672 156489 3559088 72948377 9573 0 89321 0 0 0
cpu1 3873089 0 1502850 70458657 4154 0 52448 0 0 0
cpu2 5896683 0 1392996 69341654 1518 0 2293 0 0 0
intr 9236964064 116 65 0 0 0 0 0 0 42 0 0 0 138 0 0 10 0 871627 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4 7 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
ctxt 52889897218
btime 1466401810
processes 5196099
procs_running 5
procs_blocked 0
softirq 1915750309 0 1199417791 43441649 61826308 798090 0 62 191223519 12557883 406485007
```

The output includes the following parameters:

Parameter	Description
cpu	The number of jiffies (1/100th of a second) that the system spent in user mode, user mode with low priority, system mode, and the idle task, respectively.
page	The number of pages the system paged in and the number that were paged out (from disk).
swap	The number of swap pages that have been brought in an out.
intr	The number of interrupts received from the system boot.
disk_io	(x,y) is (major, minor):(xx, xx, xxxx, x, x) is (noinfo, read_io_ops, blks_read, write_ io_ops, blks_written).
ctxt	The number of context switches that the system underwent.

Parameter	Description
`btime`	The boot time, in seconds.
`processes`	The number of forks since boot.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show iot transportProfile

```
show iot transportProfile [<profile-name>]
```

Description

This command displays the IoT profile status.

Example

The example below shows the IoT profile status.

```
(host) [mynode] #show iot transportProfile
IoT Data Profile List
---------------------
Name                      References  Profile Status
----                      ----------  --------------
iot_xg_assettag           0
iot_xg_assettag_staging   0
test1                     0
Total:3
```

Command History

Release	Modification
ArubaOS 8.3.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip access-group

```
show ip access-group
```

Description

Displays ACLs configured for each port on Mobility Master.

Syntax

No parameters.

Examples

The example below shows part of the output of this command. If a port does not have a defined session ACL, the *Port-Vlan Session ACL* table will be blank.

```
(host) [mynode] #show ip access-group

FE 1/0:
Rx access list 200 is applied
session access list User14 is applied

Port-Vlan Session ACL
---------------------
SessionACL            Vlan     Status
----------            ----     ------
coltrane              22       configured
```

The output of this command includes the following parameters:

Parameter	Description
`Session ACL`	Name of the ACL applied to the interface.
`VLAN`	If the ACL was applied to a VLAN associated with this port, this column will show the VLAN ID.
`Status`	Shows whether or not the session ACL is configured.

Related Commands

Command	Description
interface gigabitethernet ip access-group	Configures an access group for an interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip access-list

```
show ip access-list
   brief [ipv4|ipv6]
   <string>
```

Description

This command displays a table of all configured ACLs, or show details for a specific ACL.

Syntax

Parameter	Description
`brief`	Display a table of information for all ACLs.
`<string>`	Specify the name of a single ACL to display detailed information on that ACL.

Examples

The example below shows general information for all ACLs in the Access List table.

```
(host) [mynode] #show ip access-list brief

Access list table (4 - IPv4, 6 - IPv6)
--------------------------------------
Name                          Type          Use Count  Roles
----                          ----          ---------  -----
allow-diskservices            session(4)
allow-printservices           session(4)
allowall                      session(46)   3          default-via-role default-vpn-role
authenticated
ap-acl                        session(4)    1          ap-role
ap-uplink-acl                 session(4)
apprf-authenticated-sacl      session       1          authenticated
apprf-default-via-role-sacl   session       1          default-via-role
apprf-default-vpn-role-sacl   session       1          default-vpn-role
apprf-guest-sacl              session       1          guest
apprf-stateful-dot1x-sacl     session       1          stateful-dot1x
apprf-voice-sacl              session       1          voice
captiveportal                 session(4)    2          guest-logon logon
captiveportal6                session(6)    2          guest-logon logon
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of an ACL.
`Type`	Shows that the ACL is one of the following ACL policy types: ■ Ethertype ■ Standard ■ Session ■ MAC ■ Extended

Parameter	Description
Use Count	Number of rules defined in the ACL.
Roles	Names of user roles associated with the ACL.

Include the name of a specific ACL to show detailed configuration information for that ACL. The output in the example below has been divided into two sections to better fit int this document. The output in the CLI will appear in a single, long table.

```
(host) [mynode] # show ip access-list captiveportal6

ip access-list session captiveportal6
captiveportal6
--------------
Priority  Source  Destination  Service          Application     Action   NextHopList TimeRange

--------  ------  -----------  -------          -----------     ------   ----------- ---------

1         user    md-6         svc-https                        captive

2         user    any          svc-http                         captive
3         user    any          svc-https                        captive
4         user    any          svc-http-proxy1                  captive

5         user    any          svc-http-proxy2                  captive

6         user    any          svc-http-proxy3                  captive


Log     Expired Queue TOS  8021P  Blacklist  Mirror  DisScan  IPv4/6    Contract

---     ------- ----- ---  -----  ---------  ------  -------  ------    --------

                Low                                          6
                Low                                          6
                Low                                          6
                Low                                          6
                Low                                          6
                Low                                          6
```

The output of the **show ip access-list** command may include some or all of the following parameters:

Parameter	Description
Priority	Name of an access-control list (ACL).
Source	The traffic source, which can be one of the following: ■ **alias**: The network resource (use the netdestination command to configure aliases; use the show netdestination command to see configured aliases) ■ **any**: Matches any traffic. ■ **host**: A single host IP address. ■ **network**: The IP address and netmask. ■ **user**: The IP address of the user. ■ **localip**: The set of all local IP addresses on the system, on which the ACL is applied.

Parameter	Description
Destination	The traffic destination, which can be one of the following: ■ **alias**: The network resource (use the netdestination command to configure aliases; use the show netdestination command to see configured aliases) ■ **any**: Matches any traffic. ■ **host**: A single host IP address. ■ **network**: An IP address and netmask. ■ **user**: The IP address of the user. ■ **localip**: The set of all local IP addresses on the system, on which the ACL is applied**.**
Service	Network service, which can be one of the following: ■ An IP protocol number (0-255). ■ The name of a network service (use the show netservice command to see configured services). ■ **any**: Matches any traffic. ■ **tcp**: A TCP port number (0-65535). ■ **destination port number**: specify the TCP port number (0-65535) ■ **source**: TCP or UDP source port number ■ **udp**: A UDP port number (0-65535).
Application	Name of the application to which the ACL is applied. (For a complete list of supported applications, issue the command **show dpi application all**.)
Action	Action if rule is applied, which can be one of the following: **deny**: Reject packets. **dst-nat**: Perform destination NAT on packets. **dual-nat**: Perform both source and destination NAT on packets. **permit:** Forward packets. **redirect**: Specify the location to which packets are redirected, which can be one of the following: ■ Datapath destination ID (**0-65535**). ■ **esi-group**: Specify the ESI server group configured with the esi group command ■ **opcode**: Specify the datapath destination ID (0x33, 0x34, or 0x82). Do not use this parameter without proper guidance from Aruba. **tunnel:** Specify the ID of the tunnel configured with the interface tunnel command. **src-nat**: Perform source NAT on packets.
IpsecMap	Packets can be redirected over a VPN tunnel by specifying the name of an IPsec map in the ACL. This column specifies the name of an IPsec map used by a router ACL. For more information on IPsec maps, see crypto-local ipsec-map.
Timerange	Any defined time range for this rule.
NextHopList	If the access rule uses PBR to forwards packets to a nexthop device, then this column displays the next-hop list associated with the rule. For more information on next-hop lists, see ip nexthop-list on page 628.
Tunnel	Packets can be redirected over an L3 GRE tunnel. If the ACL routes packets over a tunnel, this column specifies the tunnel used by the ACL.
TunnelGroup	Packets can be redirected over an L3 GRE tunnel group. If the ACL routes packets over a tunnel in a tunnel group, this column specifies the tunnel group used by the ACL. For more information on tunnel groups, see tunnel-group.
Log	Shows if the rule was configured to generate a log message when the rule is applied.
Expired	Shows if the rule has expired.

Parameter	Description
`Queue`	Shows if the rule assigns a matching flow to a priority queue (high or low).
`8021.p`	802.11p priority level applied by the rule (0-7).
`Blacklist`	Shows if the rule should blacklist any matching user.
`Mirror`	Shows if the rule was configured to mirror all session packets to datapath or remote destination.
`DisScan`	Shows if the rule was configured to pause ARM scanning while traffic is present.
`IPv4/6`	Shows the IP version.
`Contract`	Shows the bandwidth contract status.

Related Commands

Command	Description
ip access-list session	Configure an access list for an interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip cp-redirect-address

```
show ip cp-redirect-address
```

Description

Show the captive portal automatic redirect IP address.

Syntax

No parameters.

Examples

The example below shows the IP address to which captive portal users are automatically directed.

```
(host) [mynode] # show ip cp-redirect-address

Captive Portal IPv4 redirect Address ... 10.3.63.11
Captive Portal IPv6 redirect Address ... ::1
```

Related Commands

Command	Description
ip cp-redirect-address	This command configures a redirect address for captive portal.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip dhcp

```
show ip dhcp
  binding
  database
  relay statistics
  statistics
```

Description

This command displays the DHCP server binding, database setting, relay and pool statistics.

Syntax

Parameter	Description
`binding`	Show DHCP server bindings.
`database`	Show DHCP server settings.
`relay statistics`	Show DHCP relay statistics.
`statistics`	Show DHCP pool statistics.

Examples

The example below shows DHCP statistics for two configured networks.

```
(host) [mynode] #show ip dhcp statistics

DHCPv4 enabled; DHCPv6 enabled
DHCP Pools
----------
Network Name  Type  Active  Configured leases  Active leases  Free leases  Expired leases
Abandoned leases
------------  ----  ------  -----------------  -------------  -----------  --------------  ---
-------------
2-2-2-nw      v4    Yes     242                0              242          0               0
3-2-2-nw      v4    Yes     254                0              254          0               0
test          v4    Yes     254                0              254          0               0
2011          v6    No      5                  -              -            -               -
2012          v6    No      5                  -              -            -               -
Current leases          750
Total leases            512
```

Starting from ArubaOS 8.2.0.0, if the DHCP lease limit is configured to exceed the user limit, a warning is displayed in the command output.

```
host) (config) #show ip dhcp statistics
DHCPv4 disabled; DHCPv6 disabled
DHCP Pools
----------
Network Name  Type  Active  Configured leases  Active leases  Free leases  Expired leases
------------  ----  ------  -----------------  -------------  -----------  --------------
Abandoned leases
---------- ------
Current leases          0
Total leases            2048
WARNING: DHCP lease limit increased beyond user limit. Some of the controller's services may
be impacted
```

NOTE: To make a DHCPv6 pool active, ensure that the pool name is added in vlan interface.

The output of this command includes the following parameters:

Parameter	Description
Network Name	Range of addresses that the DHCP server may assign to clients.
Type	Indicates the IP version of the DHCP server. It can be v4 or v6.
Active	Indicates if the DHCP server is active or not.
Configured leases	Number of leases configured on the DHCP server.
Active leases	Number of active DHCP leases.
Free leases	Number of available DHCP leases.
Expired leases	Number of leases that have expired because they have extended past their valid lease period.
Abandoned leases	Number of abandoned leases. Abandoned leases will not be reassigned unless there are no free leases available.

Related Commands

Command	Description
ip dhcp pool	This command configures a DHCP pool on Mobility Master.
ipv6 dhcp pool	This command configures a DHCPv6 pool on Mobility Master.
ip dhcp increase-increase-limit	This command increases the DHCP scope on a controller—7005, 7008, or 7010 Controllers—to twice the user limit.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip domain-name

```
show ip domain-name
```

Description

This command displays the full domain name and server.

Syntax

No parameters.

Examples

The following example displays that the IP domain lookup feature is enabled, and the DNS server is configured on the managed device.

```
(host) [mynode] #show ip domain-name

IP domain lookup:                Enabled
IPv6 domain lookup:              Enabled
IP Host.Domain name:             SP-VMC.
DNS servers
===========
10.13.6.110
10.13.5.200
2020::abcd:abcd
```

Related Commands

Command	Description
ip domain lookup	This command enables DNS hostname to address translation.
ip domain-name	This command configures the default domain name.
ipv6 domain lookup	This command enables IPv6 Domain Name System hostname translation for clients.
ipv6 name-server	This command configures the IPv6 address of the domain name server.
ip dhcp pool	This command configures a DHCP pool on Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The **IPv6 domain lookup** parameter was added.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip-flow-export

```
show ip-flow-export
   collector [<ipaddr>]
   gsm-cache
```

Description

This command shows information for IP flow collector and the GSM cache.

Syntax

Parameter	Description
`collector [<ipaddr>]`	Specify the IP address of the collector.
`gsm-cache`	Shows GSM cache.

Example

The following command displays information about the IP flow collector.

```
(host) [mynode] #ip-flow-export collector

Observation Domain: 168096376 (Controller IP)
Collector IP Not Configured, protocol udp, port 4739, not enabled, not connected
Upload template always, upload all sessions every 15 minute(s), no upload flow cache snapshot
15000 flow cache size, 0 flows exported, next sequence 0, 0 packets, 0 bytes
Last template send: Never, last dispatch: Never
0 Connect errors, 0 connection resets, 0 send errors, 0 flows dropped, 0 blocked sends
(RJ_LC120) #show ip-flow-export collector 1.1.1.1
Observation Domain: 168096376 (Controller IP)
Collector IP 1.1.1.1, protocol udp, port 4739, not enabled, not connected
Upload template always, upload all sessions every 15 minute(s), no upload flow cache snapshot
15000 flow cache size, 0 flows exported, next sequence 0, 0 packets, 0 bytes
Last template send: Never, last dispatch: Never
0 Connect errors, 0 connection resets, 0 send errors, 0 flows dropped, 0 blocked sends
No flows
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip-flow-export wireless-cache

```
show ip-flow-export wireless-cache
```

Description

This command displays the cache for WLAN information.

Syntax

None.

Example

```
(host) [mynode] #show ip-flow-export wireless-cache

Flags: S - Source-ip, D - Dest-ip
IP Flow Export Wireless Cache
-----------------------------
STA ip    STA mac            ESSID                 AP mac             Flags
------    -------            -----                 ------             -----
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  S
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  S
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  D
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  S
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  D
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  S
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  S
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  D
7.7.7.2   3c:77:e6:7c:43:0e  nbhardwaj-vlan700-psk  18:64:72:c7:33:1c  S
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  S
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  D
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  S
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  D
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  D
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  D
4.4.4.4   3c:77:e6:7c:47:9d  nbhardwaj-mm-psk       18:64:72:c7:33:1c  S
6.6.6.4   5c:e0:c5:5f:b9:9b  nbhardwaj-ipfix-psk    9c:1c:12:c0:86:9c  S
```

Command History

Version	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Available in the base operating system	Config or Enable mode on Mobility Master.

show ip-flow-export-profile

```
show ip-flow-export-profile
```

Description

This command shows the stats for IP flow collector profile.

Syntax

No syntax

Example

The following command displays details for the IP flow export profile

```
(host) [mynode] #show ip-flow-export-profile

IP Flow Collector Profile
-------------------------
Parameter                                       Value     Set
---------                                       -----     ---
State                                           Disabled
Interval (minutes) to upload all active sessions  15
Interval (minutes) to upload cache snapshot       0
Interval (minutes) to upload IPFIX template       0
Transport Protocol for collector connection       udp
IPFIX Collector IP address                        N/A
Transport Port for collector connection           4739
Flow Cache size in entries                        15000
Observation Domain                                0
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip health-check

```
show ip health-check <probe-ip> <src_intf>
```

Description

This command displays the health-check status of the uplink interfaces of a branch office managed device.

Syntax

Parameter	Description
`<probe-ip>`	IP address of Mobility Master.
`<src_intf>`	Source interface VLAN.

Usage Guidelines

This command should be executed from the branch office managed device.

Example

The following example displays the status of two uplinks on a branch office managed device.

```
(host-md) #show ip health-check

IP Health-Check Entries
-----------------------
Probe IP        Src Interface   State    Probe Profile   Avg RTT(ms)
--------        -------------   ------   -------------   ----------
10.10.10.254    vlan 1          UP       Default         20.4
10.10.10.254    Cellular        DOWN     Default         0
```

The output of this command includes the following data columns.

Parameter	Description
`Probe IP`	IP address of Mobility Master.
`Src Interface`	IP address of the uplink gateway interface through which the probes were sent.
`State`	Shows if the uplink is in an UP or DOWN state.
`Probe-Profile`	A branch of managed device supports only the **default** IP probe profile. For information on configuring an IP probe profile, see **ip probe default**
`Avt RTT (in ms)`	The average round trip time, in milliseconds. If the round trip time is less than 1 millisecond, the average round trip time will appear as 0.

Related Commands

Command	Description
ip probe default	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.

Command	Description
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.
show ip probe	This command displays the settings for the WAN health-check ping-probes.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Managed Device

show ip igmp

```
show ip igmp
   cluster
   config
   counters
   group maddr <maddr> [mac <mac-addr>|source <addr>]
   interface [vlan <vlan>]
   proxy-group [vlan <vlan>]
   proxy-mobility-group maddr <maddr>
   proxy-mobiity-stats
   proxy-stats
```

Description

This command displays IGMP timers and counters.

Syntax

Parameter	Description
`cluster`	See show ip igmp cluster.
`config`	Show the current IGMP configuration
`counters`	Display a list counters for the following IGMP queries: ■ received-total ■ received-queries ■ received-v1-reports ■ received-v2-reports ■ received-leaves ■ received-unknown-types ■ len-errors ■ checksum-errors ■ not-vlan-dr ■ transmitted-queries ■ forwarded
`group maddr <maddr>`	Displays the following IGMP group information: ■ mac: Specify MAC address of the specific member. ■ source: Specify the source address of the specific SSM group.
`interface vlan <vlan>`	Show IGMP interface information
`proxy-group vlan <vlan>`	Show IGMP proxy group information for a specific interface.
`proxy-mobility-group maddr <maddr>`	Display the IGMP proxy group information stored for mobile clients which are away from the managed device.
`proxy-mobiity-stats`	Display the most important messages exchanged between the mobility process and the IGMP proxy.
`proxy-stats`	Display the number of messages transmitted and received by the IGMP proxy on the upstream interface

Examples

The following example displays the IGMP interface table for all VLANs on Mobility Master.

```
(host) [mynode] #show ip igmp interface vlan 2

IGMP Interface Table
--------------------
VLAN  Addr        Netmask        MAC Address        IGMP      Snooping  Querier
Destination IGMP Proxy
----  ----        -------        -----------        ----      --------  -------     ----------
- -----------
64    10.6.4.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.4.252  CP
disabled
65    10.6.5.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.5.252  CP
disabled
1     10.6.2.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.2.252  CP
disabled
66    10.6.6.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.6.252  CP
disabled
63    10.6.3.252  255.255.255.0  00:0b:86:01:99:00  disabled  disabled  10.6.3.252  CP
disabled
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	A VLAN ID number.
Addr	IP address of a VLAN router.
Netmask	Subnet mask for the IP address.
MAC Address	MAC destination address.
IGMP	Indicates if IGMP is enabled (or disabled) on the interface.
Snooping	Indicates if IGMP snooping is enabled (or disabled).
Querier	IP address of an IGMP querier.
Destination	Traffic destination.
IGMP Proxy	Indicates if IGMP proxy is enabled (or disabled).

The following example displays the current IGMP configuration settings for Mobility Master.

```
(host) [mynode] #show ip igmp config

IGMP Config
-----------
Name                              Value
----                              -----
robustness-variable               2
query-interval                    30
query-response-interval           100
startup-query-interval            31
startup-query-count               2
last-member-query-interval        10
last-member-query-count           2
version-1-router-present-timeout  400
```

```
version-2-router-present-timeout  400
max-members-per-group             300
quick-client-convergence          enabled
ssm-range                         IANA standard range. 232.0.0.0/8
```

The output of this command includes the following parameters:

Parameter	Description
robustness-variable	This variable is increased from its default level of 2 to allow for expected packet loss on a subnetwork.
query-interval	Interval, in seconds, at which Mobility Master sends host-query messages to the multicast group address 224.0.0.1 to solicit group membership information.
query-response-interval	Maximum time, in .1 second intervals, that can elapse between when Mobility Master sends a host-query message and when it receives a response. This must be less than the **query-interval**.
startup-query-count	Number of queries that Mobility Master sends out on startup, separated by startup-query-interval. The default setting is the value of the **robustness-variable** parameter.
startup-query-interval	Interval, in seconds, at which Mobility Master sends general queries on startup. The default value of this parameter is 1/4 of the **query-interva**l.
last-member-query-count	Number of group-specific queries that Mobility Master sends before assuming that there are no local group members.
last-member-query-interval	Maximum time, in seconds, that can elapse between group-specific query messages.
version-1-router-present-timeout	Timeout, in seconds, if Mobility Master detects a version 1 IGM router.
version-2-router-present-timeout	Timeout, in seconds, if Mobility Master detects a version 2 IGM router.

The following examples displays the information on IGMP groups:

```
(host) [mynode] #show ip igmp group

IGMP Group Table
----------------
(Source,Group)            Members
--------------            -------
(172.12.2.2, 232.0.0.2)   2
(172.12.2.2, 232.0.0.1)   2
(*, 224.0.0.252)          2
(*, 239.255.255.250)      2

Total Groups: 4

(host) [mynode] #show ip igmp group maddr 232.0.0.1 source 172.12.2.2

IGMP Group (172.12.2.2, 232.0.0.1) Table
----------------------------------------
Member          MAC                Vlan  Destination  Version  Age
------          ---                ----  -----------  -------  ---
172.13.0.4      00:00:00:00:00:00  13    0/0/0        0        4
```

```
172.12.255.252  98:fc:11:c6:20:04  13    Tunnel 9     3        4
```

Related Commands

Command	Description
ip igmp	This command configures IGMP timers and counters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show ip igmp cluster

```
show ip igmp cluster
   aac-info
   bss-info
   client-info
   dmo-off-info
   info
   proxy-group
   stats
```

Description

Display IGMP related cluster information.

Syntax

Parameter	Description
`aac-info`	Show Cluster AAC information of APs.
`bss-info`	Show IGMP BSS information.
`client-info`	Show IGMP cluster client information.
`dmo-off-info`	Show list of (S,G,BSS) where DMO threshold is hit.
`info`	Show Cluster information.
`proxy-group`	Show IGMP cluster proxy database group information.
`stats`	Show cluster statistics.

Related Commands

Command	Description
ip igmp	This command configures IGMP timers and counters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Available in Config or Enable mode on managed device.

show ip interface brief

```
show ip interface brief
```

Description

This command displays the IP-related information on all interfaces in summary format.

Syntax

No parameters.

Example

```
(host) #show  ip interface brief

Interface                   IP Address / IP Netmask        Admin    Protocol     VRRP-IP
vlan 1                   172.16.0.254 / 255.255.255.0      up       up
vlan 2                      10.4.62.9 / 255.255.255.0      up       up
loopback                  unassigned / unassigned          up       up
mgmt                      unassigned / unassigned          down     down
```

The following table details the columns and content in the show command.

Column	Description
Interface	List the interface and interface identification, where applicable.
IP Address /IP Netmask	List the IP address and netmask for the interface, if configured.
Admin	States the administrative status of the interface. Enabled—up Disabled—down
Protocol	Status of the IP on the interface. Enabled—up Disabled—down
VRRP-IP	VRRP IP address associated to the interface.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show ip mobile

```
show ip mobile
   act
   active-domains
   binding [<host-ip>|<host-ipv6>|<host-macaddr>|brief]
   domain [<name>]
   global
   hat
   host [<host-ip>|<host-ipv6>|<host-macaddr>|brief]
   multicast-vlan-table [client-macaddr]
   packet-trace [<count>]
   remote <host-ip>|<host-ipv6>|<host-macaddr>
   trace <host-ip>|<host-ipv6>|<mac-addr>|{force <host-ip>|<host-ipv6>|<mac-addr>}
   traffic dropped|foreign-agent|home-agent|proxy
   trail <host-ip>|<host-ipv6><host-macaddr>
   tunnel
   visitor [<host-ip>|<host-ipv6>|<host-macaddr>|brief]
```

Description

This command displays statistics and configuration information for the mobile protocol.

Syntax

Parameter	Description
`act`	Active anchor managed device table; subnets to another managed device map.
`active domains`	IP mobility domains active on this switch
`binding`	Display a list of Home Agent Bindings
`[<host-ip>]`	Filter the Home Agent Bindings list to display data for a specific host IPv4 address.
`[<host-ipv6>]`	Filter the Home Agent Bindings list to display data for a specific host IPv6 address.
`[<host-macaddr>]`	Filter the Home Agent Bindings list to display data for a specific host MAC address.
`[brief]`	Limit the output of this command to show just two lines of data.
`domain [<name>]`	Display subnet, VLAN, and home agent information for all mobility domains, or specify a mobility domain name to view data for that domain only.
`global`	View the current Mobility Agents global configuration
`hat`	Display the active Home Agent table
`host`	Display a list of Mobile IP hosts.

Parameter	Description
[<host-ip>]	Filter the Mobile Host List to display data for a specific host IPv4 address.
[<host-ipv6>]	Filter the Mobile Host List to display data for a specific host IPv6 address.
[<host-macaddr>]	Filter the Mobile Host List to display data for a specific host MAC address.
[brief]	Limit the output of this command to show just two lines of data.
multicast-vlan-table	Displays mobility multicast VLAN table information.
mac	MAC address of the client.
packet-trace [<count>]	The output of this command shows when packets of different types were sent between a source IP or MAC address and a destination IP or MAC address.
remote <host-ip>| <host-ipv6>|<host-macaddr>	This is a debug command can be used to identify the managed device associated with the specified client IPv4 or IPv6 address or MAC address. The output of this command shows the home agent (HA) and foreign agent (FA) for a mobile client, as well as the client's roaming status.
trace	Show if the Mobile IP feature will poll remote managed device for mobility status of station.
<host-ip>	Host IPv4 address.
<host-ipv6>	Host IPv6 address.
<mac-addr>	Host MAC address
force <host-ip>| <host-ipv6>|<mac-addr>	Show if the Mobile IP feature will poll remote managed device for mobility status of station.
traffic	Display mobile IP protocol statistics for: ■ Proxy Mobile IP ■ Home Agent Registrations ■ Foreign Agent Registrations ■ Registration Revocations
dropped	Show only counters for dropped mobility traffic.
foreign-agent	Show only mobile IP foreign agent statistics. A foreign agent is the managed device which handles all mobile IP communication with a home agent on behalf of a roaming client.
home-agent	Show only mobile IP home agent statistics. A home agent for a mobile client is the managed device where the client first appears when it joins the mobility domain.
proxy	Show only counters for mobile IP proxy traffic.
trail <host-ip>| <host-ipv6>|<host-macaddr>	Show the mobile IP roaming trail by entering a host's IP (IPv4 or IPv6)or MAC address.

Parameter	Description
`tunnel`	Show the Mobile Tunnel Table for IPIP tunnels.
`visitor`	Display a list of mobile nodes visiting a foreign agent.
`[<host-ip>]`	Filter the Foreign Agent Visitor list to display data for a specific host IPv4 address.
`[<host-ipv6>]`	Filter the Foreign Agent Visitor list to display data for a specific host IPv6 address.
`[<host-macaddr>]`	Filter the Foreign Agent Visitor list to display data for a specific host MAC address.
`[brief]`	Limit the output of this command to show just two lines of data.

Examples

The example below lists mobility domains configured on the managed device, and shows information for any subnets defined on these domains.

```
(host) [mynode] #show ip mobile domain

Mobility Domains:, 2 domain(s)
------------------------------

Domain name default
   Home Agent Table, 0 subnet(s)

Domain name newdomain
   Home Agent Table, 2 subnet(s)
        subnet          mask            VlanId Home Agent         Description
        --------------- --------------- ------ ---------------    -----------------------
        10.2.124.76     255.255.255.255 1      10.4.62.2          Corporate mobility entry
        172.21.5.50     255.255.255.255 1      10.4.62.2          Reserved entries
```

The output of this command includes the following parameters:

Parameter	Description
`Home Agent`	IP address of the home agent or mobility agent.
`Description`	Description of the HAT entry.

Use the **show ip mobile host** command to track mobile users.

```
(host) [mynode] #show ip mobile host

Mobile Host List, 1 host(s)
---------------------------
9c:b7:0d:3f:a6:dd  10.16.23.219  mob1
IPv4: 10.16.23.219
IPv6: fe80::826:aa9a:fe35:53e0
2004:deed::34
Roaming Status: Home Switch/Home VLAN, Service time 0 days 01:34:19
Home VLAN 623 on network 10.16.23.0/24
DHCP lease for PC at Sun Dec 23 20:32:00 2012 for 86400 secs from 10.16.28.1
```

The output of this command includes the following parameters:

Parameter	Description
`<mac-addr> <ip-addr>`	MAC and IP addresses of the host
`Roaming Status`	Displays how long the host has used its current managed device and VLAN.
`Home VLAN`	VLAN ID, IP address and subnet of the home VLAN.
`DHCP lease`	Displays the amount of time the station has had its current DHCP lease.

Related Commands

Command	Description
ip mobile active-domain	This command configures the mobility domain that is active on the managed device.
ip mobile domain	This command configures the mobility domain on the managed device.
ip mobile foreign-agent	This command configures the foreign agent for IP mobility.
ip mobile home-agent	This command configures the home agent for IP mobility.
ip mobile proxy	This command configures the proxy mobile IP module in a mobility-enabled managed device.
ip mobile revocation	This command configures the frequency at which registration revocation messages are sent.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ip nat pool

```
show ip nat pool
```

Description

This command displays a pool of IP addresses for NAT.

Syntax

No parameters.

Examples

The example below shows the current NAT pool configuration on Mobility Master.

```
(host) [mynode]# show ip nat pools

NAT Pools
---------
Name  Start IP     End IP       DNAT IP         Flags
----  --------     ---------    -------         -----
2net  192.0.2.2    192.0.2.48   192.0.2.222
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the NAT pool.
`Start IP`	IP address that defines the beginning of the range of source NAT addresses in the pool.
`End IP`	IP address that defines the end of the range of source NAT addresses in the pool.
`DNAT IP`	Destination NAT IP address, if defined.
`Flags`	NAT pool flags, if any.

Related Commands

Command	Description
ip nat	This command configures a pool of IP addresses for NAT.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license.	Enable or Config mode on Mobility Master.

show ip nexthop-list

```
show ip nexthop-list
   details STRING
   STRING
```

Description

This command displays the next hop list settings for policy-based routing.

Syntax

Parameter	Description
`details`	Displays detailed next hop settings for policy-based routing.
`STRING`	Displays the next hop settings based on the next hop list name.

Usage Guidelines

A next hop IP is the IP address of a adjacent router or device with layer-2 connectivity to managed device. The next hop list provides redundancy for the next hop devices by forwarding the traffic to a backup next hop device in case of failures. If active next hop device on the list becomes unreachable, traffic matching a policy-based routing ACL is forwarded using the highest-priority active next hop on the list. For more information on this feature, see ip nexthop-list on page 628.

Example

The following command displays the configuration settings for the one configured next hop list.

```
(host) [mynode] #show ip nexthop-list

Nexthop-List Entries
--------------------
Name                   Type            Dest  Preemptive Failover  Nexthop
----                   ----            ----  -------------------  -------
load-balance-gateways  Active-Active         Enabled
load-balance-ipsecs    Active-Active         Enabled
traditional-ipsecs     Active-Standby        Enabled

Nexthop Dest  Nexthop Priority
------------  ----------------
              10.18.2.254(2), 10.10.10.254(1)
```

The output of this command displays the following information

Parameter	Description
`Name`	Name of the next hop list
`Type`	Type of next hop.
`Dest`	Destination prefix address.

Parameter	Description
`Preemptive Failover`	This column indicates whether preemptive failover is enabled or disabled. If preemption is enabled and a higher priority next hop becomes reachable again, packets are again forwarded to the higher priority next hop.
`Nexthop`	Next hop IP address.
`Nexthop Dest`	Next hop destination prefix address.
`Nexthop Priority`	List of the IP addresses of all next hop IPs, including the priority assigned to each device when the list was configured.

Related Commands

Command	Description
ip route	This command configures a static route on Mobility Master. (These routes can use a next hop list.)
ip nexthop-list	Configure next hop list settings for policy-based routing.

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master

show ip ospf

```
show ip ospf
   database area <area-id>
   debug route
   interface [tunnel|vlan] <id>
   neighbor
   rapng-vpn aggregate-routes <ip-addr> <mask>
   redistribute
   subnet
```

Description

Display statistics and configuration information for the OSPF routing protocol.

Syntax

Parameter	Description
`database area <area-id>`	Show database information for the OSPF protocol.
`debug route`	Show debugging information for OSPF routes.
`interface [tunnel|vlan] <id>`	Display the status of OSPF on an individual interface by specifying a tunnel or VLAN ID number. The tunnel ID range is 1-16777215.
`neighbor`	Display data for OSPF neighboring routers.
`rapng-vpn`	Display IAP-VPN information.
`aggregate-routes <ip-addr> <mask>`	Display IAP-VPN aggregate route information.
`redistribute`	Display OSPF route distribution information.
`subnet`	Display the subnets manually added to the Subnet Exclude List via the router ospfsubnet exclude <addr> <mask> command.

Example

If you issue this command without any of the optional parameters described in the table above, the **show ip ospf** command will display general router and area settings for the OSPF.

```
(host) [mynode] #show ip ospf

OSPF is currently running with Router ID 123.45.110.200
Number of areas in this router is 1
Area 10.1.1.0
        Number of interfaces in this area is 2
        Area is totally stub area
        SPF algorithm executed 0 times
```

The output of this command includes the following parameters.

Parameter	Description
`OSPF Router ID`	Verifies that OSPF is running and the router ID that OSPF is running on.
`Number of areas`	List the number of areas configured in the router.
`Area`	Displays the Area ID followed by: ■ number of interfaces in the area ■ indicates if the area is a totally stub area ■ number of times the SPF algorithm has been executed

To display OSPF settings for an individual interface, you must specify a VLAN or tunnel ID number. The example below displays part of the output of the **show ip ospf interface vlan** command.

```
(host) [mynode] #show ip ospf interface vlan 1

Vlan 1 is up, line protocol is up
Internet Address 170.1.0.1, Mask 255.255.255.0, Area 2.0.1.1
Router ID 16.1.0.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROTHER, Priority 0
Designated Router id 0.0.0.0, Interface Address 170.1.0.1
Backup designated Router id 0.0.0.0, Interface Address 170.1.0.1
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Neighbor Count is 0
Tx Stat: Hellos 7 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 7
Tx Err:  BufNull 0 BufCorrupt 0 NoMem 0 SendFail 0
Rx Stat: Hellos 0 DbDescr 0 LsReq 0 LsUpdate 0 LsAck 0 Pkts 0
LoopSend 0 RxVirtualLink 0
Rx Err:  DisCd 0 BadVer 0 BadNet 0 BadArea 0 BadDstAdr 0 BadAuType 0
BadAuth 0 BadNeigh 0 BadPckType 0 BadVirtLink 0
IntfDown 0 MySource 0 Legal 0
```

...

The output may include some or all of the following parameters.

Parameter	Description
`Vlan <number>`	Identifies that the interface type and ID are up and functional.
`Internet Address`	Internet address, network mask, and area assigned to the interface.
`Router ID`	Displays the router ID, that the network type is Broadcast, and the cost value.
`Transmit Delay`	Details of the transmit delay, state, and priority.
`Designated Router`	Details of the designated router ID and interface address.
`Backup Designated Router ID`	Details of the backup router ID and interface address.
`Timer intervals configured`	Details of elapse time intervals for Hello, Dead, Transmit (wait), and retransmit.
`Neighbor Count`	Details the number of neighbors and adjacent neighbors.

Parameter	Description
`Tx Stat`	Counters and statistics for transmitted data. ■ **Hellos**: Number of transmitted hello packets. These packets are sent every hello interval. ■ **DbDescr**: Number of transmitted database description packets. ■ **LsReq**: Number of transmitted link state request packets. ■ **LsUpdate**: Number of transmitted link state update packets. ■ **LsAck**: Number of transmitted link state acknowledgment packets ■ **Pkts**: Total number of transmitted packets.
`Tx Err`	Counters and statistics for received data. ■ **Hellos**: Number of received hello packets. These packets are sent every hello interval. ■ **DbDescr**: Number of received database description packets. ■ **LsReq**: Number of received link state request packets. ■ **LsUpdate**: Number of received link state update packets. ■ **LsAck**: Number of received link state acknowledgment packets ■ **Pkts**: Total number of received packets.
`Rx Stat`	Counters and statistics for received data. ■ **Hellos**: Number of received hello packets. These packets are sent every hello interval. ■ **DbDescr**: Number of received database description packets. ■ **LsReq**: Number of received link state request packets. ■ **LsUpdate**: Number of received link state update packets. ■ **LsAck**: Number of received link state acknowledgment packets ■ **Pkts**: Total number of received packets.
`Rx Err`	Counters and statistics for received data. ■ **Hellos**: Number of received hello packets. These packets are sent every hello interval. ■ **DbDescr**: Number of received database description packets. ■ **LsReq**: Number of received link state request packets. ■ **LsUpdate**: Number of received link state update packets. ■ **LsAck**: Number of received link state acknowledgment packets ■ **Pkts**: Total number of received packets.
`DisCd`	Number of received packets that are discarded.
`BadVer`	Number of received packets that have bad OSPF version number.
`BadNet`	Number of received packets that belong to different network than the local interface.
`BadArea`	Number of received packets that belong to different area than the local interface.
`BadDstAdr`	Number of received packets that have wrong destination address.
`BadAuType`	Number of received packets that have different authentication type than the local interface.
`BadAuth`	Number of received packets where authentication failed.
`BadNeigh`	Number of received packets which didn’t have a valid neighbor.

Related Commands

Command	Description
interface vlan ip ospf	Configure OSPF on the interface.
router ospf	Configure OSPF on the router.

Command History

Release	Modification
ArubaOS 8.2.1.0	The **Tx Err** and **Rx Err** parameters were added to the output of the **show ip ospf interface vlan** command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ip pppoe-info

```
show ip pppoe-info
```

Description

This command displays the configuration settings for PPPoE.

Syntax

No parameters.

Examples

The following example displays the current PPPoE configuration.

```
(host) [mynode] #show ip pppoe-info

PPPoE username: rudolph123
PPPoE password: <HIDDEN>
PPPoE service name: ppp2056
PPPoE VLAN: 22
```

The output of this command includes the following parameters:

Parameter	Description
`PPPoE username`	PAP username configured on the PPPoE access concentrator.
`PPPoE password`	If this parameter displays the word **<HIDDEN>**, a PAP password is configured on the PPPoE access concentrator. If this parameter is **<NONE>**, there is no PPPoE password configured.
`PPPoE service name`	PPPoE service name.
`PPPoE VLAN`	VLAN configured to use PPPoE to obtain an IP address via the command **interface vlan <id> ip address pppoe.**

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ip probe

```
show ip probe
```

Description

This command displays the **health-check** profile settings for measuring WAN reachability and latency on a managed device uplink, and the **default** probe profile settings for PBR using next-hop lists.

Syntax

No parameters.

Usage Guidelines

The health-check feature uses ping or UDP probes for measuring WAN reachability and latency. PBR routing uses ping probes to determine the reachability of devices on a next-hop list. This command should be executed from the managed device only.

Examples

The following command displays the current IP probe settings for the **default** and **health-check** IP probe profiles.

```
(host-md) #show ip probe

IP Probe Entries
----------------
Name          Probe Mode  Frequency(in sec)  Retries  Burst size
----          ----------  -----------------  -------  ----------
default       Ping        10                 19       3
health-check  Ping        10                 3        5
```

The output of this command contains the following information:

Column	Description
`Name`	Name of the ip probe profile, which is either **default** or **health-check**.
`Probe Mode`	Indicates whether the probes are sent as ping or UDP packets.
`Frequency`	Probe interval, in seconds. The managed device sends the number of probes in the **Burst Size** column during each frequency interval.
`Retries`	Number of times the managed device attempts to resend a probe.
`Burst size`	Number of probes sent during the probe frequency interval that appears in the **Frequency** column.

Related Commands

Command	Description
ip probe default	This command configures IP probes for PBR using a next-hop list.
ip probe health-check	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show ip radius

```
show ip radius
   nas-ip
   source-interface
```

Description

This command displays global parameters for configured RADIUS servers.

Syntax

Command	Description
`nas-ip`	Show the Network Access Server (NAS) IP address attribute sent in outgoing RADIUS requests.
`source-interface`	Show the source interface address of outgoing RADIUS requests.

Examples

The following example displays the RADIUS client NAS IP address:

```
(host) [mynode] #show ip radius nas-ip
RADIUS client NAS IP address = 10.168.254.221
RADIUS client NAS IPv6 address = ::1
```

The following example displays the RADIUS client source interface address of the outgoing RADIUS requests:

```
(host) [mynode] #show ip radius source-interface
Global radius client source IP address = 12.0.2.26, vlan 3
Global radius client source IPv6 address = ::, vlan 0
Per-server client source IPv4/6 addresses:
```

Related Commands

Command	Description
ip radius	Configures global parameters for configured RADIUS servers.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ip route

```
show ip route
   counters
   static
   stats
```

Description

This command displays the Mobility Master routing table.

Syntax

Command	Description
`counters`	Displays the number of routes present, categorized by type.
`static`	Include this optional parameter to display only static routes.
`stats`	Displays route statistics.

Usage Guidelines

This command displays static routes configured on the Mobility Master using the ip route command. Use the ip default-gateway command to set the default gateway to the IP address of the interface on the upstream router or switch to which you connect Mobility Master.

Examples

The following example displays the IP address of routers and the VLANs to which they are connected:

```
(host) [mynode]#show ip route
M - mgmt, U - route usable, * - candidate default, V - RAPNG VPN/Branch
Gateway of last resort is Imported from DHCP to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from CELL to network 0.0.0.0 at cost 10
Gateway of last resort is Imported from PPPOE to network 0.0.0.0 at cost 10
Gateway of last resort is 10.7.73.77 to network 0.0.0.0 at cost 1
S*    0.0.0.0/0  [1/0] via 10.7.73.77*
S    172.0.0.0/8  [1/0] via 172.16.1.253*
```

Related Commands

Command	Description
ip default-gateway	Configures the default gateway for Mobility Master or the managed device.
ip route	Configures global parameters for configured RADIUS servers.

Command History

Release	Modification
ArubaOS 8.2.1.0	The order of displaying the administrative distance and cost was changed to **[AD/Cost]** from **[Cost/AD]** in the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ip tacacs

```
show ip tacacs
   source-interface
```

Description

This command displays global parameters for configured TACACS servers.

Syntax

Command	Description
`source-interface`	Shows the source interface address of outgoing TACACS requests.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

The following example displays the TACACS client source interface address of the outgoing TACACS requests:

```
(host) [mynode] #show ip tacacs source-interface
Global tacacs client source IP address = 0.0.0.0, vlan 0
Global tacacs client source IPv6 address = ::, vlan 0
Per-server client source IPv4/6 addresses:
```

Related Commands

Command	Description
ip radius	Configures global parameters for configured RADIUS servers.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipc statistics app-ap

```
show ipc statistics app-ap {am|ap-stm|ofald|sapd}
   ap-name <ap-name>
   bssid <bssid>
   ip-addr <ip-addr>
```

Description

This command displays the Inter Process Communication (IPC) statistics for a specific AP or BSSID.

Syntax

Parameter	Description
`am`	Show IPC statistics for an air monitor.
`ap-stm`	Show IPC statistics for AP station management communication.
`ofald`	OpenFlow Agent Lite Daemon. Show OpenFlow Agent statistics running on the AP.
`sapd`	Show IPC statistics for the AP management process on the AP.
`ap-name <ap-name>`	Show IPC statistics for an AP with a specific name.
`bssid <bssid>`	Show IPC statistics for a specific Basic Service Set Identifier (BSSID). An AP's BSSID is usually the AP's MAC address.
`ip-addr <ip-addr>`	Show IPC statistics for an AP with a specific IP address. Enter the IP address in dotted-decimal format.

Usage Guidelines

Execute this command under the supervision of Aruba TAC to troubleshoot application errors. This command should be executed on a standby controller or managed device where the APs terminate.

Example

The following example shows IPC statistics for the station management process on an AP named **corp-AP-115**.

```
(host-md) #show ipc statistics app-ap ap-stm ap-name corp-AP-115
IP: 168778491, IP_STR: 10.15.90.251

Local Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg  Rx Drop   Rx Err   Tx
Ack   Rx Silent Drops
SAPM Client              0        0        0        0        0       40        0        0
  0        0
Kernel PAPI Statistics
RxSockbufSize RxSockbufHimark CurRxQLen MaxRxQLen Drops
0                    0        0        0         0
Remote Device 10.15.88.100 Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg  Rx Drop   Rx Err   Tx
Ack   Rx Silent Drops
14302                    0        0        0        0        0        1        0        0
  1        0
Allocated Buffers   1
Static Buffers      4
```

```
Static Buffer Size  1400
```

The output of this command includes the following data columns:

Parameter	Description
`Tx Msg`	Number of transmitted messages.
`Tx Blk`	Number of blocking messages transmitted.
`Tx Ret`	Number of transmitted messages that were returned.
`Tx Fail`	Number of failure messages that were transmitted.
`Rx Ack`	Number of received acknowledgments.
`Rx Msg`	Number of received messages.
`Rx Drop`	Number of received messages that were dropped.
`Rx Err`	Number of received messages with errors.
`Tx Ack`	Number of transmitted acknowledgments.
`Allocated Buffers`	Number of allocated buffers for IPC messages.
`Static Buffers`	Number of static buffers for IPC messages.
`Static Buffer Size`	Size of the static buffer.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Managed Device

show ipc statistics app-id

```
show ipc statistics app-id <app-id>
```

Description

This command displays the Inter Process Communication (IPC) statistics for a specific AP or BSSID.

Syntax

Parameter	Description
`<app-id>`	Application ID number. This number must be obtained from Aruba TAC.

Usage Guidelines

Execute this command under the supervision of Aruba TAC to troubleshoot application errors.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master or Managed Device

show ipc statistics app-name

```
show ipc statistics app-name <name>
```

Description

Display Inter Process Communication (IPC) statistics for a specific application.

Syntax

Parameter	Description	
`<name>`	One of the following application names: ■ **aaa**: Administrator Authentication ■ **ads**: Anomaly Detection ■ **auth-resp**: Authentication Response ■ **authmgr**: User Authentication ■ **certmgr**: Certificate Manager ■ **cfgm**: Config Manager ■ **cluster_mgr**: Cluster Manager ■ **cpsec**: Control-Plane Security Manager ■ **cts**: Transport Service ■ **dbsync**: Database Synchronization ■ **dds**: Distributed data store ■ **dhcp**: DHCP Server ■ **esi**: Server Load Balancing ■ **extifmgr**: External Interface Manager ■ **fpapps**: Layer 2,3 control ■ **gsmmgr**: GSM manager ■ **ha_mgr**: HA manager ■ **httpd**: HTTPD ■ **ike**: IKE Daemon ■ **l2tp**: L2TP ■ **lagm**: LAGM ■ **licensemgr**: License Manager ■ **mdns**: AirGroup mdns ■ **mobileip**: Mobile IP	■ **ntp**: NTP Daemon ■ **ofa**: OpenFlow Agent ■ **ospf**: OSPF ■ **phonehome**: PhoneHome ■ **pim**: Protocol Independent Multicast ■ **pktfilter**: Packet Filter ■ **pptp**: PPTP ■ **profmgr**: Profile Manager ■ **publisher**: Publish subscribe service ■ **resolver**: Resolver ■ **sapm**: SAPM ■ **sapm-resp**: SAPM Response ■ **snmp**: SNMP agent ■ **stm**: Station Management ■ **stm-lopri**: Station Management Low Priority ■ **syslogd**: Syslog Manager ■ **ucm**: Unified Communication Manager ■ **userdb**: User Database Server ■ **vrrp**: VRRP ■ **web_cc**: Web Content Classification ■ **wms**: Wireless Management

Usage Guidelines

Execute this command under the supervision of Aruba TAC to troubleshoot application errors.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows IPC statistics for the **sapm** process.

To view the statistics of transmitted, received, and denied messages, three additional output parameters are introduced in the **show ipc statistics** command output.

- Tx Sign—the number of messages which were signed before transmitting
- Rx Sign—the number of messages validated through digest validation

- Rx Denied—the number of messages denied due to incorrect digest

```
(host) [mynode] #show ipc statistics app-name sapm
Local Statistics
To application     Tx Msg   Tx Blk  Tx Ret Tx Fail  Rx Ack Rx Msg Rx Drop
Layer2/3                4        0       0       0       0      2    0
Multicast DNS Lis       0        0       0       0       0      3    0
License Manager         2        2       0       0       2      2    0
Profile Manager         1        0       0       0       1      1    0
NEW_CLI_START           2        0       0       0       2      3    0
Authentication          0        0       0       0       0      1    0
Syslog Manager          4        4       0       0       4      0    0
Configuration Man       3        0       0       0       0     19    0
     Rx Err   Tx Ack   Tx Sign   Rx Sign   Rx Denied Rx Silent Drops
         0        0         0         0           0      0
         0        0         0         0           0      0
         0        0         0         0           0      0
         0        0         0         0           0      0
         0        0         0         0           0      0
         0        0         0         0           0      0
         0        0         0         0           0      0
         0        0         0         0           0      0
Kernel PAPI Statistics
RxSockbufSize RxSockbufHimark CurRxQLen MaxRxQLen Drops
16777216               1152        0        1         0
Remote Device 10.4.176.95 Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg
SAPM                  2565        0        0        0        0     2667
Rx Drop   Rx Err  Tx Ack  Tx Sign   Rx Sign  Rx Denied  Rx Silent Drops
     0         0       0         0         0         0           0

Remote Device 172.200.13.3 Statistics
To application      Tx Msg   Tx Blk   Tx Ret  Tx Fail   Rx Ack   Rx Msg
SAPM                  2569        0        0        0        0     2569
Rx Drop   Rx Err   Tx Ack  Tx Sign   Rx Sign  Rx Denied Rx Silent Drops
     0         0        0         0         0         0         0
Allocated Buffers   4
Static Buffers      0
Static Buffer Size  1476
```

The output of this command includes the following data columns:

Parameter	Description
Tx Msg	Number of transmitted messages.
Tx Blk	Number of blocking messages transmitted.
Tx Ret	Number of transmitted messages that were returned.
Tx Fail	Number of failure messages that were transmitted.
Rx Ack	Number of received acknowledgments.
Rx Msg	Number of received messages.
Rx Drop	Number of received messages that were dropped.
Rx Err	Number of received messages with errors.

Parameter	Description
`Tx Ack`	Number of transmitted acknowledgments.
`Tx Sign`	Number of messages which were signed before transmitting.
`Rx Sign`	Number of messages validated through digest validation.
`Rx Denied`	Number of messages denied due to incorrect digest.
`Rx Silent Drops`	Number of received messages that are categorized as silent drops.
`Allocated Buffers`	Number of allocated buffers for IPC messages.
`Static Buffers`	Number of static buffers for IPC messages.
`Static Buffer Size`	Size of the static buffer.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **lagm** and **vrrp** parameters were added.
ArubaOS 8.0.1.0	**Tx Sign**, **Rx Sign**, and **Rx Denied** columns are added to the command output.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master or Managed Device

show ipstm

```
show ipstm debug stats
```

Description

This command displays the debug messages for the IPsec tunnel manager.

Syntax

No parameters.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv4 user-table

```
show ipv4 user-table
   ap-group <ap-group>
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   ap-name <ap-name>
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   authentication-method {dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web}
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   bssid <A:B:C:D:E:F>
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   debug
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   essid <STRING>
      ip
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   internal
      rows <start-row> <no-of-rows>
   ip <addr> [log]
   mac <A:B:C:D:E:F>
   mobile
      bindings [<start-row> <no-of-rows>|unique [rows <start-row> <no-of-rows>]]
      rows <start-row> <no-of-rows>
      unique
         bindings [<start-row> <no-of-rows>|unique [rows <start-row> <no-of-rows>]]
         rows <start-row> <no-of-rows>
         visitors [rows <start-row> <no-of-rows>]
      visitors [<start-row> <no-of-rows>|unique [rows <start-row> <no-of-rows>]]
   name <STRING> [unique]
   phy-type {[a]|[b]}
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   role <STRING>
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
   rows <start-row> <no-of-rows>
   station
   verbose
      rows <start-row> <no-of-rows>
      unique [rows <start-row> <no-of-rows>]
```

Description

This command displays the IPv4 user table entries. You can filter the output based on various parameters described in the following table.

Syntax

Parameter	Description
`ap-group <ap-group>`	Filter the output of this command by showing users connected to APs that belong to the specified AP group.

Parameter	Description
ap-name <ap-name>	Filter the output of this command by showing users connected to an AP with the specified AP name.
authentication-method	Filter the output of this command by the authentication method used for the device:
dot1x	Filer the output of this command by showing data for devices using the 802.1X authentication.
mac	Filer the output of this command by showing data for devices using the MAC authentication.
opensystem	Filer the output of this command by showing data for devices using the open (no) authentication.
psk	Filer the output of this command by showing data for devices that do not use authentication but use a PSK for encryption.
stateful-dot1x	Filer the output of this command by showing data for devices using stateful 802.1X authentication.
via-vpn	Filer the output of this command by showing data for devices that authenticate using VIA.
vpn	Filer the output of this command by showing data for devices using VPN authentication.
web	Filer the output of this command by showing data for devices using the Captive Portal authentication.
bssid	Filer the output of this command by showing users connected to the specified BSSID.
debug	Filer the output of this command by showing entries in the IPv4 user-table that are in debug mode.
essid	Filer the output of this command by showing entries in the IPv4 user table that are associated to the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
internal	Filer the output of this command by showing internal IPv4 users.
ip <A.B.C.D>	Filer the output of this command by showing IPv4 users that match the specified IPv4 address.
log	Filer the output of this command by showing the log information for the specified IPv4 client.
mac	Filer the output of this command by showing users with the specified MAC address.

Parameter	Description
mobile	Filer the output of this command by showing a list of mobile users in the IPv4 user table. The following filters are available for this parameter: ■ **bindings**—List of users that have moved away from the current managed device. ■ **rows**—Displays entries that match the specified row number. ■ **unique**—Displays unique entries in the IPv6 user-table. ■ **visitors**—Displays users that have associated with the current managed device.
name	Filer the output of this command by showing IPv4 user table entries that match the specified name.
phy-type	Filer the output of this command by showing IPv4 user table entries that match **a** or **b** phy-type.
role	Filer the output of this command by showing IPv4 user table entries that match the specified role.
rows	Filer the output of this command by showing specific rows in the IPv4 user table. Enter the starting row number and the number of rows to be displayed.
station	Filer the output of this command by showing the station table information for the IPv4 user table entries.
verbose	Filer the output of this command by showing the complete IPv4 user table with all details.

Usage Guidelines

This command should be executed from the managed device only where the APs and client terminate.

Example

The following example displays a list of internal IPv4 user entries:

```
(host-md) #show ipv4 user-table

IP                MAC               Name      Role              Age(d:h:m)  Auth
----------       ------------       ------    ----              ----------  ----
192.168.201.234  00:10:18:a9:38:e1  uccsol10  ucc-dot1x-voice   00:22:14    802.1X
192.168.201.230  5c:c5:d4:7d:c0:80  uccsol23  ucc-dot1x-voice   00:02:59    802.1X
192.168.201.252  48:51:b7:19:40:88  uccsol19  ucc-dot1x-voice   00:22:14    802.1X
192.168.201.241  5c:c5:d4:7d:c2:b5  uccsol24  ucc-dot1x-voice   00:02:59    802.1X
192.168.201.233  5c:c5:d4:7d:c0:b7  uccsol22  ucc-dot1x-voice   00:02:29    802.1X

VPN link  AP name   Roaming   Essid/Bssid/Phy                    Profile    Forward mode
--------  -------   -------   ---------------                    -------    ------------
          115-1     Wireless  UCC-DOT1X/ac:a3:1e:27:e4:b1/a-HT   UCC-DOT1X  dtunnel
          325-1     Wireless  UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X  dtunnel
          325-1     Wireless  UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X  dtunnel
          325-1     Wireless  UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X  dtunnel
          325-1     Wireless  UCC-DOT1X/ac:a3:1e:57:6d:90/a-VHT  UCC-DOT1X  dtunnel

Type  Host Name
----  ---------



User Entries: 5/5
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of the client in that row that authenticating using 802.1X authentication.
MAC	MAC address of the client.
Name	Name of the client.
Role	The role assigned to the client.
Age (d:h:m)	Total time that client is connected to managed device.
Auth	Authentication type of the client.
VPN link	Clients using VPN authentication.
AP name	Name of the AP associated with the client.
Roaming	Current roaming status of the client.
Essid/Bssid/Phy	ESSID, BSSID, and Phy to which the client is associated.
Profile	The AAA profile to which the client is associated.
Forward Mode	The client traffic forwarding mode.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable mode on Managed Device.

show ipv6 dhcp

```
show ipv6 dhcp
   binding
   database [pool<pool_name>]
```

Description

Shows DHCPv6 server settings.

Syntax

Parameter	Description
`binding`	Show DHCPv6 server bindings.
`database`	Show DHCPv6 server settings.

Examples

The example below shows the DHCPv6 database:

```
(host) [mynode] #show ipv6 dhcp database
DHCPv6 enabled
# 2001-feed-64-nw
subnet6 2001:feed::/120 {
        option vendor-class-identifier  "ArubaAP";
        option dhcp6.vendor-opts  "2001:feed::235";
        range6 2001:feed::1 2001:feed::234;
        range6 2001:feed::236 2001:feed::ffff:ffff:ffff:fffe;
}
# 2003-feed-64-nw
subnet6 2003:feed::/120 {
        option vendor-class-identifier  "ArubaAP";
        option dhcp6.vendor-opts  "2001:feed::235";
        range6 2003:feed::1 2003:feed::234;
        range6 2003:feed::236 2003:feed::ffff:ffff:ffff:fffe;
}
# DHCPv6
subnet6 2001:470:faca:4::/120 {
        default-lease-time 43200;
        max-lease-time 43200;
        option dhcp6.domain-search "test.org";
        option vendor-class-identifier  "ArubaAP";
        option dhcp6.vendor-opts  "2001:feed::235";
        option dhcp6.name-servers 2001:470:20::2;
        option dhcp6.preference 25;
        option dhcp6.usr-opt-24-DHCPv6 "Domain Search List";
        range6 2001:470:20::1 2001:470:faca:4::1;
        range6 2001:470:20::3 2001:470:faca:4:ffff:ffff:ffff:fffe;
}
```

The example below shows the DHCPv6 database for a specific pool:

```
(host) [mynode] #show ipv6 dhcp database [pool <pool-name>]
(host) [mynode] #show ipv6 dhcp database pool DHCPv6

# DHCPv6
subnet6 2001:470:faca:4::/120 {
        default-lease-time 43200;
```

```
        max-lease-time 43200;
        option dhcp6.domain-search "test.org";
        option vendor-class-identifier  "ArubaAP";
        option dhcp6.vendor-opts  "2001:feed::235";
        option dhcp6.name-servers 2001:470:20::2;
        option dhcp6.preference 25;
        option dhcp6.usr-opt-24-DHCPv6 "Domain Search List";
        range6 2001:470:20::1 2001:470:faca:4::1;
        range6 2001:470:20::3 2001:470:faca:4:ffff:ffff:ffff:fffe;
}
```

The example below shows the DHCPv6 binding information:

```
(host) [mynode] # show ipv6 dhcp binding
# Client: fe80::1cf:2e1:cd13:356b; IA ID 0x13001f3c
ia-na "\023\000\037<\000\001\000\001\030\223\211\242\000%\263J\372\364" {
cltt epoch 1364206514; # Mon Mar 25 15:45:14 2013
iaaddr 2001:470:faca:4:21a:1eff:fe00:9e6 {
binding state expired;
preferred-life 187;
max-life 300;
ends epoch 1364206814; # Mon Mar 25 15:50:14 2013
}
```

The example below shows the DHCPv6 active pools:

```
(host) [mynode] #show ipv6 dhcp active-pools
DHCPv6 Active Pools
-------------------
Vlan Pool Name
---- ---------
10   DHCPv6
```

Related Commands

Command	Description
ipv6 dhcp pool	This command configures a DHCPv6 pool on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 firewall

```
show ipv6 firewall
```

Example

This example displays the status of all firewall configurations.

```
(host) [mynode] #show ipv6 firewall

Global IPv6 firewall policies
-----------------------------
Policy                                      Action    Rate       Port
------                                      ------    ----       ----
Monitor ping attack                         Disabled
Monitor TCP SYN attack                      Disabled
Monitor IPv6 sessions attack                Disabled
Deny inter user bridging                    Disabled
Drop all IPv6 fragments                     Disabled
Per-packet logging                          Disabled
Enforce TCP handshake before allowing data  Disabled
Prohibit RST replay attack                  Disabled
Session Idle Timeout                        Disabled
Prohibit IPv6 Spoofing                      Disabled
Extension header parse length               Enabled   100 bytes
Stateful ICMP Processing                    Disabled
```

The output of this command includes the following parameters:

Parameter	Description
`Monitor ping attack`	If enabled, the managed device monitors the number of ICMP pings per second. If this value exceeds the maximum configured rate, the managed device will register a DoS attack.
`Monitor TCP SYN attack`	If enabled, the managed device monitors the number of TCP SYN messages per second. If this value exceeds the maximum configured rate, the managed device will register a DoS attack.
`Monitor IPv6 sessions attack`	If enabled, the managed device monitors the number of TCP session requests per second. If this value exceeds the maximum configured rate, the managed device will register a DoS attack sessions.
`Deny inter user bridging`	If enabled this setting prevents the forwarding of Layer-2 traffic between wired or wireless users. You can configure user role policies that prevent Layer-3 traffic between users or networks but this does not block Layer-2 traffic.
`Drop all IPv6 fragments`	If enabled, all IPv6 fragments are dropped.
`Per-packet logging`	If active, and logging is enabled for the corresponding session rule, this feature logs every packet.

Parameter	Description
`Enforce TCP handshake before allowing data`	If enabled, this feature prevents data from passing between two clients until the three-way TCP handshake has been performed. Enabling this option causes mobility to fail. So, disable this option if you have mobile clients on the network as.
`Prohibit RST replay attack`	If enabled, this setting closes a TCP connection in both directions if a TCP RST is received from either direction.
`Session Idle Timeout`	Shows if a session idle timeout interval has been defined.
`Prohibit IPv6 Spoofing`	Status on IPv6 spoofing. When this option is enabled, IP and MAC addresses are checked; possible IP spoofing attacks are logged and an SNMP trap is sent.
`Extension header parse length`	Shows the extension header parse length, with a maximum value of 100 bytes.
`Stateful ICMP Processing`	If enabled, stateful ICMP processing is enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 global

```
show ipv6 global
```

Description

Displays IPv6 global config information.

Example

The following example displays the global status of the IPv6 packet.

```
(host) [mynode] #show ipv6 global
Global IPv6 Packet Processing is Enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master.

show ipv6 interface

```
show ipv6 interface [brief]
```

Description

View IPv6-related information on all interfaces.

Syntax

Parameter	Description
`brief`	Optional parameter. If specified, displays the IPv6-related information on all the interfaces in a summary format.

Example

```
(host) [mynode] #show IPv6 interface
VLAN1 is up line protocol is down
IPv6 Router Advertisements are disabled
IPv6 is disabled
VLAN46 is up line protocol is up
IPv6 is enabled, link-local address is fe80::1a:1e00:2e00:9f0
Global unicast address(es):
2046:eab::25, subnet is 2046:eab::/64
IPv6 Router Advertisements are disabled
VLAN50 is up line protocol is up
IPv6 Router Advertisements are disabled
IPv6 is disabled
VLAN10 is up line protocol is up
IPv6 is enabled, link-local address is fe80::1a:1e00:a00:9f0
Global unicast address(es):
2010:eab::1, subnet is 2010:eab::/64
fc01:eab::1, subnet is fc01:eab::/64
IPv6 Router Advertisements are enabled
loopback is up line protocol is up
IPv6 is enabled, link-local address is fe80::1a:1e0f:ff00:9f0
Global unicast address:
2046:eab::2, subnet is 2046:eab::2/128
TUNNEL2 is up line protocol is up
tunnel mode is Layer2 IPv6 GRE, tunnel vlan 10
tunnel source ipv6 address is 2046:eab::25
tunnel destination ipv6 address is 2047:eab::25

(host) [mynode] #show ipv6 interface brief
Interface                    [Status/Protocol]
vlan 800                     [  up/up   ]
  unassigned
vlan 1                       [  up/down]
  unassigned
vlan 802                     [  up/up   ]
  fe80::b:8603:226d:863c/64
  2082::802:1/64
vlan 32                      [  up/up   ]
  unassigned
vlan 801                     [  up/up   ]
  fe80::b:8603:216d:863c/64
  2005:81::1/64
vlan 50                      [  up/down]
```

```
  fe80::b:8600:326d:863c/64
  2050:3::50:1/64
loopback                    [  up/up  ]
  fe80::b:860f:ff6d:863c/64
mgmt                        [down/down]
  unassigned
tunnel 2                    [  up/up  ]
  unassigned
```

The following table details the columns and content in the show command.

Column	Description
`Interface`	List the interface and interface identification with the IPv6 address and netmask for the interface, if configured.
`Status/Protocol`	States the administrative status and the IPv6 status on the interface. Enabled—up Disabled—down

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master.

show ipv6 mld cluster

```
show ipv6 mld cluster
   aac-info
   bss-info
   client-info
   dmo-off-info
   info
   proxy-group
   stats
```

Description

Display MLD configuration details for a cluster.

Syntax

Parameter	Description
`aac-info`	Show cluster AAC information of APs.
`bss-info`	Show IGMP BSS information.
`client-info`	Show IGMP cluster client information.
`dmo-off-info`	Show list of (S,G,BSS) where DMO threshold is hit.
`info`	Show cluster information.
`proxy-group`	Show IGMP cluster proxy database group information.
`stats`	Show cluster statistics.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on managed device.

show ipv6 mld config

```
show ipv6 mld config
```

Description

Displays MLD configuration details.

Example

This example displays the current MLD configuration values.

```
(host) [mynode] #show ipv6 mld config

MLD Config
----------
Name                      Value
----                      -----
robustness-variable       2
query-interval            125
query-response-interval   100
ssm-range                 FF3X::4000:1 - FF3X::FFFF:FFFF
```

The output of this command includes the following parameters:

Parameter	Description
`robustness-variable`	Denotes the value that is used to calculate the timeout value of an MLD client.
`query-interval`	Denotes the time interval at which the MLD query is sent.
`query-response-interval`	Denotes the time interval at which the MLD query response should be received.
`ssm-range`	Denotes the source specific multicast range. When you enter the SSM Range ensure that the upstream router has the same range, else the multicast stream would be dropped. **NOTE:** Only SSM enabled clients can subscribe to the multicast stream in the multicast range. The default ssm-range in case of IPv6 is FF3X::4000:1 - FF3X::FFFF:FFFF, this range is configurable. If MLDv1 or a non SSM client sends a report on a specified SSM range, it is rejected by the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 mld counters

```
show ipv6 mld counters
```

Description

Displays the statistics of MLD.

Example

This example displays the MLD statistics for the following values.

```
(host) [mynode] #show ipv6 mld counters

MLD Statistics
--------------
Name                    Value
----                    -----
received-total          0
received-queries        0
received-v1-reports     0
received-v1-leaves      0
received-v2-reports     0
received-unknown-types  0
len-errors              0
checksum-errors         0
not-vlan-dr             0
transmitted-queries     0
forwarded               0
non-conforming-mld      0
```

The output of this command includes the following parameters:

Parameter	Description
`received-total`	The total number of MLD messages.
`received-queries`	The total number of MLD queries.
`received-v1-reports`	The total number of MLD v1 reports received.
`received-v1-leaves`	The total number of MLD v1 leave messages received.
`received-v2-reports`	The total number of MLD v2 reports received.
`received-unknown-types`	The total number of unrecognized messages received.
`len-errors`	The total number of error message where the length check has failed.
`checksum-errors`	The total number of error message where the checksum has failed.
`not-vlan-dr`	The number of messages received for which the current managed device is not the designated router.
`transmitted-queries`	The total number of transmitted MLD queries.
`forwarded`	The total number of MLD messages forwarded.
`non-conforming-mld`	The total number of non confirming MLD messages.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 mld group

```
show ipv6 mld group
```

Example

This example displays MLD group details.

```
(host) [mynode] #show ipv6 mld group

MLD Group Table
---------------
Group               Members  Mode     Age
-----               -------  ----     ---
ff02::1:ff00:0      2        Exclude  4
ff02::1:ff00:1900   2        Exclude  1
ff1e::2             2        Include  0
ff02::1:3           4        Exclude  1
ff02::202           2        Exclude  4
ff02::2             3        Exclude  1
ff02::1:ff20:d6e2   2        Exclude  4
ff02::c             4        Exclude  2
ff02::1:ffab:4027   2        Exclude  6
ff02::d             2        Exclude  1
ff02::1:ff00:12     2        Exclude  4
ff02::1:ffd6:4d41   1        Exclude  7
ff02::16            2        Exclude  1
ff02::1:ffd6:4d40   1        Exclude  1
ff02::1:ff8a:4951   2        Exclude  4
ff02::1:ff5b:aac4   2        Exclude  11
ff02::1:ff9f:df01   2        Exclude  3
Total Groups: 17
```

The output of this command includes the following parameters:

Parameter	Description
`Group`	Name of MLD groups.
`Members`	Number of members in an MLD group.
`Mode`	Managed device supports two IPv6 multicast source filtering modes - Include and Exclude. In Include mode, the reception of packets sent to a specified multicast address is enabled only from the source addresses listed in the source list. In Exclude mode, the reception of packets sent to a specific multicast address is enabled from all source addresses (MLDv1 mode).
`Age`	This parameter specifies the aging time.

This example displays MLD group address details.

```
(host) [mynode] #show ipv6 mld group maddr ff1e::2 mac 9c:b7:0d:3f:a8:fc

MLD member 9c:b7:0d:3f:a8:fc Table
----------------------------------
Source        Age
------        ---
2001:feed::2  26
```

The output of the `show ipv6 mld group` command includes the following parameters:

Parameter	Description
`Source`	IP address of the multicast source.
`Age`	This parameter specifies the aging time.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 mld interface

```
show ipv6 mld interface
```

Example

This example displays MLD status on VLANs. To view details for a specific VLAN, you can specify the VLAN ID.

```
(host) [mynode] #show ipv6 mld interface

MLD Interface Table
-------------------
VLAN  Link local address  Snooping  Proxy     Querier  Querier-dest  Upstream querier
Upstream port
----  ------------------  --------  -----     -------  ------------  ----------------  -------
------
1     ::                  disabled  disabled  ::       unknown       ::                -
160   ::                  disabled  disabled  ::       unknown       ::                -
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	Denotes the VLAN ID.
Link local address	IP address of the VLAN interface.
Snooping	Status of MLD snooping.
Proxy	Status of MLD proxy configuration.
Querier	IPv6 address of the MLD querier for the VLAN.
Querier-dest	Denotes the destination of MLD querier on VLAN.
Upstream querier	Denotes the address of upstream MLD querier on VLAN.
Upstream port	Denotes the destination of upstream MLD querier on VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 mld proxy-group

```
show ipv6 mld proxy-group [vlan <vlan>]
```

Example

This example displays MLD proxy-group details.

```
(host) [mynode] #show ipv6 mld proxy-group
MLD Proxy Group Table
---------------------
VLAN  Addr                    Group              Num Members
----  ----                    -----              -----------
10    fe80::b:8600:a61:cc5c   ff1e::5            2
10    fe80::b:8600:a61:cc5c   ff02::1:ff9e:dc4c  1
10    fe80::b:8600:a61:cc5c   ff02::1:3          2
10    fe80::b:8600:a61:cc5c   ff02::1:ff83:d718  1
10    fe80::b:8600:a61:cc5c   ff02::1:ff13:356b  1
10    fe80::b:8600:a61:cc5c   ff02::c            2
Total displayed proxy groups: 6
```

The output of this command includes the following parameters:

Parameter	Description
VLAN	Denotes the VLAN ID.
Addr	IP address of the VLAN interface.
Group	Name of MLD group.
Num Members	Number of members in an MLD group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 mld proxy-stats

```
show ipv6 mld proxy-stats
```

Example

This example displays the status of the MLD proxy.

```
(host) [mynode] #show ipv6 mld proxy-stats
MLD Proxy Statistics(Upstream)
------------------------------
Name      Sent  Received
----      ----  --------
Queries   -     39
Joins     51    112
Leaves    9     0
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Type of packet.
`Sent`	Number of packets sent.
`Received`	Number of packets received.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show ipv6 mld proxy-mobility-group

```
show ipv6 mld proxy-mobility-group [maddr <maddr>]
```

Example

This example displays MLD proxy-mobility-group details.

```
(host) [mynode] #show ipv6 mld proxy-mobility-group
MLD MIP Group Table
-------------------
Group      Members
-----      -------
ff1e::2     1
ff02::1:3   2
ff02::c     1
```

The output of this command includes the following parameters:

Parameter	Description
`Group`	Name of MLD mobility group.
`Members`	Number of members in an MLD mobility group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 mld proxy-mobility-stats

```
show ipv6 mld proxy-mobility-stats
```

Example

This example displays the details of MLD proxy-mobility statistics.

```
(host) [mynode] #show ipv6 mld proxy-mobility-stats

MLD Mobility Multicast Statistics
---------------------------------
Name               Sent  Received
----               ----  --------
Joins              -     2
Leaves             -     0
Intra-move         -     1
Inter-move         -     0
Client-away        -     0
Back-home          -     0
Query-db           -     0
Query-foreign-db   -     0
Query-home-db      -     0
Add-visitor        -     0
Replies            0     -
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Type of packet.
`Sent`	Number of packets sent.
`Received`	Number of packets received.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show ipv6 neighbors

```
show ipv6 neighbors
```

Description

Displays the IPv6 neighbors configured on a VLAN interface.

Usage Guidelines

This command displays the IPv6 neighbors configured on a VLAN interface via the ipv6 neighbor command.

Examples

The example below shows the ipv6 neighbors configured on VLAN 1 .

```
(host) [mynode] #show ipv6 neighbors vlan 1

IPv6 Neighbors
--------------
IPv6 Address           Age  Link-layer Addr    State      Interface
------------           ---  ---------------    -----      ---------
2cce:205:160:100::fe   -    00:0b:86:61:13:28  PERMANENT  vlan 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master.

show ipv6 pd status

```
show ipv6 pd status
```

Description

Displays the prefix obtained by the PD client on uplink.

Example

The following example displays the status of the IPv6 prefix deligation.

```
(host)[mynode] #show ipv6 pd status
DHCPv6 PD Client is enabled
Uplink VLAN     : 100
Label           : site1
Prefix          : 2001:0:3::/48
65536 unique /64 prefixes are derivable from the acquired IA PD lease
Preferred lifetime 604800s, Valid lifetime 2592000s
Last request/renewal for the lease done at Thu Apr 14 04:46:15 2016
Lease expires at Sat May 14 04:46:15 2016
Downlink VLANs
--------------
VlanId  Prefix
------  ------
101      2001:0:3:12:1:2:3:4/64
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master.

show ipv6 ra

```
show ipv6 ra [proxy | status]
```

Description

Displays the RA proxy server information and IPv6 RA.

Examples

The example below shows the IPv6 RA status on the VLAN interfaces .

```
(host) [mynode] #show ipv6 ra status

IPv6 RA Status
--------------
VlanId  State    Prefix(es)
------  -----    ----------
1       enabled  2001:abcd:1234:dead::/64
220     enabled  2200:eab:feed:12::/64
230     enabled  2300:eab:feed::/64
7       enabled  2001:470:faca:2::/64
                 2001:470:faca:3::/64
                 2001:470:faca:4::/64
```

The example below shows the status of the IPv6 proxy RA:

```
(host) #show ipv6 ra proxy
IPv6 RA Proxy status: enabled
IPv6 RA Proxy interval: 600
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **proxy** parameter was introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master.

show ipv6 route

```
show ipv6 route [counters | static]
```

Description

Displays the IPv6 routing table.

Syntax

Command	Description
`counters`	Displays the number of routes present, categorized by type.
`static`	Include this optional parameter to display only static IPv6 routes.

Usage Guidelines

This command displays static IPv6 routes configured on the managed device via the ipv6 route command. Use the ipv6 default-gateway command to set the default gateway to the IPv6 address of the interface on the upstream router or switch to which you connect the managed device.

Examples

The examples below show the ipv6 address of routers and the VLANs to which they are connected.

```
(host) [mynode] #show ipv6 route
Codes: C - connected, O - OSPF, R - RIP, S - static
       M - mgmt, U - route usable, * - candidate default

Gateway of last resort is 2001::3 to network ::/128 at cost 1
S*    ::/0 [1/0] via 2001::3*
C    2001::/64 is directly connected, VLAN1
C    2010:abcd:1234:dead::/64 is directly connected, VLAN10

(host) [mynode] #show ipv6 route static
Gateway of last resort is 2001::3 to network ::/128 at cost 1
S*    ::/0 [1/0] via 2001::3*
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master.

show ipv6 user-table

```
show ipv6 user-table
   ap-group <ap-group>
   ap-name <ap-name>
   authentication-method <dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web>
   bssid <A:B:C:D:E:F>
   debug
   essid <STRING>
   internal
   ip <A.B.C.D> [log]
   mac <A:B:C:D:E:F>
   mobile {[bindings][visitors]}
   name <STRING>
   phy-type {[a]|[b]}
   role <STRING>
   rows <NUMBER> <NUMBER>
   station <rows|unique>
   verbose <rows|unique>
```

Description

Displays IPv6 user table entries. You can filter the output based on various parameters are described in table.

Syntax

Parameter	Description
`ap-group <ap-group>`	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
`ap-name <ap-name>`	Filter the output of this command by showing users connected to an AP with the specified AP name.
`authentication-method`	Filter the output of this command by the authentication method used for the device:
`dot1x`	Show data for devices using 802.1X authentication.
`mac`	Show data for devices using MAC authentication.
`opensystem`	Show data for devices using open (no) authentication.
`psk`	Show data for devices that do not use authentication but use a PSK for encryption.
`stateful-dot1x`	Show data for devices using stateful 802.1X authentication.
`via-vpn`	Show data for devices that authenticate using Aruba VIA.
`vpn`	Show data for devices using VPN authentication.
`web`	Show data for devices using captive portal authentication.
`bssid`	Displays entries in the IPv6 user-table that are associated to the specified BSSID.

Parameter	Description
debug	Displays entries in the IPv6 user-table that are in debug mode.
essid	Displays entries in the IPv6 user-table that are associated to the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
internal	Displays internal IPv6 users.
ip <A.B.C.D>	Displays IPv6 users that match the specified IPv6 IP address.
log	Displays the log information for the specified IPv6 client.
mac	Displays users with the specified MAC address.
mobile	Displays list of mobile users in the IPv6 user table. The following filters are available for this parameter: ■ **bindings**—list of users that have moved away from the current controller. ■ **rows**—displays entries that match the specified row number. ■ **unique**—displays unique entries in the IPv6 user-table. ■ **visitors**—displays users that have associated with the current controller.
name	Displays IPv6 user table entries that match the specified name.
phy-type	Displays IPv6 user table entries that match **a** or **b** phy-type.
role	Displays IPv6 user table entries that match the specified role.
rows	Displays specific rows in the IPv6 user table. Enter the starting row number and the number of rows to be displayed.
station	Displays the station table information for the IPv6 user table entries.
verbose <rows|unique>	Displays the complete IPv6 user table with all details.

Example

This example displays a list of users.

```
(host) [mynode] #show ipv6 user-table
Users
-----
IP                                MAC                Name     Role      Age(d:h:m)  Auth    VPN
link  AP name  Roaming  Essid/Bssid/Phy                      Profile  Forward mode  Type
Host Name
----------                      ------------       ------    ----      ----------  ----    ----
----  -------  -------  ---------------                     -------  ------------  ----
---------
2010:eab::59ee:264a:a702:ca57  c0:14:3d:d9:e2:1b  salz      guest     00:04:30    802.1X
     AP-105   Away     IPv6-dot1x-7220/00:24:6c:11:88:40/g-HT  default  tunnel        Win 7
User Entries: 1/1
```

This example displays 802.1X authenticated users in the IPv6 user table.

```
(host) [mynode] #show ipv6 user-table authentication-method dot1x

Users
-----
    IP                                  MAC                Name     Role      Age(d:h:m)
Auth    VPN link  AP name            Roaming   Essid/Bssid/Phy             Profile
----------                             ------------       ------    ----      ----------  --
--    --------  -------           -------   ---------------           -------
```

```
fe80::216:ceff:fe2c:b485                  00:16:ce:2c:b4:85  Wing-A   logon     00:00:06
802.1X           00:0b:86:c1:0e:8c  Wireless  Wing-A/00:0b:86:90:e8:c0/g  default-dot1x
2003:d81f:f9f0:1001:617c:9151:6d25:f754  00:16:ce:2c:b4:85  Wing-A   logon     00:00:06
802.1X           00:0b:86:c1:0e:8c  Wireless  Wing-A/00:0b:86:90:e8:c0/g  default-dot1x
```

The output of this command includes the following parameters:

Parameter	Description
IP	IP address of the client in that row that authenticating using 802.1X
MAC	MAC address of the client.
Name	Name of the client.
Role	The role assigned to the client.
Age(d:h:m)	Total time that client is connected to controller.
Auth	Authentication type.
AP name	Name of the AP associated with the client.
Roaming	Current roaming status of the client.
Essid/Bssid/Phy	ESSID or BSSID or Phy to which the client is associated.
Profile	Displays the AAA profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Enable or Config mode on Mobility Master.

show jitter

```
show jitter <probe_ip> <src_intf>
```

Description

This command displays the debug messages for the IPsec tunnel manager.

Syntax

Command	Description
<probe_ip>	IP address of a remote host to which the managed device is connected.
<src_intf>	Source interface VLAN of a remote host to which the managed device is connected.

Usage Guidelines

This command should be executed from the managed device only.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Managed Device

show keys

```
show keys [all]
```

Description

This command displays if optional keys and features are enabled or disabled on Mobility Master.

Syntax

Parameter	Description
`all`	Include this optional parameter to display the status of all optional keys and features. If this parameter is omitted, the output displays the status of the most commonly used features and keys.

Example

The following example displays the status of the most commonly used keys and features on Mobility Master:

```
(host) [mynode] #show keys all

Licensed Features
-----------------
Feature                                                 Status
-------                                                 ------
Access Points                                           10240
MUXes                                                   Unlimited
External Servers                                        Unlimited
xSec Users                                              Unlimited
CIM Users                                               Unlimited
Contexts                                                Unlimited
3rd-party Remote APs                                    Unlimited
RF Protect                                              0
VPN Server Module                                       16384
xSec Module                                             0
Application-Acceleration Remote APs                     Unlimited
Next Generation Policy Enforcement Firewall Module      10240
Advanced Cryptography                                   0
WebCC                                                   10240
Beta AP                                                 0
MM                                                      0
WLAN Switch                                             ENABLED
RF Protect                                              ENABLED
RF Director                                             ENABLED
Policy Enforcement Firewall                             ENABLED
Auto Radio Resource Alloc                               ENABLED
Adaptive Radio Management                               ENABLED
VPN Server                                              ENABLED
Wired 802.1X                                            ENABLED
Secure Access                                           ENABLED
Wired Grid Points                                       ENABLED
xSec Module                                             ENABLED
Remote AP VPN Termination                               ENABLED
Location API                                            DISABLED
Mesh Visualization                                      DISABLED
Power Over Ethernet                                     DISABLED
Application Acceleration                                DISABLED
Centralized Encryption                                  DISABLED
```

```
Policy Enforcement Firewall for VPN users          DISABLED
Advanced Cryptography                              ENABLED
Maritime Regulatory Domain                         DISABLED
X86 VM SKU Activate                                DISABLED
WebCC                                              ENABLED
Beta AP                                            DISABLED
```

Related Commands

Command	Description
show license	View the license usage database (including the license key strings).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show lacp

```
show lacp
   sys-id
   <id> {counters|internal|neighbor}
```

Description

This command displays the Link Aggregation Control Protocol (LACP) configuration status.

Syntax

Parameter	Description
sys-id	LACP system ID.
<id>	Group ID. Range is 0-7.
counters	Enter the keyword **counters** to view the LACP traffic.
internal	Enter the keyword **internal** to view the LACP internal information.
neighbor	Enter the keyword **neighbor** to view the LACP neighbor information.

Example

This command returns the port priority and the MAC address (comma separated). In the example below, the port priority is the default value 32768 followed by the MAC address 00:0B:86:40:37:C0.

```
(host) [mynode] #show lacp sys-id
32768,00:0B:86:40:37:C0
```

The port uses the group number +1 as its “actor admin key”. By default, all the ports use the long timeout value (90 seconds).

```
(host) [mynode] #show lacp 0 neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting fast LACPDUs
        A - Device is in active mode P - Device is in passive mode

Partner's information
---------------------
Port    Flags  Pri  OperKey  State Num  Dev Id
----    -----  ---- -------  ----- ---- ----------------
FE 1/1  SA     1    0x10     0x45  0x5  00:0b:86:51:1e:70
FE 1/2  SA     1    0x10     0x45  0x6  00:0b:86:51:1e:70
```

When a port, in a LAG, is disconnected (that is, the partner device is different than the other ports or the neighbor times out or can not exchange LACPDUs with the partner), the port status is displayed as **DOWN**. See the following example.

```
(host) [mynode] #show lacp 0 internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting fast LACPDUs
        A - Device is in active mode P - Device is in passive mode

Port    Flags  Pri  AdminKey  OperKey  State Num  Status
----    -----  ---- --------  -------- ----- ---- -------
```

```
FE 1/1   SA      1     0x1        0x1        0x45   0x2   DOWN
FE 1/2   SA      1     0x1        0x1        0x45   0x3   UP
```

The “counters” option allows you to view LACP received (Rx) traffic, transmitting (Tx) traffic, data units (DU) received and transmitted by port.

```
(host) [mynode] #show lacp 0 counters

Port     LACPDUTx   LACPDURx   MarkrTx   MarkrRx   MrkrRspTx MrkrRspRx
----     --------   --------   -------   --------  --------- ---------
FE 1/1   10         10         0         0         0         0
FE 1/2   12         12         0         0         0         0
```

Related Commands

Command	Description
lacp group	Enables LACP and configure on the interface.
lacp port-priority	Configures the LACP port priority.
show interface port-channel	Displays information for a specified port-channel interface.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platform	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show lc-cluster

```
show lc-cluster
   exclude-vlan
   group-membership
   group-profile
   gsm counters
   heartbeat counters
   load distribution
   papi counters
   vlan-probe
   <profile> {ap|controller|upgrade}
```

Description

Displays information related to vlan, membership, profile, heartbeat, and so on for a cluster.

Syntax

Parameter	Description
`exclude-vlan`	Displays a list containing vlans excluded from L2 Probing
`group-membership`	Displays the active cluster member of cluster profile
`group-profile`	Displays the cluster profile
`gsm counters`	Displays the counters pertaining to various GSM events
`heartbeat counters`	Displays the cluster node health parameters such as heartbeat related counters, last time of node disconnect, critical process crash count and other information.
`load distribution`	Displays the current load distribution
`ap`	Displays the current load distribution on the AP
`client`	Displays the current load distribution on the client
`papi`	Displays the cluster messaging related counters.
`vlan-probe`	Displays the Cluster VLAN Probe information.
`<profile>`	Displays the name of the cluster profile.
`ap {details}`	Displays the details of the APs in the cluster.
`controller {details|ip|ipv6}`	Displays the controllers details in the cluster. Use one of the following parameters: ■ **details**: Displays the details of the controllers in the cluster. ■ **ip <ipv4_addr> [active {ap [details]}]**: Displays the IP address details of the controllers in the cluster. ■ **ipv6 <ipv6_addr> [active {ap [details]}**: Displays the IPv6 address details of the controllers in the cluster.

Parameter	Description
upgrade	Displays the upgrade details of controllers and APs in the cluster. Use one of the following parameters: ■ **stats**: Displays the statistics of the cluster upgrade. ■ **status**: Displays the upgrade status of each controller and AP.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

An example output of the **show lc-cluster group-membership** command.

```
Cluster Enabled, Profile Name = "test4nodecluster"
Redundancy Mode On
Active Client Rebalance Threshold = 50%
Standby Client Rebalance Threshold = 75%
Unbalance Threshold = 5%
Cluster Info Table
------------------
Type IPv4 Address    Priority Connection-Type STATUS
---- --------------- -------- --------------- ------
peer     10.17.65.34      128    L2-Connected CONNECTED (Leader, last HBT_RSP 11

       ms ago, RTD = 0.000 ms)
self     10.17.65.35      128    N/A CONNECTED (Member) peer     10.17.65.36     128
N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
peer     10.17.65.37      128    N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
peer     10.17.65.38      128    N/A INCOMPATIBLE (BUILD_STRING_MISMATCH)
```

An example output of the **show lc-cluster exclude-vlan** command.

```
#show lc-cluster exclude-vlan
---------------------------
VLANs excluded from probing
---------------------------
1
```

An example output of the **show lc-cluster group-profile** command.

```
#show lc-cluster group-profile cluster_test

IPv4 Cluster Members
--------------------
CONTROLLER-IP  PRIORITY  MCAST-VLAN  VRRP-IP  VRRP-VLAN
-------------  --------  ----------  -------  ---------
10.17.65.34    128       0           0.0.0.0  0
10.17.65.35    128       0           0.0.0.0  0
Redundancy:Yes
Active Client Rebalance Threshold:50%
Standby Client Rebalance Threshold:75%
Unbalance Threshold:5%
```

An example output of the **show lc-cluster gsm** command.

```
#show lc-cluster gsm counters
```

```
Cluster GSM Channel Counters
----------------------------
STA Channel: Adds                                                    >> 0
STA Channel: Deletes                                                 >> 0
STA Channel: Activates                                               >> 0
STA Channel: Deactive and Dormant Deletes                            >> 0
Cluster STA Channel: Dormant Adds                                    >> 0
Cluster STA Channel: Dormant Deletes                                 >> 0
Cluster STA Channel: Dormant Section Update                          >> 0
Cluster STA Channel: Section Update                                  >> 0
Cluster STA Channel: STA not found during Dormant Section Update     >> 0
Cluster STA Channel: STA not found during Section Update             >> 0
AP Channel: Adds                                                     >> 0
AP Channel: Deletes                                                  >> 0
Cluster AP Channel: Dormant Adds                                     >> 0
Cluster AP Channel: Deactivates                                      >> 0
Cluster AP Channel: Dormant Deletes                                  >> 0
BSS Channel: Adds                                                    >> 0
BSS Channel: Deletes                                                 >> 0
BSS Channel: Section Update                                          >> 0
BSS Channel: BSS not found during Section Update                     >> 0
Cluster BSS Channel: Dormant Adds                                    >> 0
Cluster BSS Channel: Deactivates                                     >> 0
Cluster BSS Channel: Dormant Deletes                                 >> 0
```

An example output of the **show lc-cluster heartbeat** command.

```
#show lc-cluster heartbeat counters

Cluster Heartbeat Counters
--------------------------
IPv4 Address         RES      RSR   MIS  HMPD LMRPD  IDPD CPDPD CDPD LMHINT
 LTOD
--------------- -------- -------- ----- ----- ----- ----- ----- ---- ------ ------------------
------
10.17.65.34    28147    28147     0    61     0     0     0     0    376 Thu Jun 16 23:53:48
2016
10.17.65.36        0        0     0     0     0     0     0     0      0
10.17.65.37        0        0     0     0     0     0     0     0      0
10.17.65.38        0        0     0     0     0     0     0     0      0
-----------PREAMBLE-----------------
RES    - REQ SENT
RSR    - RSP RCVD
MIS    - MISSES
HMPD   - HBT MISS PEER DEAD
LMRPD  - LINK MAP RCVD PEER DEAD
IDPD   - IPSEC DOWN PEER DEAD
```

An example output of the **show lc-cluster papi** command.

```
#show lc-cluster papi counters
Cluster PAPI Counters
---------------------
RX STM UP                               >>  1
RX STM DOWN                             >>  1
RX AUTH UP                              >>  0
RX AUTH DOWN                            >>  0
RX ISAKMPD UP                           >>  0
RX ISAKMPD DOWN                         >>  0
RX DDS UP                               >>  0
RX DDS DOWN                             >>  0
```

```
TX SOS CLUSTER ENABLE SUCCESS            >>  2
TX SOS CLUSTER ENABLE FAIL               >>  0
TX SOS CLUSTER DISABLE SUCCESS           >>  1
TX SOS CLUSTER DISABLE FAIL              >>  0
TX SOS CLUSTER PEER ADD SUCCESS          >> 127
TX SOS CLUSTER PEER ADD FAIL             >>  0
TX SOS CLUSTER PEER DEL SUCCESS          >>  0
TX SOS CLUSTER PEER DEL FAIL             >>  0
```

An example output of the **show lc-cluster load** command.

```
#show lc-cluster load distribution ap

Cluster Load Distribution for APs
---------------------------------
Type IPv4 Address    Active APs     Standby APs
---- --------------- -------------- ---------------
self     10.15.146.3              3               3
peer     10.15.146.4              1               3
peer     10.15.146.5              1               0
peer     10.15.146.6              1               0
Total: Active APs 6 Standby APs 6


#show lc-cluster load distribution client

Cluster Load Distribution for Clients
-------------------------------------
Type IPv4 Address    Active Clients Standby Clients
---- --------------- -------------- ---------------
self     10.15.146.3              0               0
peer     10.15.146.4              0               1
peer     10.15.146.5              0               0
peer     10.15.146.6              1               0
Total: Active Clients 1 Standby Clients 1
```

An example output of the **show lc-cluster vlan-probe** command.

```
#show lc-cluster vlan-probe status

Cluster VLAN Probe Status
-------------------------
Type IPv4 Address    REQ-SENT REQ-FAIL ACK-SENT ACK-FAIL REQ-RCVD ACK-RCVD VLAN_FAIL CONN-TYPE
START/STOP
---- --------------- -------- -------- -------- -------- -------- -------- --------- ---------
---------
peer     10.17.65.34      248        0      372        0      372      248         0   L2 Conn
    5/   5
peer     10.17.65.36        0        0        0        0        0        0         0       N/A
    0/  49
peer     10.17.65.37        0        0        0        0        0        0         0       N/A
    0/  49
peer     10.17.65.38        0        0        0        0        0        0         0       N/A
    0/  49
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The parameter details of **<profile>** were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode or enable mode in the managed device

show lc-rap-pool

```
show lc-rap-pool <pool_name>
```

Description

This command displays the remote AP inner IP pool for cluster deployment.

Syntax

Parameter	Description
`pool_name`	Name of the local IP pool to show.

Example

The output of the example below displays the remote AP inner IP pool that can be used for cluster deployment.

```
(host) [mynode] (config) #show lc-rap-pool rap-cluster
IP addresses used in pool rap-cluster
3.1.1.3-3.1.1.10
Total:-
8 IPs used - 51134 IPs free - 51142 IPs configured
LC RAP Pool Total Allocs/Deallocs/Reserves : 8/0/0
LC RAP Pool Allocs/Deallocs/Reserves(succ/fail) : 8/0/(0/0)
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platform	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show lcd-menu

```
show lcd-menu
```

Description

This command displays the current LCD Menu configuration on the managed device.

Syntax

No parameters.

Example

The following example displays the output of the **show lcd-menu** command.

```
(host) [mynode] #show lcd-menu

lcd-menu
--------
Parameter                                  Value
---------                                  -----
menu maintenance upgrade-image partition0  enabled
menu maintenance upgrade-image partition1  enabled
menu maintenance upgrade-image             enabled
menu maintenance upload-config             enabled
menu maintenance factory-default           enabled
menu maintenance media-eject               enabled
menu maintenance reload-system             enabled
menu maintenance halt-system               enabled
menu maintenance                           enabled
menu                                       enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show lclist

```
show lclist
```

Description

This command displays the list of managed devices connected to Mobility Master.

Syntax

No parameters.

Example

The following command displays the list of managed devices connected to Mobility Master.

```
(host) [mynode] #show lclist

All LC List
-----------
IP Address      Name            Location          Model      Version                  Status
----------      ----            --------          -----      -------                  ------
192.0.2.15      Standy-HQ       Building1.floor1  ArubaMM    8.0.0.0-svcs-ctrl_55561  up
192.0.2.16      Corp-7240       Building1.floor1  Aruba7240  8.0.0.0-svcs-ctrl_55561  up
192.0.2.17      Corp-7210       Building1.floor1  Aruba7210  8.0.0.0-svcs-ctrl_55561  up
192.0.2.18      Corp-7220       Building1.floor1  Aruba7220  8.0.0.0-svcs-ctrl_55561  up
192.0.2.19      Corp-VPNC       Building1.floor1  Aruba7010  8.0.0.0-svcs-ctrl_55561  up
192.0.2.20      Corp-BOC1       Building1.floor1  Aruba7010  8.0.0.0-svcs-ctrl_55561  up
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show license

```
show license [limits]|[passphrase]
```

Description

Displays the license table or Mobility Master passphrase.

Syntax

Parameter	Description
`limits`	Enter the keyword **limit** to display the current license limits.
`passphrase`	Issue the **show license passphrase** command to identify the Mobility Master passphrase. This passphrase is used in the licensing website to generate a Mobility Master (MM) license, or to generate a sharable license that can be added to Mobility Master license pools.

Example

An example output of the **show license** command.

```
(host)[node] # show license

License Table
-------------
Key                                                 Installed   Expires  Flags  Service Type
---                                                 ---------   -------  -----  ------- -----
x7kbiBm5-3jI5MiBY-HVTAH/ci-llxPiKBV-dY8QGBMg-240    2010-01-21  Never           Access Points:
1024
                                                    21:00:22
itY24Hca-HSQlvJhi-yZtW6RB7-HGuBXzIq-N6hd6TNV-nZk    2010-01-21  Never      E    120abg Upgrade:
128
                                                    21:01:03
oqdLOxZ6-+FS5DT2P-iNmtvc3o-NFyasYrO-ixGUrszE-4uo    2010-01-21  Never      E    121abg Upgrade:
128
                                                    21:01:13
GIleLrCX-d8lxt3z5-vQC50n60-f31amOxu-Rf0uEoTn-qXQ    2010-01-21  Never      E    124abg Upgrade:
128
                                                    21:01:22
ldsXG7ik-pj/HVm4t-Qt3541UC-3wzC+Efj-yn08g/HF-/Dg    2010-01-21  Never      E    125abg Upgrade:
128
                                                    21:01:3
sJvaPL88-gWDdlMpj-LZMZ2YKK-2fU8NV6l-XIH4wRk8-44I    2010-05-05  Never      E    RF Protect: 512
                                                    08:51:57
QtemJpLj-Qm5D9WvK-8c9lbaL6-t2nU6/Pj-LSNd00FZ-tJo    2010-05-05  Never      E    RF Protect: 1024
                                                    08:52:07
                                                    21:18:55
WNx6RasB-Qn9YVZ+5-giraq0Uy-aoIqS3as-FXmFh5dY-cSs    2010-01-21  Never      E    xSec Module:
1024
                                                    21:20:56
u/GdQHWa-m4bzUCMC-ydMsWTif-hDMDajyB-qAlIMwnN-pGM    2010-01-25  Never      E    Policy
Enforcement Firewall for VPN users
                                                    18:44:19
F9dGNdjV-EmwLhqlI-oKMQQepZ-b9Jl3OB2-HQjwmc+r-vhI    2010-01-25  Never      E    Next Generation
Policy Enforcement Firewall Module: 128
                                                    18:44:19
```

```
License Entries: 11

Flags: A - auto-generated; E - enabled; R - reboot required to activate
```

The output of this command includes the following data columns:

Parameter	Description
`Key`	The license key.
`Installed`	The license installation date and time.
`Expires`	The date that your evaluation license expires is listed in this column. Permanent license will always have a “Never” in this column. Expired evaluation licenses will also be indicated in this column.
`Flags`	This column displays some status about your license. The legend for this column appears at the bottom of the display output. They are: **A**: The license is auto-generated. **E**: The license if fully enabled. **R**: You must reboot your controller to fully enable this license.
`Service Type`	The license name (feature).

Related Commands

To view additional statistics for license key usage, use the command show keys.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The **passphrase** parameter is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

show license aggregate

```
show license aggregate
```

Description

Display the total number of licenses of each license type in all Mobility Master licensing pools.

Syntax

No Parameters.

Usage Guidelines

Execute this command from any configuration node in the Mobility Master CLI to view the licenses in the global licensing pool and any local license pools, as well as the number of clients using each pool.

Example

The following example displays output of the **show license aggregate** command.

```
Aggregate License Table for pool /
----------------------------------
Hostname     IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR  WebCC
--------     ----------  --------  ---  ---  ----------  -----------  ---  -----
From Server                        6    3    0           0            0    0

Last update (secs. ago)
-----------------------
60

Total no. of clients: 0
Aggregate License Table for pool /SC
------------------------------------
Hostname     IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR  WebCC
--------     ----------  --------  ---  ---  ----------  -----------  ---  -----
From Server                        128  128  128          64          16   16

Last update (secs. ago)
-----------------------
60
Total no. of clients: 20

Aggregate License Table for pool /India
---------------------------------------
Hostname     IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR  WebCC
--------     ----------  --------  ---  ---  ----------  -----------  ---  -----
From Server                        512  512  512         128          64    64

Last update (secs. ago)
-----------------------
60
Total no. of clients: 88

Aggregate License Table for pool /USA
-------------------------------------
Hostname     IP Address  Mac addr  AP   PEF  RF Protect  xSec Module  ACR  WebCC
--------     ----------  --------  ---  ---  ----------  -----------  ---  -----
From Server                        512  512  512         128          128  32
```

```
Last update (secs. ago)
-----------------------
60

Total no. of clients: 91
```

The output of this command includes the following data columns:

Parameter	Description
Hostname	Name of the device that supplied the licensing information. If this command is executed on a Mobility Master, the hostname field displays the value **from server**.
IP Address	IP address of the device that supplied the licensing information. If this command is executed on a Mobility Master, the IP address field remains blank.
AP	Total number of AP licenses in the licensing pool.
PEF	Total number of Policy Enforcement Firewall (PEF) licenses in the licensing pool.
RF Protect	Total number of RFprotect licenses in the licensing pool.
xSec Module	Total number of Extreme Security (xSec) licenses in the licensing pool.
ACR	Total number of advanced Cryptography (ACR) licenses in the licensing pool.
Last update (secs. ago	Time, in seconds, that has elapsed since the licensing table on Mobility Master was updated.
Total mumber of clients	This value indicates the total number of clients using licenses from the licensing pool.

Related Commands

Command	Description
show license key	Display information about a specific license key.
show license keys	Display information about all installed license keys.
show license box	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license box

```
show license box remote remote-ip-addr <ip-addr>
```

Description

Display the device-specific licenses used by a remote managed device.

Syntax

Parameter	Description
`remote remote-ip-addr <ip-addr>`	IP address of the managed device.

Usage Guidelines

Execute this command from the CLI of a managed device to view license limits applied to that managed device from its licensing pool

Example

The following example displays output of the **show license box remote remote-ip-addr <ip-addr>** command.

```
Box Licenses Table
------------------
Key                            Feature                                  Expiration  Status
---                            -------                                  ----------  ------
cvK33n5l-MeXuHi7N-gRyIa4As-Gh  X86 VM SKU Activate                      Never       E/Active
V3rBYtzd-hOtVXuKi-WZeEYJUl-9k  Policy Enforcement Firewall for VPN users  Never       E/Active
```

The output of this command includes the following data columns:

Parameter	Description
`Key`	License key on the managed device
`Feature`	Licensing feature enabled by the license key
`Expiration`	This field displays the expiration date for evaluation or subscription licenses.
`Status`	Current status of the license.

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Master licensing pools.
show license key	Display information about a specific license key.
show license keys	Display information about all installed license keys.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.0.1.0	The **remote remote-ip-addr** parameter was introduced, and the **remote ip-addr** parameter was deprecated.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license client-table

```
show license client-table
```

Description

Display the license limits applied to each managed device

Syntax

No Parameters.

Usage Guidelines

Execute this command from the CLI of a managed device to view license limits applied to that managed device from its licensing pool

Example

The following example displays output of the **show license client-table** command.

```
(host)[node] #show license client-table
Built-in limit: 0
License Client Table
--------------------
Service Type         System Limit  Server Lic.  Used Lic.  Remaining Lic.  FeatureBit
------------         ------------  -----------  ---------  --------------  ----------
Access Points        499           250          10         240             enabled
Next Gen PEF Module  499           250          10         240             enabled
RF Protect           499           0            0          0               disabled
Adv Cryptography     999999        0            0          0               disabled
WebCC                499           250          10         240             enabled
MM-VA                500           495          5          495             enabled
MC-VA-RW             499           0            0          0               enabled
MC-VA-EG             499           0            0          0               enabled
MC-VA-IL             499           0            0          0               enabled
MC-VA-JP             499           0            0          0               enabled
MC-VA-US             499           0            0          0               enabled
VIA                  499           0            0          0               enabled
```

The output of this command includes the following data columns:

Parameter	Description
`Service Type`	Type of license on the managed device.
`System Limit`	The maximum number of licenses supported by the man platform.
`Server Lic.`	Number of licenses available for use by the licensing client. **NOTE:** This number is limited by the total license capacity of the managed device platform. A managed device cannot use more licenses than is supported by that managed device platform, even if additional license are available.
`Used Lic.`	Total number of licenses of each license type used by the managed device.
`Remaining Lic.`	Total number of remaining licenses available in the licensing pool

Parameter	Description
`Feature Bit`	This column indicates whether these license features are enabled or disabled. For more information about enabling a sharable license, see license-pool-profile-root.

Related Commands

To view additional statistics for the licenses in each license pool, access the Mobility Master CLI and execute the command show license aggregate.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The output of this command displays information for VIA licenses introduced in ArubaOS 8.2.0.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on managed devices

show license debug

```
show license debug
```

Description

Displays a summary of Mobility Master's licensing role and IP address.

Syntax

No parameters

Example

The following example shows the output of the **show license debug** command.

```
(host)[node] # show license debug

Summary of licensing state
Centralized Licensing: Enabled
Switch Role: Master
License Role: License Server
Switch IP: 10.16.16.160
```

The output of this command includes the following data columns:

Parameter	Description
`Centralized licensing`	Shows if centralized licensing is enable or disabled.
`Switch Role`	Role of the device using the configuration on which this command is run.
`License Role`	Licensing role of the controller on which this command is run. Mobility Master be a licensing client or a licensing server. Managed devices can be licensing clients only.
`Master IP`	IP address used by Mobility Master. If a Mobility Master redundant pair is using VRRP, this parameter displays the VRRP virtual IP address.
`Switch IP`	IP address assigned to the device using the configuration on which this command is run.
`License Server IP`	Mobility Master IP address.

Related Commands

To view additional statistics for license usage on Mobility Master, use the command show license aggregate.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master and managed devices.

show license heartbeat stats

```
show license heartbeat stats
```

Description

Display the license heartbeat statistics between the centralized licensing server and the license client.

Syntax

No Parameters.

Usage Guidelines

If your deployment uses the centralized licensing feature, issue this command from the CLI of a centralized licensing server to view heartbeat requests to and responses from each licensing client associated to that licensing server. If you issue this command from a licensing client, the output displays information for that one client only.

Example

The following example displays output of the **show license heartbeat stats** command issued from the licensing server.

```
(host)[node] #show license heartbeat stats
License Heartbeat Table
-----------------------
IP Address      HB Req  HB Resp         Total Missed    Last Update
10.3.17.130     233     233             0               18
10.3.17.120     233     233             0               19
10.3.17.190     234     234             0               9
10.3.17.140     233     233             0               7
```

The output of this command includes the following data columns:

Parameter	Description
`IP address`	IP address of the licensing client.
`HB Req`	Heartbeat requests sent from the licensing client.
`HB Resp`	Heartbeat responses received from the license server.
`Total Missed`	Total number of heartbeats that were not received by the licensing client.
`Last Update`	Number of seconds elapsed since the licensing client last sent a heartbeat request.

Related Commands

Parameter	Description
show license aggregate .	View additional statistics for license usage on the licensing server master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on centralized licensing master or licensing client controllers.

show license key

```
show license key <key>
```

Description

Display information about a specific evaluation or subscription license key.

Syntax

Parameter	Description
`<key>`	License key

Usage Guidelines

Issue this command from the Mobility Master CLI to view the status of an installed evaluation or subscription license key.

Example

The following example displays output for the **show license key** command. In this example, the output has been modified to appear in two separate sections. In the actual CLI, this output appears in a single, long row.

```
(host)[node] #show license key eLNB35l-2lF-3WE

Key Attributes:
---------------
Feature  Type       Expiration           GraceExpiration      TotalCount
-------  ----       ----------           ---------------      ----------
WebCC    Subscript  2017-05-03 10:36:54  2017-08-31 10:36:54  10

AvailableForAllocation  Status
----------------------  ------
10                      E/Active
Flags: E - enabled; R - reboot/activation key required to activate; D - Not enabled on Local
Controller
```

The output of this command includes the following data columns:

Parameter	Description
`Key`	License key
`Feature`	Feature type supported by the license key
`Type`	ArubaOS supports the **permanent**, **evaluation** or **subscription** license types, but this command displays information about evaluation and subscription licenses only.
`Expiration`	The expiration date for the subscription or evaluation license key.
`GraceExpiration`	The grace period for which a subscription remains fully active after the subscription key expiration date.
`TotalCount`	The total number of licenses supported by the license key.

Parameter	Description
`AvailableforAllocation`	The total number of licenses that are still available for allocation
`Status`	This column shows the current status of the license, including whether it is active or expired, and whether that licensing feature is enabled on Mobility Master or the stand-alone controller.

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Master licensing pools.
show license keys	Display information about all installed license keys.
show license box	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license keys

```
show license keys
   [feature-type acr|ap|mc-va-eg|mc-va-il|mc-va-jp|mc-va-rw|mc-va-us|pefng|rfp|acr|xsc|
   [webc|mm]
   [license-type perm|eval|subscript|non-perm]
```

Description

Display information about all license keys installed on Mobility Master.

Syntax

Parameter	Description
`Feature-type`	View a list of license keys for the specified feature type.
`acr`	View Advanced Cryptography (ACR) licenses.
`ap`	View AP licenses.
`mc-va-eg`	View MC-VA-EG license type information for Egypt.
`mc-va-il`	View MC-VA-IL license type information for Israel.
`mc-va-jp`	View MC-VA-JP license type information for Japan.
`mc-va-rw`	View MC-VA-RW license type information for rest of the world (all other countries)
`mc-va-us`	View MC-VA-US license type information for United States.
`mm`	View MM licenses for Mobility Master.
`pef`	View Policy Enforcement Firewall (PEF) licenses.
`rfp`	View RF Protect licenses.
`xsc`	View xSec licenses.
`License-type`	View a list of license keys of the specified license type.
`perm`	Display a list of permanent licenses.
`eval`	Display a list of evaluation licenses.
`subscript`	Display a list of subscription licenses .
`non-perm`	Display a list of non-permanent licenses (evaluation and subscription).

Usage Guidelines

Issue this command from the Mobility Master CLI to view the status of an installed license keys.

Example

The following example displays output for the **show license keys** command. In this example, the output has been modified to appear in two separate sections. In the actual CLI, this output appears in a single, long row.

Example

```
(host)[node]#show license keys
License Keys info
-----------------
Key      Feature  Type       Expiration           GraceExpiration      TotalCount
---      -------  ----       ----------           ---------------      ----------
7eWKHB6 PEFNG    Perm       Never                N/A                  500
Ryw+Sau AP       Perm       Never                N/A                  500
aHfQ8hZ ACR      Eval       2016-06-02 11:17:18  N/A                  64
eLNBA35 WebCC    Subscript  2017-05-03 10:36:54  2017-08-31 10:36:54  10

AvailableForAllocation  Status
----------------------  ------
450                     E/Active
450                     E/Active
64                      E/Expires in 29 days
10                      E/Active
```

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Master licensing pools.
show license key	Display information about a specific license key.
show license_box	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.2.0.0	The following parameters under **feature-type** were added: ■ **mc-va-eg** ■ **mc-va-il** ■ **mc-va-jp** ■ **mc-va-rw** ■ **mc-va-us**
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license passphrase

```
show license passphrase
```

Description

Display the Mobility Master passphrase used to generate licenses for a Mobility Master deployment.

Syntax

No Parameters.

Usage Guidelines

Issue this command for a network where the Mobility Master software is installed on a VM. This command is not supported on stand-alone controllers, the Mobility Master appliance or managed devices.

Example

```
(host)[node] #show license passphrase
5I0N3bI6-exkTWLkq-P05tfofQ-d6NvLJR91
```

Related Commands

Command	Description
show inventory	Display the Mobility Master serial number used to generate licenses for a Mobility Master deployment.
product serial-number	This command configures the product serial-number for a managed device on a Virtual Machine (VM).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license platform-limits

```
show license passphrase
```

Description

Display the licensing limits for Mobility Master or the controller platform upon which this command is issued.

Syntax

No Parameters.

Usage Guidelines

To view licensing limits for Mobility Master managed devices, you must access the CLI of that specific node.

The output of this command displays limits for currently supported licenses, as well as limits for deprecated license types no longer supported by this software version.

Example

The output of the following command displays platform limits for all licenses supported by Mobility Master.

```
(host)[node] #show license platform-limits
License Platform Limits
-----------------------

License Platform Limits
-----------------------
Limit   Value
-----   -----
999999  Access Points
999999  Remote Access Points
999999  Ortronics Access Points
999999  Outdoor Mesh Access Points
999999  Wireless Intrusion Protection Module
999999  VPN Service Module
4096    xSec Users
999999  Indoor Mesh Access Points
999999  120abg Upgrade
999999  121abg Upgrade
999999  124abg Upgrade
999999  125abg Upgrade
999999  Policy Enforcement Firewall Module
999999  Advanced Cryptography
0       SAP
999999  WebCC
999999  Beta AP
```

The following example displays platform limits for all licenses supported by a 7005 controller.

```
(host)[node] #show license platform-limits
License Platform Limits
-----------------------
Limit  Value
-----  -----
16     Access Points
16     Remote Access Points
16     Ortronics Access Points
32     Outdoor Mesh Access Points
16     Wireless Intrusion Protection Module
4096   VPN Service Module
4096   xSec Users
```

```
32      Indoor Mesh Access Points
16      120abg Upgrade
16      121abg Upgrade
16      124abg Upgrade
16      125abg Upgrade
16      Policy Enforcement Firewall Module
4096    Advanced Cryptography
0       SAP
16      WebCC
16      Beta AP
```

Related Commands

Command	Description
show license aggregate	Display the total number of licenses of each license type in all Mobility Master licensing pools.
show license key	Display information about a specific license key.
show license box	Display the device-specific licenses used by a managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license-pool-profile

```
show license-pool-profile [<profile>]
```

Description

Use this command to display a list of license pools, or display the licenses allocated for a specific pool.

Syntax

Parameter	Description
`<profile>`	(Optional) The name of the profile for which you are creating a local license pool, for example, **Northwest**. The profile name is limited to 63 characters. **NOTE:** In ArubaOS 8.0.x releases, the licensing pool profile name was required to be the license pool configuration path. Starting in ArubaOS 8.1, the **license-pool-path** parameter is introduced to configure the license pool path, and the profile name can be any string of 63 characters or less.

Usage Guidelines

All managed devices associated to the same Mobility Master can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Master. However, ArubaOS also allows you to create individual licensing pools at a configuration node, allowing managed devices below that node to share licenses amongst themselves but not with other managed devices.

Starting in ArubaOS 8.1, the license-pool-path parameter displays the license pool path for the profile, up to 255 characters, for example, /USA/northwest.

NOTE: If you upgrade a legacy ArubaOS deployment to ArubaOS 8.1 or later, the license-pool-path parameter is automatically derived from the license-pool-profile <profile> name.

You must use the **license add** command to add license keys to the Mobility Master before you can allocate sharable licenses to a license pool, or associate a non-sharable license with an individual managed device, then issue the **license-pool-profile-root** command to enable licensing features on Mobility Master.

Examples

```
(host)[node] (config) #show license-pool-profile v6cluster

License pool profile "v6cluster"
--------------------------------
Parameter                                 Value
---------                                 -----
License pool path                         /md/v6cluster-1
AP permanent licenses                     600
AP expiry licenses                        N/A
PEFNG permanent licenses                  600
PEFNG expiry licenses                     N/A
RFP permanent licenses                    N/A
RFP expiry licenses                       N/A
ACR permanent licenses                    N/A
ACR expiry licenses                       N/A
WebCC expiry licenses                     N/A
WebCC subscription licenses               N/A
VIA permanent licenses                    N/A
VIA expiry licenses                       N/A
MM permanent licenses                     600
MM expiry licenses                        N/A
```

```
MC-VA Egypt permanent licenses              N/A
MC-VA Egypt expiry licenses                 N/A
MC-VA Israel permanent licenses             N/A
MC-VA Israel expiry licenses                N/A
MC-VA Japan permanent licenses              N/A
MC-VA Japan expiry licenses                 N/A
MC-VA USA permanent licenses                N/A
MC-VA USA expiry licenses                   N/A
MC-VA Rest of the world permanent licenses  N/A
MC-VA Rest of the World expiry licenses     N/A
```

Syntax

Parameter	Description
`license-pool-path <license-pool-path>`	The name of the profile , for example, Northwest. The profile name is limited to 63 characters. **NOTE:** In ArubaOS 8.0.x releases, the licensing pool profile name was required to be the license pool configuration path. Starting in ArubaOS 8.1, the **license-pool-path** parameter is introduced to configure the license pool path, and the profile name can be any string of 63 characters or less. **NOTE:** name.
`AP Permanent Licenses` `AP Expiry License`	These two fields show the numbers of permanent and temporary AP licenses.
`PEFNG Permanent Licenses` `PEFNG Expiry License`	These two fields show the numbers of permanent and temporary Next Generation Policy Enforcement Firewall (PEFNG) licenses.
`RFP Permanent Licenses` `RFP Expiry License`	These two fields show the numbers of permanent and temporary RF Protect (RFP) licenses.
`ACR Permanent Licenses` `ACR Expiry License`	These two fields show the numbers of permanent and temporary ArubaOS Advanced Cryptography (ACR) licenses .
`WebCC Permanent Licenses` `WebCC Expiry License`	These two fields show the numbers of permanent and temporary Web Content Classification (WebCC) licenses.
`VIA Permanent Licenses` `VIA Expiry License`	These two fields show the numbers of permanent and temporary Virtual Intranet Access (VIA) licenses.
`MM Permanent Licenses` `MM Expiry License`	These two fields show the numbers of permanent and temporary Mobility Master licenses in pool.
`via-licenses`	VIA licenses suport Virtual Intranet Access (VIA) or 3rd party VPN client . VIA licenses are not consumed for site-to-site VPNs. If a managed device or standalone controller has a PEFV license, that device will not consume VIA licenses from a licensing pool, as a single PEFV license supports all VIA and 3rd party VPN clients, up to the full user capacity for that device.
`webcc-licenses`	Add WebCC licenses to the selected pool. The Web Content Classification (WebCC) license is a subscription-based, per-AP license.

Parameter	Description
`eval`	(Optional) Include this keyword to add an evaluation license.
`<num>`	Number of licenses supported by the license key.

Related Commands

Version	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license	This command allows you to install, delete, and manage software licenses on Mobility Master.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show license-pool-profile-root

```
show license-pool-profile [<node-path>]
```

Description

Use this command to determine the license types that are enabled and sharable via the root licensing profile

Syntax

No parameters

Usage Guidelines

All managed devices associated to the same Mobility Master can share a pool of licenses, comprised of all the sharable licenses added to the Mobility Master. However, ArubaOS also allows you to create individual licensing pools at a configuration node, allowing managed devices below that node to share licenses amongst themselves but not with other managed devices.

You must use the **license add** command to add license keys to the Mobility Master before you can allocate sharable licenses to a license pool, or associate a non-sharable license with an individual managed device, then issue the **license-pool-profile-root** command to enable licensing features on Mobility Master.

Examples

```
(host) ^[mynode] (config) #show license-pool-profile-root
License root(/) pool profile
----------------------------
Parameter              Value    Set
---------              -----    ---
enable PEFNG feature   Enabled
enable RFP feature     Enabled
enable XSEC feature    true
enable ACR feature     true
enable WebCC feature   true
```

Related Commands

Version	Description
license-pool-profile-root	Use this command to enable shared license features within the global licensing pool.
license	This command allows you to install, delete, and manage software licenses on the controller.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced

Command Information

Platform	License	Command Mode
Available on all platforms	Available in the base operating system	Enable and config mode on Mobility Master

show license server-table

```
show license server-table
```

Description

Display the license server table for each licensing pool as it appears on the centralized licensing server.

Syntax

No Parameters.

Usage Guidelines

If your deployment uses the centralized licensing feature, issue this command from the CLI of a centralized licensing server to view to view licensing counts for each supported license type.

Example

The following example displays part of the output of the **show license server-table** command issued from a licensing server. The complete output displays a separate table for each licensing pool.

```
(host) [node] #show license server-table
License Server Table for pool /
-------------------------------
Service Type            PoolSize  ExpiredLic  ActualPoolSize  UsedLic  RemainingLic  Warnings
                        FeatureBit
------------            --------  ----------  --------------  -------  ------------  --------
                        ----------
Access Points           2337      547         1790            0        1790          Some
licenses expired        enabled
Next Gen PEF Module     419       419         0               0        0             Some
licenses expired        enabled
RF Protect              9864      32          9832            0        9832          Some
licenses expired        enabled
xSec Module             0         0           0               0        0             None
                        enabled
Advanced Cryptography   254       0           254             0        254           Some
licenses expiring       enabled
WebCC                    0         0           0               0        0             None
                        disabled
MM-VA                   13750     10500       3250            0        3250          Some
licenses expired        enabled
MM-VA                   500       0           500             5        495           None
                        enabled
MC-VA-RW                0         0           0               0        0             None
                        enabled
MC-VA-EG                0         0           0               0        0             None
                        enabled
MC-VA-IL                0         0           0               0        0             None
                        enabled
MC-VA-JP                0         0           0               0        0             None
                        enabled
MC-VA-US                0         0           0               0        0             None
                        enabled
VIA                     0         0           0               0        0             None
                        enabled
```

The output of this command includes the following data columns:

Parameter	Description
`ServiceType`	Type of license on the licensing server.
`PoolSize`	The total number of licenses assigned to that licensing pool. This number includes both expired and active licenses.
`ExpiredLic`	Number of expired licenses for each license type,
`ActualPoolSize`	The total number of active licenses currently available for devices and users in the selected license pool. The **ActualPoolSize** value is the total number of licenses in the pool (**PoolSize**) value minus the expired licenses (**ExpiredLic**).
`UsedLic.`	Total number of licenses of each license type reported as used by the licensing clients or licensing server.
`RemainingLic.`	Total number of remaining licensing available in the licensing table.
`Warnings`	This column displays warnings if licenses have exired, or if licenses used on a per-session basis are no longer sufficient to support the client demand.
`FeatureBit`	This column indicates whether these license features are enabled or disabled. For more information about enabling a sharable license, see license-pool-profile-root.

Related Commands

To view additional statistics for license usage on the licensing server master, use the command show license aggregate.

Command History

Release	Modification
ArubaOS 8.2.0.0	The output of this command displays information for VIA licenses introduced in ArubaOS 8.2.0.0.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and config mode on Mobility Master

show license-usage

```
show license-usage
   acr
   ap
   client [pool <pool>][verbose]
   user
   via
   xsec
   web-cc
```

Description

Display license usage information.

Syntax

Parameter	Description
`acr`	Show ACR license usage
`ap`	Show AP license usage information.
`client [pool <pool>] [verb-ose]`	Show license usage for the global configuration pool, or specify a pool name to view license usage within a specific license pool. Use the optional **verbose** parameter too display aggregated license usage for each configuration node and managed devices in those nodes.
`user`	Show Policy Enforcement Firewall (PEF) user license usage.
`via`	Show VIA license usage information.
`webcc`	Show WebCC license usage information.
xsec	Show Extreme Security (xSec) user and tunnel license usage.

Examples

The following example displays the user license usage.

```
(host) #show license-usage user

User License Usage
------------------
Name                 Value
----                 -----
License Limit        2048
License Usage        12
License Available    2036
License Exceeded     0
```

The AP license usage is displayed below:

```
(host) #show license-usage AP
```

```
AP Licenses
-----------
Type                       Number
----                       ------
AP Licenses                512
RF Protect Licenses        512
PEF Licenses               512
Overall AP License Limit   512

AP Usage
--------
Type              Count
----              -----
Active CAPs       3
Standby CAPs      0
RAPs              0
Remote-node APs   0
Tunneled nodes    0
Total APs         3

Remaining AP Capacity
---------------------
Type  Number
----  ------
CAPs  509
RAPs  509
```

When you issue the **show license-usage client** command from the CLI of a controller configured as a centralized licensing server, the output displays license usage statistics for each licensing client associated to that server. Include the **verbose** parameter to display license statistics for individual configuration nodes and the devices in those nodes. The output in the example below is separated into multiple tables to better fit in this document. In the ArubaOS CLI, the output appears in a single wide table.

```
(MM)[mynode] #show license-usage client verbose
License Clients License Usage for pool /
----------------------------------------
Hostname  IP Address    Mac addr           AP   PEF   RF Protect
--------  ----------    --------           ---- ----  ----------
RagSC     10.15.90.33   00:0c:29:71:10:15  0    0      0
Rag-LC1   10.15.88.100  00:1a:1e:01:b2:28  3    3      0
TOTAL                                      3    3      0

ACR   WebCC   MM    MC-VA-RW   MC-VA-EG   MC-VA-IL   MC-VA-JP   MC-VA-US   VIA
----  ------  ----  ---------  ---------  ---------  ---------  ---------  ----
0     0       0     0          0          0          0          0          0
0     0       0     0          0          0          0          0          0
0     0       0     0          0          0          0          0          0

Last update (secs. ago)
16
Total no. of clients: 0

Node level usage details for pool /
-----------------------------------------------
Node-Path  AP   PEF   RF Protect  ACR   WebCC  MM    MC-VA-RW   MC-VA-EG   MC-VA-IL   MC-VA-JP
---------  ---  ---  -----------  ----  ------ ----  ---------  ---------  ---------  --------
/          0    0     0           0     0      0     0          0          0           0
MC-VA-US   VIA
---------  ---
0          0


License Clients License Usage for pool /md/hq/voip/x86
------------------------------------------------------
```

```
Hostname  IP Address  Mac addr  AP    PEF   RF Protect   ACR   WebCC   MM    MC-VA-RW   MC-VA-
--------  ----------  --------  ----  ----  -----------  ----  ------  ----  ---------  ------
EG   MC-VA-IL   MC-VA-JP   MC-VA-US   VIA  Last update (secs. ago)
---  ---------  ---------  ---------  ---  ----------------------
Total no. of clients: 0

Node level usage details for pool /md/hq/voip/x86
-------------------------------------------------
Node-Path  AP   PEF   RF Protect  ACR   WebCC  MM    MC-VA-RW   MC-VA-EG   MC-VA-IL   MC-VA-JP
---------  ---  ---  -----------  ----  ------ ----  ---------  ---------  ---------  --------
/          0    0     0           0     0      0     0          0          0           0
MC-VA-US   VIA
---------  ---
0          0
```

The output of the show license-usage client command includes the following data columns:

Parameter	Description
Hostname	Name of the licensing client controller.
IP Address	IP address of the licensing client controller.
AP	Total number of AP licenses used by a licensing client associated with this controller.
PEF	Total number of Policy Enforcement Firewall (PEF) licenses used by a licensing client associated with this controller.
RF Protect	Total number of RFprotect licenses used by a licensing client associated with this controller.
ACR	Total number of advanced Cryptography (ACR) licenses used by a licensing client associated with this controller.
WebCC	Total number of Web Content Classification (WebCC) licenses used by a licensing client associated with this controller.
MM	Total number of Mobility Master (MM) licenses used by a licensing client associated with this controller.
MC-VA-RW MC-VA-EG MC-VA-IL MC-VA-JP MC-VA-US	Total number of regional licenses required to terminate APs on a virtual controller. Different MC-VA-XX license types enable APs to support regional channels for the following countries: ■ MC-VA-US: United states ■ MC-VA-JP: Japan ■ MC-VA-IL: Israel ■ MC-VA-EG: Egypt ■ MC-VA-RW: Rest of the world (all other countries)
Last update (secs. ago)	Time, in seconds, that has elapsed since the licensing table on the licensing client was updated.

Command History

Release	Modification
ArubaOS 8.0.1.0	The **verbose** parameter was added.
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system. The output of this command varies, according to the licenses currently installed on the controller.	Config or Enable mode on Mobility Master.

show lldp interface

```
show lldp interface gigabitethernet <slot/module/port>
```

Description

This command displays the LLDP interfaces information.

Syntax

Parameter	Description
`gigabitethernet <slot/module/port>`	.Displays LLDP information on a gigabitethernet interface.

Example

The example shows two commands. The output of the **show lldp interface** command displays information for all LLDP interfaces.

```
(host) #show lldp interface
LLDP Interfaces Information
---------------------------
Interface LLDP TX LLDP RX LLDP-MED TX interval Hold Timer
--------- ------- ------- -------- ----------- ----------
GE1/3     Enabled Enabled Enabled 30 120
```

The following example only shows information for the GE1/3 interface.

```
(host)[node] #show lldp interface gigabitethernet 0/0/3
Interface: gigabitethernet 0/0/3
LLDP Tx: Enabled, LLDP Rx: Enabled
LLDP-MED: Enabled
Transmit interval: 30, Hold timer: 120
```

Parameter	Description
`Interface`	Name of an LLDP interface.
`LLDP TX`	Shows if LLDP Protocol Data Unit (PDU) transmission is enabled or disabled.
`LLDP RX`	Shows if the managed device has enabled or disabled processing of received LLDP PDUs.
`LLDP-MED`	Shows if LLDP MED protocol is enabled or disabled.
`TX interval`	The LLDP transmit interval, in seconds.
`Hold Timer`	The LLDP transmit hold multiplier.

Command History

Release	Modification
ArubaOS 8.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show lldp neighbor

```
show lldp neighbor interfaces gigabitethernet <slot/module/port> [detail]
```

Description

This command displays information about LLDP peers.

Syntax

Parameter	Description
`gigabitethernet <slot/module/port>`	Displays LLDP information on a gigabitethernet interface.
`detail`	Include details.

Example

The command in the first example below shows that the ports GE0/0/1 and GE0/0/2 recognize each other as an LLDP peers.

```
(host)#show lldp neighbor
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (O)Other
LLDP Neighbor Information
-------------------------
Local Intf Chassis ID Capability Remote Intf Expiry-Time (Secs)
---------- ----------- ----------- ----------- ------------------
GE0/0/1 00:0b:86:6a:25:40 B:R GE0/0/17 105
GE0/0/2 00:0b:86:6a:25:40 B:R GE0/0/18 105
System name
-----------
Aruba 7220
Aruba 7220
Number of neighbors: 2
(host) #show lldp neighbor interface gigabitethernet 0/0/3 detail
Interface: gigabitethernet  0/0/3, Number of neighbors: 1
------------------------------------------------------------
Chassis id: d8:c7:c8:ce:0d:63, Management address: 192.168.0.252
Interface description: bond0, ID: d8:c7:c8:ce:0d:63, MTU: 1522
Device MAC: d8:c7:c8:ce:0d:63
Last Update: Thu Sep 27 10:59:37 2012
Time to live: 120, Expires in: 103 Secs
System capabilities : Bridge,Access point
Enabled capabilities: Access point
System name: IAP-105
System description:
ArubaOS (MODEL: 105), Version 6.1.3.4-3.1.0.0 (35380)
Auto negotiation: Supported, Enabled
Autoneg capability:
10Base-T, HD: yes, FD: yes
100Base-T, HD: yes, FD: yes
1000Base-T, HD: no, FD: yes
Media attached unit type: 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode (30)
MAC: 7c:d1:c3:c7:e9:72: Blacklist
MAC: 9c:b7:0d:7d:0b:72: Blacklist
MAC: 7c:d1:c3:d1:02:c8: Blacklist
```

The output of the **`show lldp neighbor`** command includes the following information:

Parameter	Description
Local Intf	Slot and port number.
Chassis ID	MAC address of the LLDP Peer.
Capability	Shows the capabilities of the peer to operate as a router, bridge, access point, phone or other network device.
Remote Intf	Remote interface.
Expiry-time	Expiry time.
System Name	Name of the peer system, as supplied by the peer.

The output of the **show lldp neighbor interface gigabitethernet <slot/module/port> detail** command varies, depending upon the type of LLDP peer detected. The output in the example above contains the following information:

Parameter	Description
Interface	Name of the port for which you are viewing LLDP neighbor information.
Number of Neighbors	Number of LLDP neighbors seen by the port.
Chassis id	MAC address of the neighbor device.
Management address	MAC address of the neighbor's management port.
Interface description	Description of the LLDP neighbor interface.
ID	Interface ID of the LLDP neighbor interface.
MTU	Maximum Transmission Unit size allowed by the neighbor device in bytes.
Device MAC	Shows the MAC address of the IAP connected to the MAS port.
Last Update	Date and time the neighbor device's status changed.
Time to live	Time, in seconds, for which this information is valid.
Expires in	Time, in seconds, before this information is considered invalid.
System capabilities	This column shows the capabilities of the peer to operate as a router, bridge, access point, phone or other network device.
Enabled capabilities	This column if the peer has been actively configured to operate as a router, bridge, access point, phone or other network device.
System name	Name of the peer system, as supplied by the peer.
System description	Description of the peer system, as supplied by the peer.
Auto negotiation	Shows if link auto-negotiation is enabled for the peer interface.

Parameter	Description
`Media attached unit type`	This parameter displays additional details about an LLDP-MED device attached to the interface. The specific details depend upon the capabilities of the device.
`VLAN`	VLAN ID assigned to the peer interface.
`pvid`	Indicates if the VLAN ID is assigned to the peer access port.
`MAC`	Shows the MAC address of the rogue AP detected by the Instant AP(IAP), which is blacklisted by the MAS.
`LLDP-MED`	Shows details for LLDP-MED (Media Endpoint Discovery), if applicable.
`Device Type`	Type of LLDP-MED device connected to the peer interface.
`Capability`	Capabilities of the LLDP-MED device connected to the peer interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show lldp statistics

```
show lldp statistics  gigabitethernet <slot/module/port>
```

Description

This command displays the LLDP statistics information.

Syntax

Parameter	Description
`gigabitethernet <slot/module/port>`	Displays LLDP information on a gigabitethernet interface.

Usage Guidelines

By default, this command displays LLDP statistics for the entire list of LLDP interfaces. Include a slot/module/port number to display statistics only for that one interface.

Example

The example command below shows LLDP statistics for the Gigabit Ethernet interface **0/0/0**.

```
(host) #show lldp statistics interface gigabitethernet 0/0/0

LLDP Statistics
---------------
Interface             Received  Unknow TLVs  Malformed  Transmitted
---------             --------  -----------  ---------  -----------
gigabitethernet0/0  1249      0            0          1249
```

The output of this command includes the following information:

Parameter	Description
`Interface`	Name of an LLDP interface.
`Received`	Number of packets received on that interface.
`Unknown TLVs`	Number of LLDP Protocol Data Units (PDUs) with an unknown type-length-value (TLV).
`Number of Malformed packets`	Number of malformed packets received on that interface.
`Transmitted`	Number of packets transmitted from that interface.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show local-cert-mac

```
show local-cert-mac
   tag <mac>
```

Description

Display the IP, MAC address and certificate configuration of a managed device in a Mobility Master/managed device configuration.

Syntax

Parameter	Description
`tag <tag>`	IP address of the managed device or MAC address of the managed device.

Usage Guidelines

By default the output of this command shows each managed device's IP and MAC address and the type of certificate used by those managed devices (Custom or Factory). Use the optional **tag** parameter to display information for a managed device only.

Example

The output of this command shows that two managed devices have a custom certificate installed.

```
(host)[node] # show local-cert-mac
Local Switches configured by Local Certificate
-----------------------------------------------
Switch IP of the Local  MAC address of the Local  Cert-Type  CA cert
----------------------  ------------------------  ---------  -------
10.4.62.3               0B:86:F0:12:AC:15         Custom     CAcert
10.4.62.5               00:0B:86:F0:05:60         Custom     Undefined
```

The output of this command includes the following information:

Column	Description
Switch IP of the Local	IP address of the managed device.
MAC address of the Local	MAC address of a managed device with a local certificate.
Cert-Type	Type of certificate used by the local managed device. ■ Custom: User-installed, custom certificate ■ Factory: Factory-installed certificate
CA Cert	Name of the Certificate Authority (CA) certificate.

Related Commands

Command	Description	Mode
local-factory-cert	This command configures the factory-installed certificate for secure communication between a managed device and Mobility Master.	Enable or Config mode on Mobility Master.
local-custom-cert	This command configures a custom certificate for secure communication between a managed device and Mobility Master.	Enable or Config mode on managed device or Mobility Master

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master

show localip

```
show localip
```

Description

Displays the IP address and VPN shared key between master and local.

Syntax

No parameters.

Example

The output of this command shows the managed device's IP address and shared key between Mobility Master and managed devices.

```
(host)[node] # show localip

Local Switches configured by Local Switch IP
--------------------------------------------
Switch IP address of the Local  Key
------------------------------  ---
0.0.0.0                         ********
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

show localipv6

```
show localipv6
```

Description

Shows the IP address and preshared key for the managed device on a Mobility Master.

Syntax

Parameter	Description
<tag>	Show VPN configuration of a specific Local Switch or Output Modifiers.

Example

This example shows the IPv4 and IPv6 addresses configured .

```
(host) [mynode] (config) #show localipv6
Local Switches configured by Local Switch IPv6
----------------------------------------------
Switch IPv6 address of the Local  Corres IPv4 address of the Local  Key
------------------------------  ------------------------------  ---
2002::1                         1.1.1.1                         ********
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show local-peer-mac

```
show local-peer-mac tag <local-mac-addr>
```

Description

This command is used to display the MAC address used for secure communication based between Mobility Master and managed devices.

Syntax

Parameter	Description
`tag <local-mac-addr>`	The managed device's MAC address.

Example

Include the optional tag<local-mac-addr>

```
(host) [mynode] (config) #local-peer-mac 00:0c:29:00:00:00 ipsec 123456
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

show local-userdb

```
show local-userdb
   maximum-expiration
   start <offset>
   page <page-size>
   username <username>
   verbose
```

Description

Shows information about user's accounts in the local user database.

Syntax

Parameter	Description
`maximum-expiration`	How long the account is valid, in minutes, in the internal database.
`start <offset>`	Display records starting at a specific database record number defined by the <offset> parameter.
`page <page-size>`	Number of user entries to display .
`username <username>`	Show data for a specific user.
`verbose`	Display the following additional details for each database entry. ■ Full-Name ■ Company ■ Phone ■ Comments ■ Start-Date ■ Creation-Date ■ Sponsor-Fullname ■ Sponsor-Email ■ Sponsor-Dept ■ Opt-Field-1 ■ Opt-Field-2 ■ Opt-Field-3 ■ Opt-Field-4 ■ Grantor-Role ■ VLAN ■ NASIP

Usage Guidelines

Issue this command without any parameters to display a general overview of user's accounts in the database. Use the **maximum-expiration** parameter to show how long the account is valid for in minutes. Use the **start <offset> page <page_size>** parameters to control which user account records in the database display initially and the number of account records displayed on a page.

Example

This example shows the basic summary of user accounts in the database.

```
(host)[node] #show local-userdb maximum-expiration start 5 page 4
```

```
local-userdb maximum-expiration 90

User Summary
------------
Name           Password  Role   E-Mail  Enabled  Expiry  Status  Sponsor-Name  Grantor-Name
----           --------  ----   ------  -------  ------  ------  ------------  ------------
guest-0657984  ********  guest          Yes              Active                admin
guest-8330301  ********  guest          Yes              Active                admin
guest-5433352  ********  guest          Yes              Active                admin
guest-3469360  ********  guest          Yes              Active                admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the user.
`Password`	The user's password.
`Role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
`E-mail`	Shows the email address of the user account.
`Enabled`	Shows whether the account is enabled or disabled.
`Expiry`	Shows the expiration date for the user account. If this is not set, the account does not expire.
`Status`	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
`Sponsor-Name`	Shows the sponsor's name.
`Grantor-Name`	Shows the grantor's name.
`User Entries`	Shows the number of user accounts in the database.

Related Commands

Command	Description
local-userdb add	Use this command to configure the parameters displayed in the output of this show command.
local-userdb-guest add	Use this command to configure parameters for a guest user account.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master.

show local-userdb-guest

```
show local-userdb-guest
   maximum-expiration
   start <offset>
   page <page-size>
   username <username>
   verbose
```

Description

Shows information about guest accounts in the local user database.

Syntax

Parameter	Description
`maximum-expiration`	How long the account is valid, in minutes, in the internal database.
`start <offset>`	Display records starting at a specific database record number defined by the <offset> parameter.
`page <page-size>`	Number of user entries to display .
`username <username>`	Show data for a specific user.
`verbose`	Display the following additional details for each database entry. ■ Full-Name ■ Company ■ Phone ■ Comments ■ Start-Date ■ Creation-Date ■ Sponsor-Fullname ■ Sponsor-Email ■ Sponsor-Dept ■ Opt-Field-1 ■ Opt-Field-2 ■ Opt-Field-3 ■ Opt-Field-4 ■ Grantor-Role ■ VLAN ■ NASIP

Usage Guidelines

Issue this command without any parameters to display a general overview of guest accounts in the database. Use the **maximum-expiration** parameter to show how long the account is valid for in minutes. Use the **start <offset> page <page_size>** parameters to control which guest account records in the database display initially and the number of account records displayed on a page.

Example

This example shows the basic summary of guest user accounts in the database.

```
(host)[node] #show local-userdb-guest maximum-expiration start 5 page 4
```

```
local-userdb-guest maximum-expiration 90

Guest UserSummary
-----------------
Name           Password  Role   E-Mail  Enabled  Expiry  Status  Sponsor-Name  Grantor-Name
----           --------  ----   ------  -------  ------  ------  ------------  ------------
guest-0657984  ********  guest          Yes              Active                admin
guest-8330301  ********  guest          Yes              Active                admin
guest-5433352  ********  guest          Yes              Active                admin
guest-3469360  ********  guest          Yes              Active                admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
Name	Name of the user.
Password	The user's password.
Role	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
E-mail	Shows the email address of the user account.
Enabled	Shows whether the account is enabled or disabled.
Expiry	Shows the expiration date for the user account. If this is not set, the account does not expire.
Status	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
Sponsor-Name	Shows the sponsor's name.
Grantor-Name	Shows the grantor's name.
User Entries	Shows the number of user accounts in the database.

Related Commands

Command	Description
local-userdb add	Use this command to configure the parameters displayed in the output of this show command.
local-userdb-guest add	Use this command to configure parameters for a guest user account.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master.

show local-userdb-public-access

```
show local-userdb-public-access
   maximum-expiration
   start <offset>
   page <page-size>
   username <username>
   verbose
```

Description

Shows information about public-access user accounts in the local user database.

Syntax

Parameter	Description
`maximum-expiration`	How long the account is valid, in minutes, in the internal database.
`start <offset>`	Display records starting at a specific database record number defined by the <offset> parameter.
`page <page-size>`	Number of user entries to display .
`username <username>`	Show data for a specific user.
`verbose`	Display the following additional details for each database entry. ■ Full-Name ■ Company ■ Phone ■ Comments ■ Start-Date ■ Creation-Date ■ Sponsor-Fullname ■ Sponsor-Email ■ Sponsor-Dept ■ Opt-Field-1 ■ Opt-Field-2 ■ Opt-Field-3 ■ Opt-Field-4 ■ Grantor-Role ■ VLAN ■ NASIP

Usage Guidelines

Issue this command without any parameters to display a general overview of guest accounts in the database. Use the **maximum-expiration** parameter to show how long the account is valid for in minutes. Use the **start <offset> page <page_size>** parameters to control which account records in the database display initially and the number of account records displayed on a page.

Example

This example shows the basic summary of public access user accounts in the database.

```
(host)[node] #show local-userdb-guest maximum-expiration start 5 page 4
local-userdb-guest maximum-expiration 90
```

```
Guest UserSummary
-----------------
Name           Password  Role   E-Mail  Enabled  Expiry  Status  Sponsor-Name  Grantor-Name
----           --------  ----   ------  -------  ------  ------  ------------  ------------
guest-0657984  ********  guest          Yes              Active                admin
guest-8330301  ********  guest          Yes              Active                admin
guest-5433352  ********  guest          Yes              Active                admin
guest-3469360  ********  guest          Yes              Active                admin

User Entries: 11
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the user.
`Password`	The user's password.
`Role`	Role for the user. This role takes effect when the internal database is specified in a server group profile with a server derivation rule. If there is no server derivation rule configured, then the user is assigned the default role for the authentication method.
`E-mail`	Shows the email address of the user account.
`Enabled`	Shows whether the account is enabled or disabled.
`Expiry`	Shows the expiration date for the user account. If this is not set, the account does not expire.
`Status`	Shows whether the profile has enabled or disabled the ability to use the HTTP protocol to redirect users to the captive portal page.
`Sponsor-Name`	Shows the sponsor's name.
`Grantor-Name`	Shows the grantor's name.
`User Entries`	Shows the number of user accounts in the database.

Related Commands

Command	Description
local-userdb add	Use this command to configure the parameters displayed in the output of this show command.
local-userdb-guest add	Use this command to configure parameters for a guest user account.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master

show localip

```
show localip
```

Description

Displays the IP address and VPN shared key between master and local.

Syntax

No parameters.

Example

The output of this command shows the managed device's IP address and shared key between Mobility Master and managed devices.

```
(host)[node] # show localip

Local Switches configured by Local Switch IP
--------------------------------------------
Switch IP address of the Local  Key
------------------------------  ---
0.0.0.0                         ********
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

show log all

```
show log all|ap-debug|arm|arm-user-debug|errorlog|network|security|system|user|user-debug|wireless  [<number>]
```

Description

Show the log files on Mobility Master or a managed device.

Syntax

Parameter	Description
`all`	Issue the command **show log all** to display all log files. Include this parameter after one of the log file types (for example, **show log security all**) to display all log files of the selected type.
`ap-debug`	Display AP debug log files.
`arm`	Display ARM log files.
`arm-user-debug`	Display ARM user debug log files.
`errorlog`	Display error log files.
`network`	Display network log files.
`<number>`	Include this parameter at the end of the show log command to start displaying the log output from the specified number of lines from the end of the log.
`security`	Display security log files.
`system`	Display system log files.
`user`	Display user log files.
`user-debug`	Display user debug log files.
`wireless`	Display wireless log files.

Example

This example shows the most ten recent security log entries for the controller.

```
(host)[node] (config) #show log security 5
May 2 02:11:51 :125022:  <WARN> |aaa|  Authentication failed for User admin, Logged in from 10.20.34.2 port 62419, Connecting to 10.16.13.18 port 22 connection type SSH
May 2 02:20:03 :126005:  <WARN> |wms| |ids| Interfering AP: The system classified an access point (BSSID 94:b9:0f:15:6f:63 and SSID hpn-byod on CHANNEL 6) as interfering. Additional Info: Detector-AP-Name:40:e3:d6:cf:61:96; Detector-AP-MAC:40:e3:d6:76:19:64; Detector-AP-Radio:2.
May 2 02:26:13 :126005:  <WARN> |wms| |ids| Interfering AP: The system classified an access point (BSSID 94:b9:0f:15:6f:60 and SSID ethersphere-wpa2 on CHANNEL 6) as interfering. Additional Info: Detector-AP-Name:40:e2:d6:c1:dc:ae; Detector-AP-MAC:40:e2:d6:8d:ca:e0; Detector-AP-Radio:2.
```

```
May 2 02:33:47 :126005:  <WARN> |wms| |ids| Interfering AP: The system classified an access
point (BSSID ac:a3:1e:56:ac:70 and SSID  on CHANNEL 40) as interfering. Additional Info:
Detector-AP-Name:40:e3:d6:cf:61:96; Detector-AP-MAC:40:e3:d6:76:19:70; Detector-AP-Radio:1.
May 2 02:39:24 :126005:  <WARN> |wms| |ids| Interfering AP: The system classified an access
point (BSSID 94:b4:0f:15:6f:61 and SSID ethersphere-voip on CHANNEL 6) as interfering.
Additional Info: Detector-AP-Name:40:e3:d6:c0:dc:ae; Detector-AP-MAC:40:e3:d6:8d:ca:e0;
Detector-AP-Radio:2.
Mar  3 13:57:53  localdb[567]: <133006> <ERRS> |localdb|  User admin Failed Authentication
Mar  3 13:57:53  localdb[567]: <133019> <ERRS> |localdb|  User admin was not found in the
database
Mar  3 13:57:53  localdb[567]: <133019> <ERRS> |localdb|  User admin was not found in the
database
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master

show log ap-debug

```
show log ap-debug{[<number>][all]}
```

Description

Show the controller's AP debug logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the AP debug logs for the controller.

Example

This example shows the ten most recent AP debug logs for the controller.

```
(host)[node] #show log ap-debug 10

Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): Copyright (c) 2005-2006 Atheros Communications, Inc.
All Rights Reserved
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi0: Base BSSID 00:1a:1e:25:97:d0, 16 available
BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): wifi1: Base BSSID 00:1a:1e:25:97:c0, 16 available
BSSID(s)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): edev->dev_addr=00:1a:1e:ca:59:7c
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21):  ^H<6>Ethernet Channel Bonding Driver: v3.0.1
(January 9, 2006)
Nov 24 20:54:24  KERNEL(AP39@10.6.1.21): secure_jack_link_state_change: Error finding device
eth0
Nov 24 20:54:25  KERNEL(AP39@10.6.1.21): Kernel watchdog refresh ended.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show log arm-user-debug

```
show log arm-user-debug{[<number>][all]}
```

Description

Show the controller's ARM user debug logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the ARM user debug logs for the controller.

Example

This example shows the controller's last ten ARM user debug logs.

```
(host)[node] #show log arm-user-debug 10

Aug 12 16:03:03 :508164:  <DBUG> |ARM Process|  Client Match: Found 11v Capable STA
b0:ee:45:49:60:3c
Aug 12 16:03:03 :508201:  <DBUG> |ARM Process|  Client Match: Sending BSS transition req to
client b0:ee:45:49:60:3c token 14
Aug 12 16:03:03 :508202:  <DBUG> |ARM Process|  Client Match: Timer started for BTM response
STA b0:ee:45:49:60:3c timerid 5176652
Aug 12 16:03:06 :508161:  <DBUG> |ARM Process|  Client Match Received probe report: AP
6c:f3:7f:e7:1d:20 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk for client b0:ee:45:49:60:3c
with signal -44
Aug 12 16:03:06 :508161:  <DBUG> |ARM Process|  Client Match Received probe report: AP
d8:c7:c8:46:e0:00 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk for client b0:ee:45:49:60:3c
with signal -38
Aug 12 16:03:06 :508161:  <DBUG> |ARM Process|  Client Match Received probe report: AP
6c:f3:7f:e7:1d:20 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk for client b0:ee:45:49:60:3c
with signal -35
Aug 12 16:03:11 :508161:  <DBUG> |ARM Process|  Client Match Received probe report: AP
d8:c7:c8:46:e0:00 ESSID sganu-wpa2-psk Assoc ESSID sganu-wpa2-psk for client b0:ee:45:49:60:3c
with signal -36
Aug 12 16:03:13 :508203:  <DBUG> |ARM Process|  Client Match: Timer cleared for BTM response
STA b0:ee:45:49:60:3c timerid 5176652
Aug 12 16:03:13 :508186:  <DBUG> |ARM Process|  Client Match: Tracking unsuccessful failure
for client b0:ee:45:49:60:3c num fails 0 btm rejects 0 btm timeouts 4
Aug 12 16:03:13 :508185:  <DBUG> |ARM Process|  Client Match: move status: Uncontrolled-Radio
complete move for client b0:ee:45:49:60:3c from Source AP ap135 d8:c7:c8:46:e0:00 Eff_Signal -
0 dBm (Signal -0 dBm EIRP 0 dBm) to Target AP ac 6c:f3:7f:e7:1d:20 Eff_Signal -0 dBm (Signal -
0 dBm EIRP 0 dBm) Actual AP ap135 d8:c7:c8:46:e0:00 Time diff 9 Reason Denied; User action
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show log bssid-debug

```
show log bssid-debug{[<number>][all]}
```

Description

A Basic Service Set Identifier (BSSID) uniquely defines each wireless client and Wireless Broadband Router. This command shows the controller's BSSID debug logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the BSSID debug logs for the controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show log errorlog

```
show log errorlog{[<number>][all]}
```

Description

Show the controller's system errors and other critical information.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the error logs for the controller.

Example

This example shows the ten most recent system log errors.

```
(host)[node] #show log errorlog 10

Mar 5 10:30:34 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue
AP detected with SSID cto-dnh-blah, BSSID 00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and
IP 10.3.49.254
Mar 5 10:31:39 <sapd 404080>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: ADHOC
network detected with Src 00:13:ce:45:91:a0, BSSID 02:13:ce:2d:37:50, ESSID adhoc_ap70 Channel
11 and RSSI 22
Mar 5 10:32:12 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue
AP detected with SSID cto-dnh-blah, BSSID 00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and
IP 10.3.49.254
Mar 5 10:32:46 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue
AP detected with SSID cto-dnh-blah, BSSID 00:0b:86:b5:86:c0, Wired MAC 00:0b:86:02:ee:00, and
IP 10.3.49.254
Mar 5 10:40:32 <localdb 133019>  <ERRS> |localdb|  User admin was not found in the database
Mar 5 10:40:32 <localdb 133006>  <ERRS> |localdb|  User admin Failed Authentication
Mar 5 10:41:10 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue
AP detected with SSID sw-rlo-open, BSSID 00:0b:86:c9:9e:20, Wired MAC 00:00:00:00:00:00, and
IP 0.0.0.0
Mar 5 10:41:31 <sapd 106007>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Rogue
AP detected with SSID QA_MARORA_VOCERA, BSSID 00:0b:86:c9:9e:21, Wired MAC 00:0b:86:02:ee:00,
and IP 10.3.49.254
Mar 5 10:48:01 <sapd 404080>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: ADHOC
network detected with Src 00:13:ce:45:d9:4d, BSSID 02:13:ce:28:40:48, ESSID adhoc_ap70 Channel
11 and RSSI 8
Mar 5 11:04:21 <sapd 404080>  <ERRS> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: ADHOC
network detected with Src 00:13:ce:45:d9:4d, BSSID 02:13:ce:2d:37:50, ESSID adhoc_ap70 Channel
11 and RSSI 9
```

Command HistoryCommand History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show log essid-debug

```
show log essid-debug{[<number>][all]}
```

Description

Show the controller's ESSID debug logs.

An Extended Service Set Identifier (ESSID) is used to identify the wireless clients and Wireless Broadband Routers in a WLAN. All wireless clients and Wireless Broadband Routers in the WLAN must use the same ESSID.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the ESSID debug logs for the controller.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master or managed devices

show log network

```
show log network{[<number>][all]}
```

Description

Show the controller's system network errors.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the network logs for the controller.

Example

This example shows the controller's recent network log errors

```
(host)[node] #show log network all

Feb 17 14:47:14 :209801:  <WARN> |fpapps|  Physical link down: port 1/1
Feb 17 14:48:04 :209801:  <WARN> |fpapps|  Physical link down: port 1/1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master or managed devices

show log security

```
show log security{[<number>][all]}
```

Description

Show the controller's security logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the security logs for the controller.

Example

This example shows the controller's last seven security logs.

```
(host)[node] #show log security 7

Mar 5 11:53:43 :124004:  <DBUG> |authmgr|  Local DB auth failed for user admin, error (User
not found in UserDB)
Mar 5 11:53:43 :124003:  <INFO> |authmgr|  Authentication result=Authentication failed(1),
method=Management, server=Internal, user=10.100.100.66
Mar 5 11:53:43 :124004:  <DBUG> |authmgr|  Auth server 'Internal' response=1
Mar 5 11:53:43 :125027:  <DBUG> |aaa|  mgmt-auth: admin, failure, , 0
Mar 5 11:53:43 :125024:  <NOTI> |aaa|  Authentication Succeeded for User admin, Logged in from
10.100.100.66 port 1778, Connecting to 10.3.49.100 port 22 connection type SSH
Mar 5 11:53:58 :103060:  <DBUG> |ike|  ipc.c:ipc_get_cfgm_role:2826 Sending REQUEST for CFGM
Role
Mar 5 11:53:58 :103060:  <DBUG> |ike|  ipc.c:get_local_cfg_trigger_ike:2653 IKE got trigger
from CFGM : state :3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master or managed devices

show log system

```
show log system{[<number>][all]}
```

Description

Show the controller's system logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the system logs for the controller.

Example

This example shows the controller's last ten system logs.

```
(host)[node] #show log system 10

Mar 5 11:55:59 :316073:  <DBUG> |wms|  Received New AP Message: AP 00:0b:86:b5:87:c2 Status 1
Num-WM 0
Mar 5 11:55:59 :316083:  <DBUG> |wms|  mysql: UPDATE ap_table SET ssid='qa-abu-customerissue',
current_channel='11', type='generic-ap', ibss='no', phy_type='80211g', rap_type='interfering',
match_mac='00:00:00:00:00:00', power_level='255', status='up' WHERE id='71575' ;
Mar 5 11:55:59 :316029:  <DBUG> |wms|  Sending message to Probe: IP:10.3.49.253 Msg-
Type:PROBE_RAP_TYPE  AP 00:0b:86:b5:87:c2 Type:1
Mar 5 11:55:59 :316036:  <DBUG> |wms|  Received New STA Message: MAC 00:0b:86:b5:87:c2 Status
0
Mar 5 11:55:59 :316032:  <DBUG> |wms|  STA Probe: ADD Probe 00:0b:86:a2:e7:40 for STA
00:0b:86:b5:87:c2
Mar 5 11:56:00 :399814:  <DBUG> |fpapps|  PoE: RAN THRU ITERATION 2
Mar 5 11:56:00 :326001:  <DBUG> |AP 1.1.1@10.3.49.253 sapd|  AM: am_read_bss_data_stats: radio
0: pktsIn 0 pktsOut 0 bytesIn 0 bytesOut 0
Mar 5 11:56:00 :326001:  <DBUG> |AP 1.1.1@10.3.49.253 sapd|  AM: am_read_bss_data_stats: radio
0: pktsIn 0 pktsOut 52107 bytesIn 0 bytesOut 18143486
Mar 5 11:56:01 :326001:  <DBUG> |AP 1.1.1@10.3.49.253 sapd|  AM: MPPS 2722 CPPS 338 PKTS
452036609 BYTES 2062458092 INTR 334327351
Mar 5 11:56:02 :399814:  <DBUG> |fpapps|  PoE: Evaluating port 1/5 rv is 0 and crv is 1
state :3
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master or managed devices

show log user

```
show log user{[<number>][all]}
```

Description

Show the controller's user logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the user logs for the controller.

Example

This example shows the controller's last ten user logs.

```
(host)[node] #show log user 10

Mar 5 13:29:57 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:32:08 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:36:41 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:38:42 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:40:41 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:42:51 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:47:03 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:49:07 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:53:08 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
Mar 5 13:55:14 :501083:  <WARN> |stm|  Probe request: 00:0b:86:cd:1a:00: Invalid Station MAC
address from AP 10.3.49.253-00:0b:86:a2:e7:40-1.1.1
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show log user-debug

```
show log user-debug{[<number>][all]}
```

Description

Show the controller's user debug logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the user debug logs for the controller.

Example

This example shows the controller's last ten user debug logs.

```
(host)[node] #show log user-debug 10

Mar 5 13:57:24 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:57:24 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:41-1.1.1 SSID
Mar 5 13:58:26 :501082:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:58:26 :501085:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:26 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:26 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:41-1.1.1 SSID
Mar 5 13:58:27 :501082:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1
Mar 5 13:58:27 :501085:  <DBUG> |stm|  Probe request: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:27 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:40-1.1.1 SSID
Mar 5 13:58:27 :501090:  <DBUG> |stm|  Probe response: 00:18:f8:ab:77:a4: AP 10.3.49.253-
00:0b:86:a2:e7:41-1.1.1 SSID
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show log wireless

```
show log wireless{[<number>][all]}
```

Description

Show the controller's wireless logs.

Syntax

Parameter	Description
`<number>`	Start displaying the log output from the specified number of lines from the end of the log.
`all`	Shows all the wireless logs for the controller.

Example

This example shows the controller's last ten wireless logs.

```
(host)[node] #show log wireless 10

Mar 5 13:59:31 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID mak-cp-psk and BSSID 00:0b:86:8b:70:20
Mar 5 13:59:35 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID  and BSSID 00:0b:86:c0:06:83
Mar 5 13:59:38 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID  and BSSID 00:0b:86:c0:06:85
Mar 5 13:59:41 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID  and BSSID 00:0b:86:89:f9:42
Mar 5 13:59:41 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID QA-SANJAY-OSUWIRELESS and BSSID 00:0b:86:89:f9:40
Mar 5 13:59:44 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID QA-SANJAY-OSUVOICE and BSSID 00:0b:86:8c:fb:c0
Mar 5 13:59:44 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID Google and BSSID 00:0b:86:4f:82:c0
Mar 5 13:59:47 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID QA-SANJAY-OSUVOICE and BSSID 00:0b:86:89:f9:41
Mar 5 13:59:50 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID  and BSSID 00:0b:86:c0:06:86
Mar 5 13:59:50 :404003:  <WARN> |AP 1.1.1@10.3.49.253 sapd|  AM 00:0b:86:a2:e7:40: Interfering
AP detected with SSID cto-dnh-blah and BSSID 00:0b:86:60:b8:80
```

Command History

This command was available in ArubaOS 3.0.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show logging

```
show logging facility|server|{level [verbose]}
```

Description

the IP address of the remote logging server, as well as facility log types and their associated facility levels.

Syntax

Parameter	Description
`facility`	View the facility used when logging messages into the remote syslog server.
`server`	Show the IP address of a remote logging server.
`level [verbose]`	Show logging levels at which the messages are logged. Include the optional verbose parameter to display additional data for logging subcategories and processes.

Usage Guidelines

The ArubaOS logging levels follow syslog convention:

- level 7: Emergency
- level 6: Alert
- level 5: Critical
- level 4: Errors.
- level 3: Warning
- level 2:Notices
- level 1:Informational
- level 0: Debug

The default logging level is **leve1 1**. You can change this setting via the **logging** command.

Example

This example below displays defined logging levels for each logging facility.

```
(host)[node] #show logging level

LOGGING LEVELS
--------------
Facility  Level
--------  -----
network   warnings
security  warnings
system    warnings
user      warnings
wireless  warnings
```

This example below displays the IP address of a remote log server. If a remote log server has not yet been defined, this command will not display any output.

```
(host)[node] #show logging server
```

```
Remote Server: 1.1.1.1

FACILITY MAPPING TABLE
----------------------
local-facility  severity   remote-facility
--------------  --------   ---------------
user            debugging  local1
```

Related Commands

Command	Description
logging	Use this command to specify the IP address of the remote logging server, as well as facility log types and their associated facility levels.

Command History

Version	Description
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master

show loginsessions

```
show loginsessions
```

Description

Displays the current administrator login sessions statistics.

Syntax

No parameters.

Example

Issue this command to display the admin login session statistics.

```
Session Table
-------------
ID  User Name  User Role  Connection From  Idle Time  Session Time
--  ---------  ---------  ---------------  ---------  ------------
1   admin      root       10.100.102.43    00:00:00   00:27:59
```

The output includes the following parameters:

Parameter	Description
`ID`	Sessions identification number
`User Name`	Administrator's user name
`User Role`	Administrator's role
`Connection From`	The IP address from which the administrator is connecting
`Idle Time`	Amount of time the user has been idle
`Session Time`	Total time the session has been open

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Configuration mode on Mobility Master

show mac-address-table

```
show mac-address-table
```

Description

Displays a MAC forwarding table.

Syntax

No parameters.

Example

Issue this command to display the MAC forwarding table.

```
Dynamic Address Count:           0
Static Address (User-defined) Count:             0
System Self Address Count:               0
Total MAC  Addresses :           6
Maximum MAC addresses :                  6
MAC Address Table
------------------
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
00:0b:86:00:00:00    Mgmt          1     vlan 1
00:0b:86:f0:05:60    Mgmt          1     vlan 1
00:0b:86:00:00:00    Mgmt          62    vlan 62
00:0b:86:f0:05:60    Mgmt          62    vlan 62
00:0b:86:00:00:00    Mgmt          4095  vlan 4095
00:0b:86:f0:05:60    Mgmt          4095  vlan 4095
```

The output includes the following parameters:

Parameter	Description
`Dynamic Address Count`	Count of dynamic addresses currently associated with the managed device.
`Static Address (User-defined) Count`	Count of static, user-defined addresses associated with the managed device.
`System Self Address Count`	Number of self system addresses.
`Total MAC Addresses`	Total number of MAC addresses associated with the managed device.
`Maximum MAC Addresses`	Maximum number of MAC addresses.
`Destination Address`	Destination MAC address.
`Address Type`	Destination address type.
`VLAN`	Associated VLAN.
`Destination Port`	Destination port.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show master-configpending

```
show master-configpending
```

Description

Displays the list of global commands which are not saved and are not sent to the managed device.

Syntax

No parameters.

Example

This example below displays the commands which are not saved and are not sent to the managed device.

```
(host) #show master-configpending

aaa profile "default-xml-api"
aaa xml-api server "10.17.93.2"
aaa xml-api server "10.17.93.2"
aaa xml-api server "10.17.93.2" key "12345678"
aaa profile "default-xml-api"
aaa profile "default-xml-api" xml-api-server "10.17.93.2"
user-role "logon"
user-role "logon" captive-portal "default"
user-role "logon"
user-role "logon" no captive-portal "default"
user-role "logon"
user-role "logon" captive-portal "default"
voice rtp-analysis-config
voice rtp-analysis-config rtp-analysis
voice rtp-analysis-config rtp-analysis
voice rtp-analysis-config no rtp-analysis
voice rtp-analysis-config rtp-analysis
```

Related Commands

Command	Description
master-redundancy	This command associates a VRRP instance with Mobility Master redundancy.
master-local	This command displays the statistics between the managed device and Mobility Master.
switches	This command provides the details on the switches connected to Mobility Master, including Mobility Master itself.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Master.

show master-local stats

```
show master-local stats [<ip-addr>] [<page>]
```

Description

Display statistics for communication between Mobility Master and managed devices.

Syntax

Parameter	Description
`<ip-addr>`	Include the IP address of a managed device to display statistics that managed device only.
`<page>`	Start displaying the output of this command at the specified page number.

Usage Guidelines

By default, Mobility Master and managed devices exchange heartbeat messages every 10 seconds. These Heartbeats include a configuration timestamp. If a Mobility Master has later timestamp than the managed device, the state of the managed device changes from 'Update Successful' to 'Update Required'.

Example

This example below shows statistics for all communications between the Mobility Master and the managed devices.

```
(host) [mynode] #show master-local stats

Missed -> HB Resp from Master
-----------------------------
IP Address  HB Req      HB Resp     Total Missed  Last Sent Missed  Peer Reset  Cfg Terminate
Last Synced
----------  ------      -------     ------------  ----------------  ----------  -------------
-----------
10.6.2.252  194721      194208      926           0                 105         1
Thu Feb 26 21:12:04 2009
```

The output of this command includes the following data columns:

Parameter	Description
`IP Address`	IP address of the managed device.
`HB Req`	Heartbeat requests sent from the managed device.
`HB Resp`	Heartbeat responses sent from the Mobility Master.
`Total Missed`	Total number of heartbeats that were not received by the managed device.
`Last Sent Missed`	This counter will increment if the managed device misses the last heartbeat from the peer managed device. This counter will keep on incrementing until the heartbeat message is received from peer.

Parameter	Description
`Peer Reset`	The number of times the connection to peer is been reset. The connection could reset due to network connectivity problems or when the peer switch reboots.
`Cfg Terminate`	Number of times the managed device has failed to upgrade to a new configuration
`Last Synced`	Timestamp showing the last time the managed device synched its configuration from the Mobility Master.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show master-l3redundancy

```
show master-l3redundancy {config-sync|status}
```

Description

Displays the Layer-3 configuration and database sync status as well as the current status of Layer-3-domain Mobility Master redundancy.

Syntax

Parameter	Description
`config-sync <status>`	Displays Layer-3 configuration and database sync status.
`status`	Displays current status of L3-domain master redundancy.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Examples

The example below executed on the managed device displays the health of primary and secondary data centers.

```
(host) #show master-l3redundancy status
L3 Redundancy Status

--------------------

Role IP Address Status

---- ---------- ------

Master 10.9.196.151 Down

Secondary Master 10.9.196.152 Up
```

The example below executed on the managed device displays Layer-3 redundancy configuration.

```
(host) #show master-l3redundancy

L3 Sync Role:Primary

L3 Redundant Peer IP:10.9.196.154

IKE PSK: 16c591a3789da6eef4420a5fe45967c3f1cf1bc457464244
```

The example below executed on the managed device displays the L3 configuration and database sync status.

```
(host)# show master-l3redundancy config-sync state

(host)# show database synchronize
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on managed device.

show master-redundancy

```
show master-redundancy
```

Description

Display the Mobility Master's redundancy configuration.

Syntax

No parameters.

Example

This example below shows the current master redundancy configuration, including the ID number of the master VRRP virtual router and the IP address of the peer managed device for master redundancy.

```
(host) [mynode] (config) #show master-redundancy
Master redundancy configuration:
    VRRP Id 120 current state is MASTER
    Peer's IP Address is 10.17.65.117
    Peer's IPSEC Key is ********
```

Related Commands

Command	Description
master-redundancy master-vrrp	This command associates a VRRP instance with Mobility Master redundancy.
vrrp	This command configures the VRRP.
master-redundancy peer-ip	This command configures the IP address and preshared key or certificate for a redundant Mobility Master on another Mobility Master.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show memory

```
show memory
   aaa
   amon_recvr
   amon_sender
   ap {ble_daemon|llpd|meshd|ofald|rapper|rfd|sapd|stm}
      {ap-name <ap-name>}|{bssid <bssid>}|{ip-addr <ip-addr>}
   apprf
   arci-cli-helper
   arm
   auth
   ble_relay
   certmgr
   cfgdist
   cfgm
   cli
   cluster_mgr
   cpsec
   ctrlmgmt
   dbsync
   dds
   debug
   dhcpd
   dhcpdwrap
   ecc
   fpapps
   fw_visibility
   gsmmgr
   ha_mgr
   ip_flow_export
   isakmpd
   l2tpd
   lagm
   licensemgr
   lldpd
   mdns
   mobileip
   mon_serv
   ofa
   ospf
   phonehome
   pim
   pptpd
   profmgr
   rtpa
   slb
   snmpd
   stm
   syslogdwrap
   ucm
   udbserver
   upgrademgr
   vrrp
   web_cc
   wms
   <cr>
```

Description

This command displays the availability of used and available memory on Mobility Master, or include a process name to show memory information for a process on the AP or Mobility Master.

Syntax

Parameter	Description
`aaa`	Displays memory information for the AAA process.
`amon_recvr`	Displays the memory information for the **amon_recvr** process.
`amon_sender`	Displays the memory information for the **amon_sender** process
`ap`	Displays memory information for a process running on a specific AP or BSSID. ■ **ble_daemon**: Displays the memory information for the ble_daemon process. ■ **lldpd**: Displays the memory information for the LLDP process. ■ **meshd**: Displays the memory information for the meshd process. ■ **ofald**: Displays the memory information for the OpenFlow Agent Lite Daemon process. ■ **rapper**: Displays the memory information for the rapper process. ■ **rfd**: Displays the memory information for the rfd process. ■ **sapd**: Displays the memory information for the sapd process. ■ **stm**: Displays the memory information for the AP stm process.
`apprf`	Displays the memory information for the AppRF process.
`arci-cli-helper`	Displays the memory information for the arci-cli-helper process.
`arm`	Displays the memory information for the ARM process.
`auth`	Displays the memory information for the authentication process.
`ble_relay`	Displays the memory information for the ble relay process.
`certmgr`	Displays the memory information for the certmgr process.
`cfgdist`	Displays the memory information for the cfgdist process.
`cfgm`	Displays the memory information for the cfgm process.
`cli`	Displays the memory information for the cli process.

Parameter	Description
cluster_mgr	Displays the memory information for the cluster_mgr process.
cpsec	Displays the memory information for the cpsec process.
ctrlmgmt	Displays the memory information for the ctrlmgmt process.
dbsync	Displays the memory information for the dbsync process.
dds	Displays the memory information for dds process.
debug	Displays detailed memory information to debug memory errors.
dhcpd	Displays the memory information for the DHCP process.
dhcpdwrap	Displays the memory information for the dhcpdwrap process.
ecc	Displays the DRAM ecc counters.
fpapps	Displays the memory information for the fpapps process.
fw_visibility	Displays the memory information for the fw_visibility process.
gsmmgr	Displays the memory information for gthe smmgr process.
ha_mgr	Displays the memory information for the HA_MGR process.
ip_flow_export	Displays the memory information for the ip flow export process.
isakmpd	Displays the memory information for the isakmpd process.
l2tpd	Displays the memory information for the l2tpd process.
lagm	Displays the memory information for the lagm process.
licensemgr	Displays the memory information for the licensemgr process.
lldpd	Displays the memory information for the lldpd process.
mdns	Displays the memory information for the mDNS process.
mobileip	Displays the memory information for the mobileip process.
mon_serv	Displays the memory information for the mon_serv process.
ofa	Displays the memory information for the OpenFlow Agent process.

Parameter	Description
ospf	Displays the memory information for the OSPF process.
phonehome	Displays the memory information for the phonehome process.
pim	Displays the memory information for the pim process.
pptpd	Displays the memory information for the pptpd process.
profmgr	Displays the memory information for the profmgr process.
rtpa	Displays the memory information for the rtpa process.
slb	Displays the memory information for the slb process.
snmpd	Displays the memory information for the snmpd process.
stm	Displays the memory information for the stm process.
syslogdwrap	Displays the memory information for the syslogdwrap process.
ucm	Displays the memory information for the UCM process.
udbserver	Displays the memory information for the udbserver process.
upgrademgr	Displays the memory information for the upgrademgr process.
vrrp	Displays the memory information for the vrrp process.
web_cc	Displays the memory information for the WebCC process.
wms	Displays the memory information for the WMS process.

Usage Guidelines

Include the name of a process to show memory information for that process. Use this command under the supervision of Aruba technical support to help debug process errors.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The command **show memory** displays, in Kilobytes, the total memory on Mobility Master, the amount of memory currently being used, and the amount of free memory.

```
(host) [mynode] #show memory

Memory (Kb): total: 256128, used: 162757, free: 93371
```

Include the name of a process to show memory statistics for that process. The example below shows memory statistics for **mobileip**.

```
(host) [mynode] #show memory mobileip
```

```
Type           Num Allocs     Size Allocs      Peak Allocs      Peak Size
------         ------------   -------------    -------------    -----------
default              1947          336545             2027         336698

PC                   Allocs           Size
----                 ------           -----
0x7f6eba49f06b            2           1136
0x7f6eba4b71f2          545           8065
0x7f6eba4d239c            1             20
0x7f6eba4d3556            1             33
0x7f6eba7c5c78            2            640
0x7f6eba9fc057            1           1968
0x7f6eba9fcc1d            1          66160
0x7f6ebb515ac6            1           4816
0x7f6ebc0492d6          585          32760
0x7f6ebc049ec5          543          30408
0x7f6ebc04a6e0            5            280
0x7f6ebc04bae2           36           3744
0x7f6ebc04bb05           36          14704
0x7f6ebc04bd4e           51           1224
0x7f6ebc04be5e            9            288
0x7f6ebc054e3e           22            528
0x7f6ebc0555be           12            480
0x7f6ebc28838d            1            120
0x7f6ebc289b1d           15           1320
0x7f6ebc289cfe            1           1176
0x7f6ebc28aaff            5            440
0x7f6ebc28b654            1             88
0x7f6ebc28b667            1           8192
0x7f6ebca7755a            5            120
0x7f6ebca78679            2             16
0x7f6ebcc8d462           15            660
0x7f6ebcc8d4a2            1             88
0x7f6ebcc941d8            1           6448
0x7f6ebcc946fa            1          41000
0x7f6ebcc94717            1          41000
0x7f6ebcc94baf            1          11263
0x7f6ebcc98ec3            3          14696
0x7f6ebcc9a49f            1             16
0x4137b6             1             64
0x41bdfb             1          41000
0x435200             1             88
0x4358ac             2            272
0x4369f1             3            120
0x436a64             9            288
0x437f3a             3            168
0x45ba3a             3             72
0x45c277             4            288

total                                  336545                        336698
```

The output of this command includes the following columns:

Column	Description
Type	The **show memory** command only shows information for predefined processes, so this column always displays the parameter **default**.

Column	Description
`Num Alloc`	Current number of memory allocations.
`Size Allocs`	Total size of all memory allocations, in bytes.
`Peak Allocs`	Maximum number of allocations used throughout in the life of the process.
`Peak Size`	Maximum size of allocations used throughout in the life of the process, in bytes.
`PC`	Program counter: the address of a memory allocation. (For internal use only)
`Allocs`	Number of memory allocations at that program counter. (For internal use only)
`Size`	Size of all memory allocations at that program counter. (For internal use only)

Command History

Release	Modification
ArubaOS 8.2.0.0	The **lagm** and **vrrp** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show mgmt-role

```
show mgmt-role
```

Description

This command allows the user to view a list of management role configurations.

Syntax

No parameters.

Example

Issue this command to display a list of management user roles.

```
Management User Roles
---------------------
ROLE                 DESCRIPTION
----                 -----------
root                 Super user role
read-only            Read only commands
network-operations   network-operations
guest-provisioning   guest-provisioning
location-api-mgmt    location-api-mgmt
no-access            Default role, no commands are accessible for this role
location-api-mgmt    location-api-mgmt
```

The output includes the following parameters:

Parameter	Description
`Role`	Name of the management user role
`Description`	Description of the management user role

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show mgmt-server

```
show mgmt-server
   message-counters process {arm|auth|dhcp|fpapps|fw_visibility|hwmon|mdns|resolver|spectrum
   stm|ucm|wms}
   profile <profile-name>
```

Description

Displays the message counter information of management server.

Syntax

Parameter	Description
`message-counters`	Message counter in the recent past.
`process {arm|auth|dhcp|fw_visibility|mdns |resolver|spectrum|stm|ucm|wms}`	Controller processes: ■ **arm**: Advanced Radio Management (ARM) ■ **auth**: Authentication ■ **dhcp**: DHCP ■ **fpapps**: Layer 2,3 control ■ **fw_visibility**: Firewall Visibility ■ **hwmon**: Hardware monitor ■ **mdns**: AirGroup ■ **resolver**: Resolver ■ **spectrum**: Spectrum Analysis ■ **stm**: Station Management ■ **ucm**: Unified Communication Manager ■ **wms**: WLAN Management System
`profile <profile-name>`	Displays the list of configuration profiles and the details of the specified configuration profiles for the management server.

Example

The output of this command shows the message counter information of the WLAN Management System process in the controller.

```
(host)[node] (config) #show mgmt-server message-counters process wms

Message Counter History
-----------------------
Message Number  Time                     Packets  Monitored AP Info  Monitored AP Stats
Monitored STA Info  Monitored STA Stats
--------------  ----                     -------  -----------------  ------------------  -----
-------------  -------------------
82              Tue Apr 2 14:56:43 2013  1        0                  0                   3
               3
81              Tue Apr 2 14:56:13 2013  1        14                 218                 2
               67
80              Tue Apr 2 14:55:43 2013  1        0                  0                   0
               2
79              Tue Apr 2 14:55:13 2013  1        0                  0                   0
               2
```

The output of the following command displays the details of the default-amp management configuration profile:

```
            (host)[node] #show mgmt-server profile default-amp
Mgmt Config profile "default-amp" (Predefined (editable))
---------------------------------------------------------
Parameter         Value
---------         -----
Stats             Enabled
Tag               Enabled
Sessions          Enabled
Monitored Info    Disabled
Monitored Stats   Disabled
Misc              Enabled
Location          Enabled
Voice Info        Disabled
```

Command History

Release	Modification
ArubaOS8.2.0.0	The **fpapps** and **hwmon** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show mgmt-servers

```
show mgmt-servers
```

Description

Displays list of management servers that receive Advanced Monitoring (AMON) messages from the controller.

Syntax

Parameter	Description
`mgmt-servers`	Management Servers. This could be AirWave Management Server or any other server that receive messages from the controller using AMON protocol.

Example

The output of this command shows list of management servers.

```
(host)(mynode) #show mgmt-servers
List of Management Servers
--------------------------
Primary Server  Profile      Transport-method
--------------  -------      ----------------
2001::2         default-amp  secure-udp
40.40.40.1      default-amp  secure-udp
10.1.1.11       default-amp  udp
20.16.11.1      default-ale  udp
Num Rows:4
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	Listed primary servers with IPv6 address.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show mgmt-users

```
show mgmt-users [ <username> |
   local-authentication-mode <username> |
   ssh-pubkey <username> |
   webui-cacert <username> ]
```

Description

Displays a list of management users on the controller and details of each management user.

Syntax

Parameter	Description
`username`	To view details of a specific management user.
`local-authentication-mode`	Status of local-authentication mode.
`ssh-pubkey`	Number of management users using the ssh-pubkey.
`webui-cacert`	Number of management users using web CA certificates.

Example

The output of this command shows the client certificate name, username, user role, and revocation checkpoint for management users using the ssh-pubkey in the controller.

```
(host)[node]#show mgmt-user ssh-pubkey

SSH Public Key Management User Table
------------------------------------
CLIENT-CERT  USER    ROLE   STATUS   REVOCATION CHECKPOINT
-----------  ----    ----   ------   --------------------
client1-rg   test1   root   ACTIVE   ca-rg
client2-rg   test2   root   ACTIVE   none
client3-rg   test3   root   ACTIVE   ca-rg
client1-rg   test4   root   ACTIVE   ca-rg
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show mobility-managers

```
show mobility-managers
```

Description

Use the command to display information for MMS server.

Example

Execute the following command to display the MMS information:

```
(host) [mm] (config) #show mobility-managers
MMS SERVERS
-----------
HOST      USER NAME   PORT   INTERVAL   RETRY   RTLS-PORT   ACTIVE
----      ---------   ----   --------   -----   ---------   ------
1.1.1.1   testUN      162    60         3       8000
MMS config sync state:    Ready
Last Cfg sync result:     None
Automatic config update:  Disabled
MMS config ID:            0
Controller config ID:     0
Config update success:    0
Config update failures:   0
```

Related Commands

Command	Description
mobility-manager	This command configures the mobility manager server for the managed device to communicate with it.

Command History

Release	Modification
ArubaOS 8.0.0.0	This command was introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Master.

show mon-serv

```
show mon-serv
   ap-microboot-stats
   device-count
   function-stats
   max-q-stats
   message-stats
   mon-device-operation-stats
   queue-stats
   radio-microboot-stats
   sta-microboot-stats
   vap-microboot-stats
```

Description

This command shows the detailed statistics of monitoring server.

Syntax

Parameter	Description
`ap-microboot-stats`	Displays the AP micro-bootstrapping statistics.
`device-count`	Displays the count of devices that are added or deleted.
`function-stats`	Displays the summary of monitoring server activities.
`max-q-stats`	Displays the details of maximum queue statistics.
`message-stats`	Displays the AMON and monitoring server message statistics.
`mon-device-operation-stats`	Displays the device operation statistics.
`queue-stats`	Displays the current queue statistics.
`radio-microboot-stats`	Displays the micro-bootstrapping statistics of AP radios.
`sta-microboot-stats`	Displays the STA micro-bootstrapping statistics.
`vap-microboot-stats`	Displays the VAP micro-bootstrapping statustics.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows the device operation statistics on the monitoring server.

```
(host) [mynode] #show mon-serv mon-device-operation-stats

Device Type: 0 [MON_DEVICE_TYPE_NETWORK]

Add Count          : 7
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 0

Device Type: 1 [MON_DEVICE_TYPE_NETWORK_FWV]

Add Count          : 0
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 0

Device Type: 2 [MON_DEVICE_TYPE_AP]

Add Count          : 316
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 909

Device Type: 3 [MON_DEVICE_TYPE_RADIO]

Add Count          : 1615
Delete Count       : 1615
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 909

Device Type: 4 [MON_DEVICE_TYPE_STA]

Add Count          : 138
Delete Count       : 157
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 909

Device Type: 5 [MON_DEVICE_TYPE_USER]

Add Count          : 205
Delete Count       : 36
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 909

Device Type: 6 [MON_DEVICE_TYPE_SSID]

Add Count          : 0
Delete Count       : 0
Add Bulk Count     : 0
Delete Bulk Count  : 0
Delete All Count   : 0
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show mon-serv-fwv-lc-table

```
show mon-serv-fwv-lc-table
   airgroup
   bootstrap-stats <ip-addr>
```

Description

This command shows the status of local controllers and AirGroup counters on the monitoring server.

Syntax

Parameter	Description
`airgroup`	Displays the AirGroup counters.
`bootstrap-stats <ip-addr>`	Displays the bootstrapping statistics.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows the counter statistics on the controller.

```
(host) [mynode] #show mon-serv-fwv-lc-table airgroup

MON_SERV Airgroup Table
-----------------------
LC IP        Servers  Users  Server Usage  User Usage  Server Ip Entries   User Ip Entries  Ag
sessions  Mode
-----        -------  -----  ------------  ----------  ------------------  ---------------  --
---------  ----
10.15.20.40  0        1      1364          1           1365                2                0
          Centralised
10.15.20.41  5        0      4             0           4                   0                0
          Centralised
10.15.20.24  5        3      4             3           5                   4                0
          Centralised
Total        10       4      1372          4           1374
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show mon-serv-lc-table

```
show mon-serv-lc-table
   airgroup
   bootstrap-stats <ip-addr>
   dev-del-stats <ip-addr>
   microboot-stats <ip-addr>
```

Description

This command shows the status and counters of monitoring server.

Syntax

Parameter	Description
`airgroup`	Shows AirGroup counters.
`bootstrap-stats <ip-addr>`	Shows bootstrap statistics for an lc-cluster.
`dev-del-stats <ip-addr>`	Shows (STM) device delete reason statistics for an lc-cluster.
`microboot-stats <ip-addr>`	Shows micro-bootstrapping statistics and threshold counts for an lc-cluster.

Usage Guidelines

This command shows the status and counters of monitoring server. For the remaining parameters, see the command syntax.

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following example shows the configuration status of all branch config groups on the controller.

```
(host) [mynode] #show mon-serv-lc-table airgroup

MON_SERV Airgroup Table
-----------------------
LC IP  Servers  Users  Server Usage  User Usage  Server Ip Entries
-----  -------  -----  ------------  ----------  ------------------

User Ip Entries  Ag sessions
---------------  -----------
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **dev-del-stats** and **microboot-stats** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

show neighbor-devices

```
show neighbor-devices
```

Description

Show neighbor device information

Syntax

No Parameters

Example

The command in the first example below shows that the managed device recognizes two neihbor devices.

```
[host] (node) # show neighbor devices
Interface objtype is 7
Capability codes: (R)Router, (B)Bridge, (A)Access Point, (P)Phone, (S)Station
(r)Repeater, (O)Other
Neighbor Devices Information
-------------------------
Local Intf      Chassis ID          Capability   Remote Intf   Expiry-Time (Secs)  System
---------       -----------         -----------  -----------   ------------------ -----------
0/0/1           00:0b:86:6a:25:40   B:R          0/0/17        105                 Aruba 7220
0/0/2           00:0b:86:6a:25:40   B:R          0/0/18        105                 Aruba 7220
```

Parameter	Description
`Local Intf`	Slot and port number of the local interface that detected the neighbor devices.
`Chassis ID`	MAC address of the neighbor device.
`Capability`	Shows the capabilities of the neighbor deviceto operate as a router, bridge, access point, phone or other network device.
`Remote Intf`	Slot and port number of the remote interface on the neighbor device
`Expiry-time`	Expiry time.
`System Name`	Name of the neighbor device, as supplied by the neighbor.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on managed devices. This command is not supported on Mobility Master.

show netdestination

```
show netdestination {ipv4 | ipv6 | <netdestination name>} [verbose]
```

Description

Displays IPv4 and IPv6 network destination information.

Syntax

Parameter	Description
`ipv4`	Displays IPv4 network destinations.
`ipv6`	Displays IPv6 network destinations.
`<netdestination name>`	Displays the name or IP addresses.
`verbose`	Prints the netdestination table entries.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

Issue this command to display all netdestination configured on this managed device. The output below displays information for all configured IPv4 and IPv6 netdestinations. To display additional detailed information for an individual netdestinations, include the name of the netdestination at the end of the command.

```
(host) [mynode] #show netdestination
Name: sep23-ipv4
Destination ID: 34
Position  Type  IP addr   Mask-Len/Range
--------  ----  -------   --------------
1         host  1.1.1.1   32
2         name  0.0.0.8   google.com
```

The output includes the following parameters:

Parameter	Description
`Name`	Network destination name.
`Destination ID`	Network destination ID.
`Position`	Network destination position.
`Type`	Network destination type.
`IP addr`	IP address of the network destination.

Parameter	Description
`Mask-Len/Range`	Network destination subnet mask and range. If the netdestination object has a defined domain or host name, that value will appear in the mask-Len or Range column.

Related commands

Command	Description
netdestination	This command configures an alias for an IPv4 network host, subnetwork, or range of addresses.
netdestination6	This command configures an alias for an IPv6 network host, subnetwork, or range of addresses.

Command History

Version	Modification
ArubaOS 8.2.1.0	The **Destination ID** parameter was added to the output.
ArubaOS 8.2.0.0	The **ipv4** and **ipv6** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	You must have a PEFNG license to configure or view a netdestination.	Enable or Config mode on Mobility Master

show netexthdr

```
show netexthdr <alias-name>
```

Description

This command displays the IPv6 extension header (EH) types that are denied.

Syntax

Parameter	Description
`<alias-name>`	Specify the EH alias name.

Usage Guidelines

Example

The following command displays the denied extended header types in the default EH:

```
(host)[mynode] #show netexthdr default

Extended Header type(s) Denied
------------------------------
51,
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show netservice

```
show netservice [<string>]
```

Description

Show network services

Syntax

Parameter	Description
`<string>`	Name of a network service.

Usage guidelines

Issue this command without the optional **<string>** parameter to view a complete table of network services on the controller. Include the **<string>** parameter to display settings for a single network service only.

Example

The following example shows the protocol type, ports and application-level gateway (ALG) for the DHCP service.

```
(host)[mynode] #show netservice svc-dhcp
Services
--------
Name      Protocol  Ports  ALG
----      --------  -----  ---
svc-dhcp  udp       67                          68
```

Related Commands

Command	Description
netservice	This command configures an alias for network protocols.

To configure an alias for network protocols, use the command netservice.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show netstat

```
show netstat
ip dst|src <ip-addr>
port dst|exclude|src <port>
raw
stats
tcp
udp
unix
```

Description

Show network statistics for current active network connections, filtered by protocol type.

Syntax

Parameter	Description
`ip dst|src <ip-addr>`	Displays network statistics filtered based on the source or destination IP address
`port dst|exclude|src <port>`	Displays network statistics filtered based on the source or destination port number. Use the **exclude** parameter to exclude a part from the output of this command.
`raw`	Show netstat raw socket statistics
`stats`	Show a network statistics summary
`tcp`	Displays network statistics for TCP sockets.
`udp`	Displays network statistics for UDP sockets.
`unix`	Displays network statistics for UNIX sockets.

Usage guidelines

Issue the **show netstat stats** command to display aggregate statistics, or protocol type, port or IP address to filter the statistics displayed in the output of this command.

Example

The following example shows incoming and outgoing packet statistics for the controller.

```
(host)[node](config) #show netstat stats
Total: 1128 (kernel 1200)
TCP:   147 (estab 82, closed 22, orphaned 0, synrecv 0, timewait 13/0), ports 0
Transport Total     IP        IPv6
*         1200      -         -
RAW       1         1         0
UDP       240       43        197
TCP       125       107       18
INET      366       151       215
FRAG      0         0         0
```

Related Commands

Parameter	Description
netservice	Configures an alias for network protocols,

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode

show ntp authentication-keys

```
show ntp authentication-keys
```

Description

Show information for the NTP authentication key.

Syntax

No parameters.

Example

The following example shows values for the NTP authentication keys—Key ID, Key Type, and the Secret.

```
(host) [mynode] # show ntp authentication-keys
Key Id Key Type Secret
------ -------- ------
41       sha1     ********
```

The output of this command includes the following parameters:

Parameter	Description
`Key ID`	The key identifier used when you configured the NTP authentication key.
`Key Type`	The key type that you used when you configured the NTP authentication key—md5 or sha1.
`Secret`	The key value for the MD5/SHA1 hash used when you configured the NTP authentication key.

Related Commands

Command	Description
ntp	Helps configure NTP authentication keys.

Command History

Release	Modification
ArubaOS 8.2.1.0	The output was modified to show the SHA1 key type and secret (in encoded format), when SHA1 authentication is configured.
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show ntp peer

```
show ntp peer <IPv4/IPv6 Address>
```

Description

Show NTP peer information.

Syntax

Parameter	Description
`<IPv4/IPv6 Address>`	IPv4/IPv6 Address of the peer.

Example

The output of this commands shows IPv4 and IPv6 address of the peer.

```
(host)[mynode]#show ntp peer 2008::2

remote 2008::2, local 2008::1
hmode client, pmode sym_active, stratum 16, precision -20
leap 11, refid [73.78.73.84], rootdistance 0.00000, rootdispersion 0.00262
ppoll 6, hpoll 6, keyid 0, version 4, association 53202
reach 000, unreach 1, flash 0x1620, boffset 0.00000, ttl/mode 0
timer 0s, flags config, bclient
reference time:      00000000.00000000  Wed, Feb  6 2036 22:28:16.000
originate timestamp: 00000000.00000000  Wed, Feb  6 2036 22:28:16.000
receive timestamp:   d6186e9b.5723196a  Sun, Oct 27 2013 21:03:23.340
transmit timestamp:  d6186e9b.5723196a  Sun, Oct 27 2013 21:03:23.340
filter delay:  0.00000  0.00000  0.00000  0.00000
0.00000  0.00000  0.00000  0.00000
filter offset: 0.000000 0.000000 0.000000 0.000000
0.000000 0.000000 0.000000 0.000000
filter order:  0        1        2        3
4        5        6        7
offset 0.000000, delay 0.00000, error bound 3.99217, filter error 0.00000
remote host:          2008::2
local interface:      2008::1
time last received:   59s
time until next send: 5s
reachability change:  61s
packets sent:         1
packets received:     1
bad authentication:   0
bogus origin:         0
duplicate:            0
bad dispersion:       1
bad reference time:   0
candidate order:      0
flags:     config, bclient

(host)[mynode]#show ntp peer 10.20.22.17

remote ::, local ::
hmode client, pmode unspec, stratum 3, precision -23
leap 00, refid [125.62.193.121], rootdistance 0.32069, rootdispersion 0.15305
ppoll 6, hpoll 6, keyid 0, version 4, association 26134
reach 001, unreach 2, flash 0x0400, boffset 0.00113, ttl/mode 0
```

```
timer 0s, flags config, bclient
reference time:      d6186d7e.c99ed7ba  Sun, Oct 27 2013 20:58:38.787
originate timestamp: 00000000.00000000  Wed, Feb  6 2036 22:28:16.000
receive timestamp:   d6186e24.f02d3f57  Sun, Oct 27 2013 21:01:24.938
transmit timestamp:  d6186e24.f02d3f57  Sun, Oct 27 2013 21:01:24.938
filter delay:  0.00113  0.00000  0.00000  0.00000
0.00000  0.00000  0.00000  0.00000
filter offset: 0.398620 0.000000 0.000000 0.000000
0.000000 0.000000 0.000000 0.000000
filter order:  0        1        2        3
4        5        6        7
offset 0.398620, delay 0.00113, error bound 2.81735, filter error 0.00276
remote host:          10.20.22.17
local interface:      10.16.32.90
time last received:   1s
time until next send: 1s
reachability change:  1s
packets sent:         2
packets received:     1
bad authentication:   0
bogus origin:         0
duplicate:            0
bad dispersion:       0
bad reference time:   0
candidate order:      0
flags:     config, bclient, iburst
```

Usage guidelines

The **show ntp peer** command is used for NTP server troubleshooting, and should only be used under the supervision of Aruba technical support. Issue the show ntp servers command to view basic settings for currently configured NTP servers.

Related Commands

Command	Description
ntp	This command configures a Network Time Protocol (NTP) server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show ntp servers

```
show ntp servers [brief]
```

Description

Show information for Network Time Protocol (NTP) servers.

Syntax

Parameter	Description
brief	Display the IP address of the defined NTP servers, iburst and key settings.

Examples

The following example shows values for the primary and backup NTP servers. The primary server is marked with an asterisk (*****) and the backup server is marked with an equals sign (**=**). Note that a backup server will not display delay, offset or dispersion data, as it is not currently in use.

```
(host) (config) #show ntp server
NTP Server Table Entries
------------------------
Flags:     * Selected for synchronization
+ Included in the final selection set
# Selected for synchronization but distance exceeds maximum
- Discarded by the clustering algorithm
= mode is client
remote                          local        st   poll   reach    delay     offset      disp
==========================================================================================
===
*2012::d63d:7eff:fe46:7309      2012::40       3 1024     377    0.00169    -0.001367
0.13815
```

The output of this command includes the following parameters:

Parameter	Description
flags	The flags indicate the status of the server.
remote	IP address of the remote NTP server defined using the CLI command ntp.
local	IP address of the local clock.
st	NTP uses hierarchical levels of clock sources, or strata, and assigns each layer a number starting with zero at the root. The **st** column in the output of this command represents the number of servers between the configured NTP server and the root reference clock.
poll	Interval, in seconds, between the local NTP server's attempt to poll the remote NTP server.
reach	An index that measures whether or not the remote NTP server could be reached at eight most recent polling intervals. If the NTP server has just been configured and hasn't yet been polled successfully, the value will be zero (0). A value of 377 indicates that the last eight poll queries were successful.

Parameter	Description
delay	Delay, in seconds, between the time that the local clock polls the NTP server and the NTP server returns a reply.
offset	The difference in time, in seconds, between the local clock and the NTP server.
disp	Dispersion represents the maximum error of the local clock relative to the reference clock, and is a measurement of the time server and network quality. Lower dispersion values are preferred over higher dispersion values.

The following example shows the **ntp servers** configuration. The NTP server IP address, key ID and iburst status are shown when the **ntp servers brief** command is used.

The following output is for IPv4:

```
(host) (config) #show ntp servers brief
server 1.1.1.1  key 1234
server 10.1.1.245 iburst key 12345
```

The following output is for IPv6:

```
(host) (config) #show ntp servers brief
server 2012::d63d:7eff:fe46:7309
```

Related Commands

To configure an NTP server, use the command ntp.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show ntp status

```
show ntp status
```

Description

Show information for a NTP server.

Syntax

No parameters.

Example

The following example shows values for the primary NTP server.

```
(host) #show ntp status

Authentication:          enabled
time since restart:      2347
time since reset:        7594
packets received:        4
packets processed:       0
current version:         0
previous version:        0
declined:                0
access denied:           0
bad length or format:    0
bad authentication:      0
rate exceeded:           0
system peer:             10.1.1.250
system peer mode:        client
leap indicator:          00
stratum:                 3
precision:               -18
root distance:           0.03236 s
root dispersion:         0.06728 s
reference ID:            [10.1.1.250]
reference time:          cd45b701.bcbc05d5  Tue, Feb 17 2009 14:21:53.737
system flags:            auth monitor ntp kernel stats
jitter:                  0.005020 s
stability:               0.866 ppm
broadcastdelay:          0.003998 s
authdelay:               0.000000 s
```

The output of this command includes the following parameters:

Parameter	Description
`authentication`	Indicates if authentication is enabled for the NTP server.
`time since restart`	Time in hours since the system was last rebooted.
time since reset	The number of seconds since the last time the local NTP server was restarted.
`packets received`	Total number of packets received.

Parameter	Description
packets processed	Number of packets received in response to previous packets sent.
current version	Number of packets matching the current NTP version.
previous version	Number of packets matching the previous NTP version.
declined	Number of packets declined.
access denied	Number of packets for which access has been denied.
bad length or format	Number of packets with invalid length, format or port number.
packets received	Total number of packets received.
bad authentication	Number of NTP packets that failed to be authenticated.
rate exceeded	Number of packets discarded due to rate limitation.
system peer	The IP address of the peer NTP server.
system peer mode	The peer mode of this remote association: ■ Symmetric Active ■ Symmetric Passive ■ Client ■ Server ■ Broadcast
leap indicator	This parameter indicates whether or not a leap-second should be inserted or removed at the end of the last day of the current month. ■ 00 no warning ■ 01 +1 second (following minute has 61 seconds) ■ 10 -1 second (following minute has 59 seconds)
stratum	The stratum level of the peer
precision	The advertised precision of the switch. This value can range from -4 and -20, inclusive.
root distance	Total round trip delay to the stratum 1 reference clock.
root dispersion	Total dispersion to the stratum 1 reference clock. This value is a cumulative measure of all errors associated with the network hops and servers between the NTP server and its stratum 1 server.
reference ID	IPv4/IPv6 address of the remote NTP server. Note: When NTP server is reachable through IPv4 address, use the address as is. If done through IPv6 address, the Reference ID is calculated instead of directly taking the IPV6 address on the NTP Server. The controller performs a MD5 checksum and the last 4 bytes are considered as the reference ID.
reference time	Time when the local system clock was last set or corrected, in NTP timestamp format.
system flags	This parameter displays any flags configured for this NTP entity.
jitter	The average magnitude of jitter between several time queries.

Parameter	Description
stability	The average magnitude of offset between several time queries
broadcastdelay	The broadcast delay of this NTP server association, in seconds.
authdelay	The authentication delay of this NTP server association, in seconds.

Related Commands

To configure an NTP server, use the command ntp.

Command History

Release	Modification
ArubaOS 3.0	Command introduced
ArubaOS 6.4	The following parameters were introduced: ■ time since restart ■ packets received ■ packets processed ■ current version ■ previous version ■ declined ■ access denied ■ bad length or format ■ bad authentication ■ rate exceeded

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show openflow

```
show openflow
   capabilities
   controller
   debug
   flow-table
   flows
   ports
   statistics
```

Description

The command displays the information such as flows, flow tables, system capabilities, and statistics related to OpenFlow on the managed device where OpenFlow is enabled.

Syntax

Parameter	Description
`capabilities`	Displays the OpenFlow system capability information.
`controller`	Displays the OpenFlow Controller information.
`debug {ap-client|event|flows| ports}`	Displays the debug information for the OpenFlow AP clients, events, flows and ports.
`flow-table`	Displays the flow table information.
`flows`	Displays the flow information of the OpenFlow agent.
`ports`	Displays all the ports configured for OpenFlow.
`statistics`	Displays the OpenFlow statistics information.

Example

The following command displays the OpenFlow capabilities on the managed device:

```
(host-md) #show openflow capabilities

Match Fields:
In Port
Ethernet Destination Address
Ethernet Source Address
Ethernet Frame Type
802.1Q Vlan ID
IP Protocol
IPv4 Source Address
IPv4 Destination Address
TCP Source Port
TCP Destination Port
UDP Source Port
UDP Destination Port
IPv6 Source Address
IPv6 Destination Address
Actions:
Output to Port
Set 802.1Q Vlan ID
```

```
Set 802.1Q Vlan Priority
Strip 802.1Q Vlan
Set Ethernet Source Address
Set Ethernet Destination Address
Set IPv4 Source Address
Set IPv4 Destination Address
Set DSCP Bits
Set TCP/UDP Source Port
Set TCP/UDP Destination Port
```

The following command displays the OpenFlow Controller information from the managed device:

```
(host-md) #show openflow controller

Controller IP Address: 10.4.131.169  Port: 6633
Connection: UP
State: ACTIVE
Local IP: 10.4.135.67
Local Port: 39703
Last Connected: Tue Jun 21 15:33:45 2016 (83618 seconds ago)
Datapath ID: 00:00:00:0b:86:bb:cd:27
Auxiliary Channel Status:On, Last Connected: Tue Jun 21 15:35:15 2016
Total Flow Count: 25
Total Port Count: 12
Total Packet In Count: 3650
Total Packet In Count (no match): 2
Total Packet Out Count: 7859
```

The following command displays the ports configured for OpenFlow:

```
(host-md) #show openflow ports

Total number of ports: 12

Openflow Port Table
-------------------
Name              Port No  Mac Address        Status
----              -------  -----------        ------
spiCA890700in     3        00:00:00:00:00:00  UP
bss6cf37fe97b70   9        6c:f3:7f:e9:7b:70  UP
spi03EE4D00out    1        00:00:00:00:00:00  UP
bss6cf37fe97b60   10       6c:f3:7f:e9:7b:60  UP
bssaca31effb820   12       ac:a3:1e:ff:b8:20  UP
GE0/0/2           4        00:0b:86:bb:cd:2a  UP
bssaca31eebc6c0   8        ac:a3:1e:eb:c6:c0  UP
bssaca31effb830   11       ac:a3:1e:ff:b8:30  UP
bssaca31eebc6d0   7        ac:a3:1e:eb:c6:d0  UP
bssaca31effcdf0   5        ac:a3:1e:ff:cd:f0  UP
bssaca31effcde0   6        ac:a3:1e:ff:cd:e0  UP
GE0/0/0           2        00:0b:86:bb:cd:28  UP
```

The following command displays the OpenFlow statistics:

```
(host-md) #show openflow statistics
Openflow Message Statistics
---------------------------
Statistics-Name          Received  Sent
---------------          --------  ----
Hello                    1         1
Echo Request             0         2724
Echo Reply               2724      0
Features Request         2         0
Features Reply           0         2
Set Config               1         0
```

```
Packet In                0         3774
Port Status              0         56
Packet Out               8111      0
Flow Mod                 26        0
Desc Request             1         0
Desc Reply               0         1
Flow Stats Reqest        2877      0
Flow Stats Reply         0         2877
Port Stats Request       1439      0
Port Stats Reply         0         1439
Port Desc Stats Request  1         0
Port Desc Stats Reply    0         1
Sos Action Add           25        25
Sos OF Enable            0         1
Sos Session Add          0         1
Sos Packet-In            3537      0
Mark Sweep Start         0         1
Mark Sweep Finished      1         0
Packet Out Local         0         11
Aux Setup                0         2
Aux Setup Retry          0         4
Aux Destroy              0         2
Aux Ready                2         0
Aux Health Chceck        8601      8601
Aux Port Map             0         15
Aux Probe                0         14
Tunnel Ipsec Update      50        0
Auth Flow Add            25        25
Auth Init                0         1
Auth Up                  1         0
Auth Wired Trusted       9         0

Miscelleneous Counters
----------------------
Counter-Name          Value
------------          -----
Ip Flow Stats Update  2459
Gsm Port Add Enqueue  296
Gsm User Add Enqueue  228
Gsm Port Add Dequeue  296
Gsm User Add Dequeue  228
```

The following command displays the OpenFlow flows:

```
(host-md) #show openflow flows

flow cookie 281474976710733
priority 32768
match:
Ethernet Type:IPv4
source IPv4 address: 192.168.61.3
destination IPv4 address: 192.168.60.60
ip proto: udp
dest tcp/udp port: 5003
actions:
output interfaces:65530
output interfaces:65533
IP ToS:2e,
set vlan pcp:6,
matched:0packets, 0bytes
Hard Timeout:60

Total number of flows: 27
```

```
flow cookie 281474976710734
priority 32768
match:
Ethernet Type:IPv4
source IPv4 address: 192.168.60.60
destination IPv4 address: 192.168.61.3
ip proto: udp
dest tcp/udp port: 5003
actions:
output interfaces:65530
output interfaces:65533
IP ToS:2e,
set vlan pcp:6,
matched:0packets, 0bytes
Hard Timeout:60
```

The following command displays the output of flow-table on the managed device with a Sample bi-directional flow installed by the OpenFlow Controller:

```
(host-md) #show openflow flow-table
Openflow Flow Table
-------------------
In Port  Src Mac  Dst Mac  Ether   Src IP           Dst IP           Proto  Src Port   Dst
Port   Packets  Bytes    Actions
-------  -------  -------  -----   ------           ------           -----  --------   -------
-   -------  -----    -------
*        *        *        0x800   *                *                17     *          5000
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                6      *          5060
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     *          5002
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                6      *          2000
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     *          32512
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                6      *          1720
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     *          5060
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                6      *          5061
   0        0        (Output:normal)
*        *        *        0x800   1.1.1.1          2.2.2.2          97     *          *
   1324     76792    (Output:controller)
*        *        *        0x800   *                *                17     *          5070-
6070  0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     *          1718-
1719  0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     1718-1719  *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     5070-6070  *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   222.173.190.239  186.173.202.254  17     60000      60000
   0        0        (Output:controller)
*        *        *        0x806   *                *                *      *          *
   2226     4558848  (Output:normal)(Output:controller)
*        *        *        0x800   192.168.61.3     192.168.60.60    17     *          5003
   0        0        (Output:normal)(Output:controller),(Set IP ToS:46),(Set Vlan pcp:6)
*        *        *        0x800   192.168.60.60    192.168.61.3     17     *          5003
   0        0        (Output:normal)(Output:controller),(Set IP ToS:46),(Set Vlan pcp:6)
*        *        *        0x800   *                *                6      5061       *
   0        0        (Output:normal)
```

```
*        *        *        0x800   *                *                6      1720       *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                6      2000       *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x86dd  ::/0             ::/0             58     136        *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     5060       *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     5002       *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     5000       *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                6      5060       *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x86dd  ::/0             ::/0             58     135        *
   0        0        (Output:normal)(Output:controller)
*        *        *        0x800   *                *                17     32512      *
   0        0        (Output:normal)(Output:controller)
Total number of flows: 27
```

The following command displays the debug event listing the flow addition on the managed device:

(host-md) #show openflow debug event

```
Printing events sorted by time (Max 1000), Total:115
--------------------------------------------
114. Wed Jun 22 15:38:09 2016 : SOS ACTIONS RESP : trans_id:27, sos action_index: 27,
ethtype:2048 sipv4:192.168.60.60 dipv4:192.168.61.3 proto:17 sport:0 dport:5003
113. Wed Jun 22 15:38:09 2016 : FLOW ADD : ethtype:2048 inport:0 srcmac:00:00:00:00:00:00
dstmac:00:00:00:00:00:00 sipv6::: sipv6::: sipv4:192.168.60.60 dipv4:192.168.61.3 proto:17
sport:0 dport:5003,idletmo:0, metadata:0, act=[(Output:normal)(Output:controller),(Set IP
ToS:46),(Set Vlan pcp:6)]
112. Wed Jun 22 15:38:09 2016 : SOS ACTIONS RESP : trans_id:26, sos action_index: 26,
ethtype:2048 sipv4:192.168.61.3 dipv4:192.168.60.60 proto:17 sport:0 dport:5003
111. Wed Jun 22 15:38:09 2016 : FLOW ADD : ethtype:2048 inport:0 srcmac:00:00:00:00:00:00
dstmac:00:00:00:00:00:00 sipv6::: sipv6::: sipv4:192.168.61.3 dipv4:192.168.60.60 proto:17
sport:0 dport:5003,idletmo:0, metadata:0, act=[(Output:normal)(Output:controller),(Set IP
ToS:46),(Set Vlan pcp:6)]
110. Wed Jun 22 15:24:33 2016 : PORT DEL : name:spi5371BD00in, dp_port:65553, ofp_port:14
109. Wed Jun 22 15:24:33 2016 : PORT DEL : name:spiFD0D7900out, dp_port:65554, ofp_port:13
```

Related Commands

Command	Description
openflow-profile	This command configures OpenFlow profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config or Enable mode on managed device.

show openflow-controller

```
show openflow-controller
   flow-table [app-name|dpid|sorted-by-dpid]
   flows [app-name <name>|dpid <dp-id>]
   hosts [dpid <dp-id>|ip-address <ip>|mac-address <mac>]
   links [dpid <dp-id>]
   ports [dpid <dp-id>]
   resource
   statistics [process-name <name>]
   summary [dpid <dp-id>]
   switches [details]
```

Description

The command displays the OpenFlow Controller configuration information on . In addition, you can view information such as flows, flow tables, hosts, and statistics related to OpenFlow Controller on Mobility Master.

Syntax

Parameter	Description
`flow-table [app-name|dpid|sorted-by-dpid]`	Displays the flow table information on Mobility Master. You can also filter the view based on the application name that installed the flow, or by datapath ID of the OpenFlow instance.
`flows [app-name <name>|dpid <dp-id>]`	Displays the flow information of the OpenFlow Controller on Mobility Master.
`hosts [dpid <dp-id>|ip-address <ip>|mac-address <mac>]`	Displays the OpenFlow host configuration information on Mobility Master. You can also filter the view by datapath ID, IP address or MAC address of the host.
`links [dpid <dp-id>]`	Displays the OpenFlow links on Mobility Master. You can also filter the output based on the datapath ID of the OpenFlow instance.
`ports [dpid <dp-id>]`	Displays the OpenFlow ports configured on Mobility Master. You can also filter the output based datapath ID of the OpenFlow instance.
`resource`	Displays the OpenFlow resource usage information on Mobility Master.

Parameter	Description
`statistics [process-name <name>]`	Displays the OpenFlow statistics information. You can also filter the output based on any of the following process names: ■ flow_manager ■ topology ■ topology_discovery ■ routing_switch ■ switch_manager ■ packetin_dispatcher ■ event_dispatcher
`summary [dpid <dp-id>]`	Displays the OpenFlow summary information on Mobility Master. You can also filter the output based datapath ID of the OpenFlow instance.
`switches [details]`	Displays the details of the OpenFlow switches on Mobility Master.

Example

The following command displays the OpenFlow Controller configuration details on Mobility Master:

```
(host) [mynode] #show openflow-controller
openflow-controller
--------------------
Parameter                   Value     Set
---------                   -----     ---
ofc state                   Enabled
ofc host-ageout-time        300
ofc mode                    passive
ofc certificate-file        none
ofc key-file                none
ofc ca-certificate-file     none
ofc tls                     Disabled
ofc port                    6633
ofc topology-discovery      Disabled
ofc auxiliary-channel-port  6633
```

The following command displays the OpenFlow Controller switches details on Mobility Master:

```
(host) [mynode] #show openflow-controller switches

Switches
--------
Dpid                     IP                    Version  Status  Auxiliary-Status/Id
Capabilities                                      Description
----                     --                    -------  ------  -------------------  ---------
---                                        -----------
00:00:00:1a:1e:01:bf:70  192.168.200.16:43364  v1.3     Up      Down/0               Flow
stats, Table stats, Port stats, Queue Stats  Aruba Networks, Inc. Aruba7240 8.0.0.0-svcs-ctrl
UCC-Sol-7240 BC0003370
00:00:00:1a:1e:01:ae:28  192.168.200.14:45570  v1.3     Up      Down/0               Flow
stats, Table stats, Port stats, Queue Stats  Aruba Networks, Inc. Aruba7210 8.0.0.0-svcs-ctrl
UCC-Sol-7210 BA0009702
00:00:00:1a:1e:01:99:e0  192.168.200.15:52066  v1.3     Up      Down/0               Flow
stats, Table stats, Port stats, Queue Stats  Aruba Networks, Inc. Aruba7220 8.0.0.0-svcs-ctrl
UCC-Sol-7220 BB0003406
```

```
00:00:00:0b:86:9a:4e:77  10.16.125.12:46797    v1.3     Up      Down/0              Flow
stats, Table stats, Port stats, Queue Stats  Aruba Networks, Inc. Aruba7010 8.0.0.0-svcs-ctrl
UCC-BOC1 CG0001826
Total number of switches: 4
```

The following command displays the OpenFlow resource usage information on Mobility Master:

(host) [mynode] #show openflow-controller resource

```
Resource Usage
--------------
Process                     PID   Uptime                 RSS (kB)  PSS (kB)  USS (kB)  Data
(kB)
-------                     ---   ------                 --------  --------  --------  ------
---
switch_daemon.0xb869a4e77   8028  1(d) 10(h) 45(m) 13(s)  7316      3997      3896      4076
switch_daemon.0x1a1e0199e0  8010  1(d) 10(h) 45(m) 15(s)  5700      2388      2288      2360
switch_daemon.0x1a1e01ae28  7944  1(d) 10(h) 45(m) 25(s)  5736      2460      2360      2492
switch_daemon.0x1a1e01bf70  7912  1(d) 10(h) 45(m) 31(s)  6604      3285      3184      3284
switch_manager              6429  1(d) 10(h) 47(m) 57(s)  5388      2658      2600      2568
event_dispatcher            6423  1(d) 10(h) 47(m) 57(s)  6196      2308      2116      18808
packetin_dispatcher         6419  1(d) 10(h) 47(m) 57(s)  7092      3421      3232      110112
flow_manager                6412  1(d) 10(h) 47(m) 57(s)  14880     10993     10796     115104
topology                    6391  1(d) 10(h) 47(m) 58(s)  5992      2267      2080      18676
routing_switch              6408  1(d) 10(h) 47(m) 58(s)  8848      4850      4644      86704
topology_discovery          6400  1(d) 10(h) 47(m) 58(s)  6616      2912      2720      19376
Total Processes: 11  RSS: 80368 (kB)  PSS: 41539 (kB)  USS: 39916 (kB)
```

The following command displays the flow table information for the routing_switch app:

(host) [mynode] #show openflow-controller flow-table app-name routing_switch

```
Flow-table
----------
Dpid                    In Port  Src Mac  Dst Mac  Ether   Src IP  Dst IP  Proto  Src Port
Dst Port  App Name        Actions
----                    -------  -------  -------  -----   ------  ------  -----  --------  -
-------  --------        -------
00:00:00:1a:1e:01:bf:70  *        *        *        0x806   *       *       *      *         *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:bf:70  *        *        *        0x86dd  *       *       58     135       *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:bf:70  *        *        *        0x86dd  *       *       58     136       *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:ae:28  *        *        *        0x86dd  *       *       58     135       *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:ae:28  *        *        *        0x86dd  *       *       58     136       *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:ae:28  *        *        *        0x806   *       *       *      *         *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:99:e0  *        *        *        0x806   *       *       *      *         *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:99:e0  *        *        *        0x86dd  *       *       58     135       *
        routing_switch  output=normal,output=controller
00:00:00:1a:1e:01:99:e0  *        *        *        0x86dd  *       *       58     136       *
        routing_switch  output=normal,output=controller
00:00:00:0b:86:9a:4e:77  *        *        *        0x86dd  *       *       58     135       *
        routing_switch  output=normal,output=controller
00:00:00:0b:86:9a:4e:77  *        *        *        0x86dd  *       *       58     136       *
        routing_switch  output=normal,output=controller
Flow-table
----------
Dpid                    In Port  Src Mac  Dst Mac  Ether  Src IP  Dst IP  Proto  Src Port
Dst Port  App Name        Actions
----                    -------  -------  -------  -----  ------  ------  -----  --------  --
------  --------        -------
```

```
00:00:00:0b:86:9a:4e:77  *        *        *        0x806  *       *       *      *         *
       routing_switch  output=normal,output=controller
Total number of flows: 12
```

The following command displays the OpenFlow port configuration on Mobility Master:

```
(host) [mynode] #show openflow-controller ports
```

```
Ports
-----
Dpid                     Port No  Name            MAC               Status  TX Packets  RX
Packets
----                     -------  ----            ---               ------  ----------  ----
------
00:00:00:1a:1e:01:bf:70  1        GE0/0/0         00:1a:1e:01:bf:71  Up      13670286
14405254
00:00:00:1a:1e:01:ae:28  2        GE0/0/0         00:1a:1e:01:ae:29  Up      7195701
8124898
00:00:00:1a:1e:01:99:e0  3        PC0             00:1a:1e:01:99:e0  Up      9064283
9704562
00:00:00:0b:86:9a:4e:77  11       GE0/0/8         00:0b:86:9a:4e:80  Down    0           0
00:00:00:0b:86:9a:4e:77  12       GE0/0/9         00:0b:86:9a:4e:81  Down    0           0
00:00:00:0b:86:9a:4e:77  13       GE0/0/10        00:0b:86:9a:4e:82  Down    0           0
00:00:00:0b:86:9a:4e:77  14       GE0/0/11        00:0b:86:9a:4e:83  Down    0           0
00:00:00:0b:86:9a:4e:77  15       GE0/0/12        00:0b:86:9a:4e:84  Down    0           0
00:00:00:0b:86:9a:4e:77  16       GE0/0/13        00:0b:86:9a:4e:85  Down    0           0
00:00:00:0b:86:9a:4e:77  17       GE0/0/14        00:0b:86:9a:4e:86  Down    0           0
00:00:00:0b:86:9a:4e:77  18       GE0/0/15        00:0b:86:9a:4e:87  Down    0           0
00:00:00:0b:86:9a:4e:77  19       GE0/0/16        00:0b:86:9a:4e:88  Down    0           0
00:00:00:0b:86:9a:4e:77  20       GE0/0/17        00:0b:86:9a:4e:89  Down    0           0
00:00:00:0b:86:9a:4e:77  21       PC0             00:0b:86:9a:4e:77  Down    0           0
00:00:00:0b:86:9a:4e:77  7        GE0/0/4         00:0b:86:9a:4e:7c  Down    0           0
00:00:00:0b:86:9a:4e:77  6        GE0/0/3         00:0b:86:9a:4e:7b  Down    0           0
00:00:00:0b:86:9a:4e:77  5        GE0/0/2         00:0b:86:9a:4e:7a  Down    0           0
00:00:00:0b:86:9a:4e:77  9        GE0/0/6         00:0b:86:9a:4e:7e  Down    0           0
00:00:00:0b:86:9a:4e:77  10       GE0/0/7         00:0b:86:9a:4e:7f  Down    0           0
00:00:00:0b:86:9a:4e:77  8        GE0/0/5         00:0b:86:9a:4e:7d  Down    0           0
00:00:00:0b:86:9a:4e:77  4        GE0/0/1         00:0b:86:9a:4e:79  Down    0           0
00:00:00:0b:86:9a:4e:77  2        GE0/0/0         00:0b:86:9a:4e:78  Up      4637389
4551706
```

Related Commands

Command	Description
openflow-controller	Configures the OpenFlow Controller on Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master.

show openflow-profile

```
show openflow-profile
```

Description

The command displays the OpenFlow profile information configured on the managed device.

Syntax

No parameters.

Example

The following command displays the OpenFlow profile information on the managed device. Execute the following commands to verify OpenFlow profile configuration on managed devices:

```
(host) [md] #show openflow-profile

Openflow-profile "default"
--------------------------
Parameter                                   Value
---------                                   -----
State                                       Enabled
Openflow mode                               passive
Openflow version                            v1.3
controller-ip                               10.16.125.115:6633
VLAN ID or range(s) of VLAN IDs             1,124,400,600
openflow tls                                Disabled
certificate-file                            none
key-file                                    none
ca-certificate-file                         none
```

Related Commands

Command	Description
openflow-profile	This command configures OpenFlow profile on the managed device

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config or Enable mode on managed device.

show packages

```
show packages [supported|upgrade-history]
```

Description

This command displays information about the downloaded and active Loadable Service Module (LSM) service packages.

Syntax

Parameter	Description
`supported`	Displays all packages supported by Mobility Master.
`upgrade-history`	Displays package installation logs.

Usage Guidelines

The following command lists all packages downloaded on a given Mobility Master:

```
(host) [mynode] #show packages

Packages
--------
Package       Name                       Version                       Build Num  Built On
                Package Version  Active
-------       ----                       -------                       ---------  --------
                ---------------  ------
airgroup      default_airgroup_pkg       ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
airmatch      default_airmatch_pkg       ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
appRF         default_appRF_pkg          ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
arm_cm        default_arm_cm_pkg         ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
nbapi_helper  default_nbapi_helper_pkg   ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
ucm           default_ucm_pkg            ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
web_cc        default_web_cc_pkg         ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
wms           default_wms_pkg            ArubaOS_MM_8.0.0.0-svcs-ctrl  55038      Mon May 16
14:44:20 PST 2016  1                YES
```

The following command lists all packages supported by a given Mobility Master:

```
(host) [mynode] #show packages supported

Packages Supported
------------------
Package Name  Version
------------  -------
airgroup      1
ucm           1
wms           1
arm_cm        1
web_cc        1
nbapi_helper  1
airmatch      1
appRF         1
```

The following command displays the package installation logs:

```
(host) [mynode] #show packages upgrade-history

May 17 21:00:11 Copying files to airgroup dir
May 17 21:00:11 Creating symbolic link to mdns binary
May 17 21:00:11 Package default_airgroup_pkg installation was successfully
May 17 21:00:12 Copying files to ucm dir
May 17 21:00:12 Creating symbolic link to ucm binary
May 17 21:00:12 Package default_ucm_pkg installation was successfully
May 17 21:00:12 Copying files to wms dir
May 17 21:00:12 Creating symbolic link to wms binary
May 17 21:00:12 Package default_wms_pkg installation was successfully
May 17 21:00:12 Copying files to arm_cm dir
May 17 21:00:12 Creating symbolic link to arm binary
May 17 21:00:12 Package default_arm_cm_pkg installation was successfully
May 17 21:00:12 Copying files to web_cc dir
May 17 21:00:12 Creating symbolic link to web_cc binary
May 17 21:00:12 Package default_web_cc_pkg installation was successfully
May 17 21:00:12 Copying files to nbapi_helper dir
May 17 21:00:12 Creating symbolic link to nbapi_helper binary
May 17 21:00:12 Package default_nbapi_helper_pkg installation was successfully
May 17 21:00:13 Copying files to airmatch dir
May 17 21:00:13 Copying airmatch binary
May 17 21:00:13 Package default_airmatch_pkg installation was successfully
May 17 21:00:13 Copying files to appRF dir
May 17 21:00:13 Creating symbolic link to appRF binary
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show packet-capture

```
show packet-capture
   controlpath-pcap [hex]
   datapath-pcap [hex]
```

Description

Displays packet capture status on the controller.

Syntax

Parameter	Description
`controlpath-pcap [hex]`	Displays controlpath packets captured in the local-filesystem.
`datapath-pcap [hex]`	Displays datapath packets captured in the local-filesystem.

Example

The output of this command shows the packet capture configuration details.

```
(host)[mynode] #show packet-capture
Active Capture Destination
--------------------------
Destination    IP         1.2.3.4
Active Capture (Controlpath)
----------------------------
Interprocess   Disabled
Sysmsg         Disabled
TCP            Enabled    Ports: 2
UDP            Enabled    Ports: 5
Other          Enabled
Active Capture (Datapath)
-------------------------
Wifi-Client    Enabled    Mac: 00:0b:86:6d:47:6c   Filter: Decrypted
Ipsec          Enabled    Peer: 10.1.1.1
(host) (config) #show packet-capture-defaults
Default Capture Destination
---------------------------
Destination    Local-Filesystem
Default Capture (Controlpath)
-----------------------------
Interprocess   Disabled
Sysmsg         Disabled
TCP            Enabled    Ports: 80 8080
UDP            Enabled    Ports: All
Other          Disabled
Default Capture (Datapath)
--------------------------
Wifi-Client    Enabled    Mac: 00:0b:86:6d:47:6c   Filter: Encrypted
Ipsec          Disabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show packet-capture-defaults

```
show packet-capture-defaults
```

Description

Displays the status of default packet capture options.

Syntax

No parameters.

Example

The output of this command shows packet capture status.

```
(host) # show packet-capture-defaults

Current Active Packet Capture Actions(current switch)
=====================================================
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.


Packet Capture Defaults(across switches and reboots if saved)
=============================================================
Packet filtering for TCP ports disabled.
Packet filtering for UDP ports disabled.
Packet filtering for internal messaging opcodes disabled.
Packet filtering for all other packets disabled.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show pan active-profile

```
show pan active-profile
```

Description

This command shows the active PAN firewall profile at the managed device level.

Syntax

No syntax.

Usage Guidelines

Issue this command to show the current active PAN firewall profile running on the managed device.

```
(host)[node]#show pan active-profile
Palo Alto Networks Active Profile
---------------------------------
Parameter                         Value
---------                         -----
Active Palo Alto Networks profile  PAN-Group-1
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show pan-options

```
show pan-options
```

Description

This command displays configured settings for integrating a branch controller with a Palo Alto Networks (PAN) firewall.

Syntax

No syntax.

Usage Guidelines

Issue this command to see the connection status of the PAN firewalls associated with the controller.

```
(host)[node]#show pan profile PAN-Group-1

Palo Alto Networks Servers Profile "PAN-Group-1"
------------------------------------------------
Parameter                                  Value
---------                                  -----
Palo Alto Networks Firewall                1.2.3.4:443 abc/********
Palo Alto Networks Firewall                2.2.2.2:123 2222/********
Palo Alto Networks Firewall                3.3.3.3:333 3333/********
Palo Alto Networks Firewall                1.1.1.1:443 admin/********
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show pan state

```
show pan state
```

Description

This command shows the current connection status of PAN firewalls.

Syntax

No syntax.

Usage Guidelines

Issue this command to see the connection status of the PAN firewalls associated with the controller.

```
(host)[node] #show pan state
Palo Alto Networks Servers Connection State[PAN-Group-1]
-------------------------------------------------------
Firewalls   State
---------   -----
1.2.3.4:443 DOWN
2.2.2.2:123 UP[11/25/13 12:45:49]Established
3.3.3.3:333 UP[11/25/13 12:45:48]Established
1.1.1.1:443 UP[11/25/13 12:45:50]Established
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master

show pan statistics

```
show pan statistics
```

Description

This command shows PAN firewall interface statistics.

Syntax

No syntax.

Usage Guidelines

Issue this command to see PAN firewall interface statistics.

```
(host)[node](config) #show pan statistics
Palo Alto Networks Interface Statistics Summary
-----------------------------------------------
Login Reqts  Logout Reqts  Refresh Reqts
-----------  ------------  -------------
0            0             0
Per-PAN server Statistics Summary
---------------------------------
PAN Server       User-ID Reqts  Sent  Skipped  Success  Failure  Last Error
----------       -------------  ----  -------  -------  -------  ----------
1.2.3.4:443  0              0     0        0        0
```

Parameter	Description
Palo Alto Networks Interface Statistics Summary	
Login Reqts	Total number of login requests.
Logout Reqts	Total number of logout requests.
Refresh Reqts	Total number of refresh requests.
Per-PAN server Statistics Summary	
PAN Server	The PAN Server IP address.
User-ID Reqts	Total number of login, logout, and refresh requests.
Sent	Number of requests sent.
Skipped	Number of requests skipped.
Success	Number of requests successfully handled.
Failure	Number of requests that were not successfully received.
Last Error	The last failure error received.

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show papi-security

```
show papi-security
```

Description

This command shows a configured papi-security profile.

Syntax

Parameter	Description	Range	Default
`PAPI Key`	The key string. The key authenticates the messages between systems.	Range: 10–64 characters	—
`Enhanced security mode`	Indicates if the enhanced security mode is enabled or disabled. This mode causes the system to reject messages when an incorrect key is used.	—	disabled

Usage Guidelines

Execute this command to show the selected papi-security profile configuration. The **papi-security** command is used to enforce advanced security options and provides an enhanced level of security.

The **Parameter** column displays the PAPI Key and Enhanced security mode parameters. The **Value** column displays a Papi key value (encrypted) and indicates whether the Enhanced security mode is enabled or disabled.

```
(host)[mynode] #show papi-security

PAPI Security Profile
---------------------
Parameter               Value
---------               -----
PAPI Key                ********
Enhanced security mode  Enabled
```

Related Commands

Command	Description
papi-security	This command enforces advanced security options and provides an enhanced level of security.

Command History

Release	Modification
ArubaOS 8.0.1 .0	This command is introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show papi kernel-socket-stats

```
show papi kernel-socket-stats
```

Description

This command shows the state of UDP PAPI sockets in the kernel.

Syntax

No syntax.

Usage Guidelines

Issue this command to show the state of the UDP PAPI sockets in the kernel. The following example shows partial output of this command.

```
(host)[node] #show papi-security
(7240-223) #show papi kernel-socket-stats Kernel PAPI Statistics
Port                                                RxSockbufSize RxSockbufHimark CurRxQLen MaxRxQLen Drops
9344(9344)                                            2097152                7104         0         3         0
8449(Utility Process)                                 2097152                   0         0         0         0
9345(9345)                                            2097152                   0         0         0         0
514(514)                                              2097152                   0         0         0         0
9476(9476)                                            2097152                   0         0         0         0
9348(9348)                                            2097152                   0         0         0         0
9220(9220)                                            2097152                   0         0         0         0
8453(Control Plane Security Daemon)                   2097152                2368         0         1         0
9222(9222)                                            2097152                   0         0         0         0
9478(9478)                                            2097152                   0         0         0         0
8455(Spectrum Process)                                2097152                   0         0         0         0
8456(STM Monitoring)                                  2097152                   0         0         0         0
9224(9224)                                            2097152                   0         0         0         0
9481(9481)                                            2097152                   0         0         0         0
9482(9482)                                            2097152                   0         0         0         0
8458(Arci cli helper server)                          2097152                   0         0         0         0
9226(9226)                                            2097152                   0         0         0         0
9483(9483)                                            2097152                   0         0         0         0
9355(9355)                                            2097152                   0         0         0         0
8459(WMS Monitoring)                                  2097152                   0         0         0         0
9484(9484)                                            2097152                   0         0         0         0
9485(9485)                                            2097152                   0         0         0         0
9486(9486)                                            2097152                   0         0         0         0
9359(9359)                                            2097152                   0         0         0         0
9231(9231)                                            2097152                   0         0         0         0
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or config mode on Mobility Master.

show perf-test reports

```
show perf-test reports
   ap {ap-name <ap-name>}|{ip-addr <ip>}|{ip6-addr <ip6>}
   controller
```

Description

Use this command under the guidance of Aruba technical support to view the results of an Iperf throughput test launched from an AP or controller.

Syntax

Parameter	Description
ap	Display the results of an Iperf throughput test launched from an AP.
`ap-name <ap-name>`	Name of the AP.
`ip-addr <ip-addr>`	IPv4 address of the AP.
`ip6-addr <ip6-addr>`	IPv6 address of the AP.
`controller`	Display the results of an Iperf throughput test launched from a controller.

Usage Guidelines

Issue this command to view a report file of test data from a client-mode Iperf throughput test launched from an AP or controller. Tests launched in server mode do not generate reports. Only 130 Series, 220 Series, and AP-105 access points connected to a 7200 Series controller support this feature.

Related Commands

Command	Description
perf-test server	Use this command under the guidance of Aruba technical support to launch an Iperf throughput test

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
7200 Series controllers	Base operating system	Enable mode on Mobility Master.

show phonehome

```
show phonehome
   global
   history
   report-status
   stats
```

Description

Use this command to view current configuration settings and debugging statistics for the PhoneHome automatic reporting feature.

Syntax

Parameter	Description
`global`	Show whether the PhoneHome service and auto-reporting is enabled or disabled, and display current HTTPS or SMTP settings for this feature.
`history`	Issue this command under the guidance of Aruba support troubleshoot PhoneHome automatic reporting.
`report-status`	Issue this command under the guidance of Aruba support troubleshoot PhoneHome automatic reporting.
`stats`	Include this parameter to show the number of weekly schedule or manual reports successfully sent to Activate or the SMTP server, the number of times the controller attempted to retry sending a report, and the number of reports that failed after one or more retry attempts, and

Usage Guidelines

The automatic reporting feature, also known as *PhoneHome* , allows a controller to securely contact Aruba support servers over the Internet to report events such as hardware failures, software malfunctions, and other critical events. When the PhoneHome automatic reporting feature is enabled, the controller sends Aruba support weekly reports about the controller's configuration, licenses, software and hardware versions, and any software malfunctions via a secure email.

Example

The following command displays global phonehome settings:

```
(host)[mynode] #show phonehome global
PhoneHome information:
PhoneHome Service:      Disabled
PhoneHome Auto-Report:  Disabled
Local SMTP server:      192.0.2.10:25
SMTP From Email:        admin@example.com
Max Attachment Size:    10 MB
SMTP Authen User:       John_Smith
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show poe

```
show poe [<slot/module/port>]
```

Description

Displays the PoE status of all or a specific port on the controller.

Syntax

No parameters.

Example

The output of this command shows the PoE status of the specified slot, module and port.

```
(host)[mynode] # show poe 0/0/2

PoE Status
----------
Port      Status  Voltage(mV)  Current(mA)  Power (mW)
----      ------  -----------  -----------  ----------
GE 0/0/2  Off      N/A           N/A          N/A
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show port link-event

```
show port link-event
```

Description

Displays the link status on each of the port on the controller.

Syntax

No parameters.

Example

The output of this command shows the link status on all ports in the controller.

```
(host)[mynode] # show port link-event

Slot/Port    UP       DOWN              Slot/Port    UP      DOWN
---------    --       ----              ---------    --      ----
  0/0/0      1        0                 0/0/1        5886    5886
  0/0/2      49751    49750             0/0/3        50      49
  0/0/3      2589     2588              0/0/5        228     227
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show port monitor

```
show port monitor
```

Description

Displays the list of ports that are configured to be monitored.

Syntax

No parameters.

Example

The output of this command shows the link status on all ports in the controller.

```
(host)[mynode]# show port monitor

Monitor Port  Port being Monitored
------------  --------------------
FE 1/10       FE 1/20
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show port mux

```
show port mux
```

Description

Displays the list of ports with MUX capability.

Syntax

No parameters.

Example

The output of this command shows the ports with MUX capability.

```
            (host)[mynode] # show port mux

  FE 2/9
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show port stats

```
show port stats [<slot/module/port>]
```

Description

Displays the activity statistics on each of the port on the controller.

Syntax

Parameter	Description
`<slot/module/port>`	Physical port in **<slot>/<module>/<port>** format.

Example

The output of this command shows the link status on all ports in the controller.

```
(host)[mynode] # show port stats

Port Statistics
---------------
Port      PacketsIn  PacketsOut  BytesIn   BytesOut  InputErrorBytes  OutputErrorBytes
CRCErrors
----      ---------  ----------  -------   --------  ---------------  ----------------  ------
---
GE 0/0/0  745969     18810       86791364  10599122  0                0                 0
GE 0/0/1  0          0           0         0         0                0                 0
GE 0/0/2  0          0           0         0         0                0                 0
GE 0/0/3  0          0           0         0         0                0                 0
GE 0/0/4  0          0           0         0         0                0                 0
GE 0/0/5  0          0           0         0         0                0                 0
```

The output of this command includes the following parameters:

Parameter	Description
`Port`	Displays the physical port on the controller.
`PacketIn`	Indicates the total number of incoming packets to the port.
`PacketOut`	Indicates the total number of outgoing packets from the port.
`BytesIn`	Indicates the total number of incoming data (in bytes) to the port.
`BytesOut`	Indicates the total number of outgoing data (in bytes) from the port.
`InputErrorBytes`	Indicates input error bytes on the port.
`OutputErrorBytes`	Indicates the output error bytes on the port.
`CRCErrors`	Indicates the Cyclic Redundancy Check (CRC) errors on the port.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show port status

```
show port status [<slot/module/port>]
```

Description

Displays the status of all ports on the controller.

Syntax

Parameter	Description
`<slot/module/port>]`	Physical port in **<slot>/<module>/<port>** format.

Example

The output of this command shows the status of all ports in the controller.

```
(host)[mynode]# show port status

Port Status
-----------
Slot-Port   PortType   AdminState   OperState   PoE   Trusted   SpanningTree   PortMode
---------   --------   ----------   ---------   ---   -------   ------------   --------
0/0/0       GE         Enabled      Up          N/A   Yes       Forwarding     Access
0/0/1       GE         Enabled      Down        N/A   Yes       Disabled       Access
0/0/2       GE         Enabled      Down        N/A   Yes       Disabled       Access
0/0/3       GE         Enabled      Down        N/A   Yes       Disabled       Access
0/0/4       GE         Enabled      Down        N/A   Yes       Disabled       Access
0/0/5       GE         Enabled      Down        N/A   Yes       Disabled       Access

Speed    Duplex
-----    ------
1 Gbps    Full
Auto      Auto
Auto      Auto
Auto      Auto
Auto      Auto
Auto      Auto
```

The output of this command includes the following parameters:

Parameter	Description
`Slot-Port`	Physical port in **<slot>/<module>/<port>** format.
`PortType`	Displays the type of physical port. ■ **FE**: Fast Ethernet ■ **GE**: Gigabit Ethernet ■ **PC**: Port Channel
`AdminState`	Indicates if the physical port is enabled or disabled.
`OperState`	Indicates if the current status of the physical port is up or down.

Parameter	Description
PoE	Indicates if the physical port is Power over Ethernet (PoE) enabled.
Trusted	Indicates if the physical port is trusted.
SpanningTree	Indicates the state of spanning tree.
PortMode	Indicates the port mode of the physical port.
Speed	Indicates the port speed.
Duplex	Indicates the direction of traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show port trusted

```
show port trusted
```

Description

Displays the list of ports configured with trusted profiles.

Syntax

No parameters.

Example

The output of this command shows the list of ports with trusted profile.

```
(host)[mynode]# show port trusted

FE 1/0
FE 1/1
FE 1/2
FE 1/3
FE 1/4
FE 1/5
FE 1/6
FE 1/7
FE 1/8
FE 1/9
FE 1/10
FE 1/11
FE 1/12
FE 1/13
FE 1/14
FE 1/15
FE 1/16
FE 1/17
FE 1/18
FE 1/19
FE 1/20
FE 1/21
FE 1/22
FE 1/23
GE 1/24
GE 1/25
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show port xsec

```
show port xsec
```

Description

Displays the list of xSec enabled ports.

Syntax

No parameters.

Example

The output of this command shows the list of xSec enabled ports.

```
(host)[mynode] #show port xsec

Xsec Ports
----------
Interface  xsec vlan  state

--------- --------- -----
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show priority-map

```
show priority-map
```

Description

Displays the list of priority maps on a interface.

Syntax

No parameters.

Example

The output of this command shows the priority maps configured on all interfaces.

```
(host)[node] # show priority-map

Priority Map
------------
ID  Name    DSCP-TOS  DOT1P-COS
--  ----    --------  ---------
1   my-map  4-20,60      4-7
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show processes

```
show processes [sort-by {cpu | memory}]
```

Description

Displays the list of all system process running on the managed device. You can sort the list either by CPU intensive or memory intensive processes.

Syntax

Parameter	Description
`sort-by`	Add a sort filter to the output
`cpu`	This will sort output based on CPU usage.
`memory`	This will sort output based on memory usage.

Example

The output of this command shows list of system processes sorted by CPU usage.

```
(host) [mynode] (config) # show priority-map

%CPU S   PID  PPID   VSZ  RSS   F  NI START     TIME      EIP CMD
 3.7 S   595   517 20908 12184 040   0 Apr24 03:39:04 303a4fa8 /mswitch/bin/fpapps
 0.2 S 12354   410  1028   296 000   0 02:13 00:00:00 30087fa8 sleep 10
 0.1 S   536   441 12012 7264 040   0 Apr24 00:09:08 100e4a74 /mswitch/mysql/libexec/mysqld --
basedir=/mswitch/mysql --datadir=/var/
 0.0 S     2     1     0    0 040   0 Apr24 00:00:00 00000000 [keventd]
 0.0 S     4     0     0    0 040   0 Apr24 00:00:00 00000000 [kswapd]
 0.0 S     6     0     0    0 040   0 Apr24 00:00:00 00000000 [kupdated]
 0.0 S    57     1     0    0 040   0 Apr24 00:00:00 00000000 [kjournald]
 0.0 S    67     1  1036  424 000   0 Apr24 00:00:00 30087fa8 /bin/sh /mswitch/bin/syslogd_
start
 0.0 S     1     0  1028  384 100   0 Apr24 00:00:12 30087fa8 init
 0.0 S   397     1  1732  804 100   0 Apr24 00:00:00 30152fa8 /mswitch/bin/nanny
/mswitch/bin/nanny_list 0
 0.0 S   399   397 14140 10172 100  0 Apr24 00:00:16 303c8fa8 /mswitch/bin/arci-cli-helper
 0.0 S   402     1   768  268 040   0 Apr24 00:00:00 30060fa8 /sbin/tftpd -s -l -u nobody
/mswitch/sap
 0.0 S    69    67  1404  752 100   0 Apr24 00:01:27 300d3fa8 /mswitch/bin/syslogd -x -r -n -m
0 -f /mswitch/conf/syslog.conf
 0.0 S   407   397  3100 1028 100   0 Apr24 00:00:00 302a0fa8 /mswitch/bin/packet_filter
 0.0 S   408   397  4296 1340 100   0 Apr24 00:00:00 30339fa8 /mswitch/bin/certmgr
 0.0 R     3     0     0    0 040  19 Apr24 00:00:01 00000000 [ksoftirqd_CPU0]
 0.0 S   453   397   700  284 000   0 Apr24 00:01:20 30087fa8 /mswitch/bin/msgHandler -g
 0.0 S   468   397  1236  492 100   0 Apr24 00:00:00 300f8fa8 /mswitch/bin/pubsub
 0.0 S   484   397 18456 14064 100  0 Apr24 00:00:19 303c8fa8 /mswitch/bin/cfgm
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platformss	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show processes monitor stats

```
show processes monitor statistics
```

Description

Displays the current status of all the processes running under the process monitor watchdog.

Syntax

No parameters.

Example

A partial example of the output of this command is shown below:

```
(host) [mynode] (config) #show process monitor statistics

   Process Monitor Statistics
   --------------------------
   Name                          State            Restarts  Timeout Value  Timeout
                                                           Chances
   ----                          -----            --------  -------------  ---------------
   /mswitch/bin/arci-cli-helper  PROCESS_RUNNING  0         120            3
   /mswitch/bin/fpcli            PROCESS_RUNNING  0         120            3
   /mswitch/bin/packet_filter    PROCESS_RUNNING  0         120            3
   /mswitch/bin/certmgr          PROCESS_RUNNING  0         120            3
   /mswitch/bin/dbstart          PROCESS_RUNNING  0         120            3
   /mswitch/bin/cryptoPOST       PROCESS_RUNNING  0         120            3
   /mswitch/bin/sbConsoled       PROCESS_RUNNING  0         120            3
   /mswitch/bin/pubsub           PROCESS_RUNNING  0         120            3
   /mswitch/bin/cfgm             PROCESS_RUNNING  0         120            3
   /mswitch/bin/syslogdwrap      PROCESS_RUNNING  0         120            3
   /mswitch/bin/aaa              PROCESS_RUNNING  0         120            3
   /mswitch/bin/fpapps           PROCESS_RUNNING  0         120            3
   /mswitch/bin/pim              PROCESS_RUNNING  0         120            3
   /mswitch/bin/lic
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show profile-errors

```
show profile-errors
```

Description

Displays the list of invalid user-created profiles.

Syntax

No parameters.

Example

The output of this command shows list of profiles that are invalid and also displays the error in those profiles. In this example, the VLAN 1000 that is mapped to a virtual-ap that does not exist.

```
(host)[node] #show profile-errors

Invalid Profiles
----------------
Profile                      Error
-------                      -----

wlan virtual-ap "test-vap"  VLAN 1000 does not exist
```

The following are the list of some profile errors:

Error	Description
Named VLAN [named_VLAN] is removed	These errors are displayed if a virtual AP profile is configure with a VLAN that does not exist.
Named VLAN [named_VLAN] is not mapped	
Named VLAN [named_VLAN] is invalid	
VLAN [x] does not exist	
Server group is invalid	This error is displayed if an AAA profile is configured an invalid server group.
User derivation rule is invalid	This error is displayed if a user role in an AAA profile is invalid.
User role is invalid	
Controller country code is undefined	These errors are displayed, if your controller is not set to the correct country code or if the country code specified in a WLAN profile does not match the controller's country code.
Country [country_name] does not match controller country [country_name]	
Opmode requires WPA key	This message is displayed if a SSID profile is configured without a WPA key.
WARNING: if weptxkey = [x], wepkey[x] must be set in order to use static WEP	This message is displayed if a SSID profile is configured to use a static WEP and the WEP is not configured.

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show profile-hierarchy

```
show profile-hierarchy
```

Description

Displays the profile hierarchy template.

Syntax

No parameters.

Usage Guidelines

The output of this command shows how profiles relate to each other, and how some higher-level profiles reference other lower-level profiles. The output of this command will vary, depending upon controller configuration and licenses.

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show profile-list aaa

```
show profile-list aaa [{alias-group [page | start]} | {authentication [captive-portal | dot1x
| mac | stateful-ntlm | wispr]} |{authentication-server [ldap | radius | tacacs | windows]} |
{profile} | {rfc-3576-server} | {server-group} | {xml-api}]
```

Description

Displays the list of AAA profiles.

Syntax

Parameter	Description
`alias-group`	Lists all alias-groups.
`page`	Specify the number of items to display
`start`	Specify the first item to display
`authentication`	List of aaa authentication profiles.
`captive-portal`	Captive portal authentication profiles.
`dot1x`	802.1X authentication profiles.
`mac`	MAC authentication profiles.
`stateful-ntlm`	Stateful-NTLM authentication profiles.
`wispr`	WISPr authentication profiles.
`authentication-server`	List of aaa authentication servers
`ldap`	List of servers using LDAP for AAA authentication.
`radius`	List of servers using RADIUS for AAA authentication.
`tacacs`	List of servers using TACACS+ for AAA authentication.
`windows`	List of Windows servers used for AAA authentication.
`profile`	Displays the AAA profile details.
`rfc-3576-server`	Displays IP address of RADIUS servers that use RFC 3576 specification to exchange authorization messages.
`server-group`	List of server group used for RADIUS accounting.
`xml-api`	List of servers configured in an external XML API server.

Example

The output of this command shows list of AAA profiles that use captive-portal authentication.

```
(host)[node] # show profile-list aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
```

```
Name     References  Profile Status
----     ----------  --------------
default  1
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list airgroupprofile

```
show profile-list airgroupprofile {cppm|domain|ipv6|page|service|start} [page | start]
```

Description

Displays the list of configured AirGroup profiles.

Syntax

Parameter	Description
`cppm`	Displays all AirGroup ClearPass Policy Manager profiles.
`domain`	Displays all AirGroup domain profiles.
`ipv6`	Displays all AirGroup IPv6 profiles.
`service`	Displays all AirGroup service profiles.
`page`	Specify the number of items to display
`start`	Specify the first item to display

Example

The output of this command shows a list of AirGroup profiles.

```
(host)[node] (config) # show profile-list airgroupprofile
AirGroup Profile List
---------------------
Name     References  Profile Status
----     ----------  --------------
default  1
```

Related Commands

Command	Description
airgroupprofile	Configures an AirGroup profile.

Command History

	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list ap

```
show profile-list ap [ enet-link-profile | mesh-cluster-profile |
   mesh-ht-ssid-profile | mesh-radio-profile | regulatory-domain-profile |
   snmp-profile | snmp-user-profile | system-profile | wired-ap-profile ]
```

Description

Displays the list of AP profiles.

Syntax

Parameter	Description
`enet-link-profile`	Display a list of AP Ethernet link profiles.
`mesh-cluster-profile`	Display a list of mesh cluster profiles used by mesh nodes.
`mesh-ht-ssid-profile`	Display a list of mesh high-throughput SSID profiles used by mesh nodes.
`mesh-radio-profile`	Display a list of mesh radio profiles used by mesh nodes.
`multizone-profile`	Display a list of all AP multizone profil
`regulatory-domain-profile`	Display a list of AP regulatory profiles.
`snmp-profile`	Display a list of SNMP profiles.
`snmp-user-profile`	Display a list of SNMPv3 user profiles.
`system-profile`	Display a list of AP system profiles.
`wired-ap-profile`	Display a list of wired AP profiles.

Example

The output of this command shows list of profiles that are invalid and also displays the error in those profiles.

```
(host)[mynode] # show profile-list aaa authentication captive-portal

Captive Portal Authentication Profile List
------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  1
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list ap-group

```
show profile-list ap-group
```

Description

Displays the status of AP groups profiles in the controller.

Syntax

No parameters.

Example

The output of this command shows the status of AP group profiles in the controller.

```
(host)[node] # show profile-list ap-group

AP group List
-------------
Name      Profile Status
----      --------------
default

Total:1
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list ap-name

```
show profile-list ap-name
```

Description

Displays the status of AP profiles in the controller.

Syntax

No parameters.

Example

The output of this command shows status of AP profiles in the controller.

```
(host)[node] # show profile-list ap-name

AP name List
------------
Name  Profile Status
----  --------------

Total:0
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list est

```
show profile-list est profile [page | start]
```

Description

Displays the list of EST profiles.

Syntax

Parameter	Description
`profile`	Displays all EST profiles.
`page`	Specify the number of items to display
`start`	Specify the first item to display

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command shows a list of EST profiles.

```
(host)[node] (config) # #show profile-list est profile

EST Profile List
----------------
Name     References  Profile Status
----     ----------  --------------
default  0

Total:1
```

Command History

	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list ha

```
show profile-list ha
   group-profile [page | start]
```

Description

Displays the list of HA profiles.

Syntax

Parameter	Description
`group-profile`	Lists all HA group information.
`page`	Specify the number of items to display
`start`	Specify the first item to display

Example

The output of this command shows list of HA group profile information.

```
(host)[node] # show profile-list ha group-profile

HA group information List
-------------------------
Name  Profile Status
----  --------------
Total:0
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list ids

```
show profile-list ids [dos-profile | general-profile | impersonation-profile |
   profile | rate-thresholds-profile | signature-matching-profile |
   signature-profile | unauthorized-device-profile ]
```

Description

Displays the status of all IDS profiles in the controller.

Syntax

Parameter	Description
`dos-profile`	Display a list of IDS DoS profiles.
`general-profile`	Display a list of IDS generate profiles.
`impersonation-profile`	Display a list IDS impersonation profile.
`profile`	Display a list of IDS profiles.
`rate-thresholds-profile`	Display a list of IDS rate threshold profiles.
`signature-matching-profile`	Display a list of IDS signature-matching profiles.
`signature-profile`	Display a list of IDS signature profiles.
`unauthorized-device-profile`	Display a list of IDS unauthorized device profiles.

Example

The output of this command shows a list of all IDS DoS profiles.

```
(host)[node] # show profile-list ids dos-profile

IDS Denial Of Service Profile List
----------------------------------
Name                    References  Profile Status
----                    ----------  --------------
default                 1
ids-dos-disabled        1           Predefined
ids-dos-high-setting    1           Predefined
ids-dos-low-setting     1           Predefined
ids-dos-medium-setting  1           Predefined

Total:5
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show profile-list lc-cluster

```
show profile-list lc-cluster
   group-profile [page | start]
```

Description

Displays the list of classic controller cluster profiles .

Syntax

Parameter	Description
`group-profile`	Lists all controller cluster profiles
`page`	Specify the number of items to display
`start`	Specify the first item to display

Example

The output of this command shows a list of all controller cluster profiles.

```
(host)[node]# show profile-list lc-cluster group-profile

Classsic Controller Cluster Profile List
------------------------
Name    Profile Status
----    --------------
LC-west
Total:1
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list license-pool-profile

```
show profile-list license-pool-profile [page | start]
```

Description

Displays the list of license pool profiles .

Syntax

Parameter	Description
page	Specify the number of items to display
start	Specify the first item to display

Example

The output of this command shows a list of all licensing pools.

```
(host)[node] (config) #show profile-list license-pool-profile
License pool profile List
-------------------------
Name            References  Profile Status
----            ----------  --------------
/md/dev         2
/md/Sunnyvale   1
/md/testpool    0
/md/Testpool2   0
```

Related Commands

Command	Description
license-pool-profile	Use this command to create a local licensing pool and allocate licenses for that licensing pool.

Command HistoryCommand History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list mgmt-server

```
show profile-list mgmt-server {profile <profile_name>} [page <number>] [start <number>]
```

Description

Displays all the Mgmt Config profiles in the controller.

Syntax

Parameter	Description
`mgmt-server {profile <profile_name>`	Specifies the name of the management server profile.
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

The output of this command shows the management server profiles in the controller.

```
(host) (config) #show profile-list mgmt-server profile
Mgmt Config profile List
------------------------
Name          References  Profile Status
----          ----------  --------------
default-ale   0           Predefined (editable)
default-amp   0           Predefined (editable)
Total:2
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list rf

```
show profile-list rf [ arm-profile | dot11a-radio-profile | dot11g-radio-profile |
   event-thresholds-profile | ht-radio-profile | optimization-profile ]
```

Description

Displays the status of all radio profiles.

Syntax

Parameter	Description
`arm-profile`	Details of Adaptive Radio Management (ARM) Profile.
`dot11a-radio-profile`	Details of AP radio settings for the 5GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
`dot11g-radio-profile`	Details of AP radio settings for the 2.4 GHz frequency band, including the ARM profile and the high-throughput (802.11n) radio profile.
`event-thresholds-profile`	Details of events thresholds profile.
`ht-radio-profile`	Details of high-throughput AP radio settings
`optimization-profile`	Details of the RF optimization profile

Example

The output of this command shows status of ARM profile.

```
(host) # show profile-list rf arm-profile

Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1
```

Command History

	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list scheduler-profile

```
show profile-list scheduler-profile [page | start]
```

Description

Displays the list of scheduler profiles.

Syntax

Parameter	Description
page	Specify the number of items to display
start	Specify the first item to display

Example

The output of this command shows a list of scheduler profiles.

```
(host)[node] (config) # show profile-list scheduler-profile
scheduler profile List
----------------------
Name     References  Profile Status
----     ----------  --------------
default  2
Total:1
```

Related Commands

Command	Description
scheduler-profile	Define a schedule profile that associates priorities to four uplink queues.

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show profile-list wlan

```
show profile-list wlan
   anyspot-profile
   bcn-rpt-req-profile
   client-wlan-profile
   dotllk-profile
   dot11r-profile
   edca-parameters-profile
   hotspot
   ht-ssid-profile
   rrm-ie-profile
   ssid-profile
   traffic-management-profile
   tsm-req-profile
   virtual-ap
   wmm-traffic-management-profile]
```

Description

Displays the status of WLAN profiles on the controller.

Syntax

Parameter	Description
anyspot-profile	Shows a list of all anyspot profiles
bcn-rpt-req-profile	Shows a list of all Beacon Report Request profiles
client-wlan-profile	Shows a list of all client WLAN profiles
dot11r-profile	Shows a list of all 802.11r profiles
dot11k-profile	Show a list of all 802.11K profiles
edca-parameters-profile	Show a list of all enhanced distributed channel access (EDCA) profile for APs or for clients (stations)
hotspot	Hotspot/Passpoint configuration settings
advertisement-profile	Shows a list of all Advertisement profile
angp-3gpp-nwk-profile	Shows a list of all ANQP 3GPP Cellular Network profiles
anqp-domain-name-profile	Shows a list of all ANQP Domain Name profiles
anqp-ip-addr-avail-profile	Shows a list of all ANQP IP Address Availability profiles
anqp-nai-realm-profile	Shows a list of all ANQP NAI Realm profiles
anqp-nwk-auth-profile	Shows a list of all ANQP Network Authentication profiles
anqp-roam-cons-profile	Shows a list of all ANQP Roaming Consortium profiles

Parameter	Description
anqp-venue-name-profile	Shows a list of all ANQP Venue Name profiles
h2qp-conn-capability-profile	Shows a list of all H2QP Connection Capability profiles
h2qp-op-cl-profile	Shows a list of all H2QP Operating Class Indication profiles
h2qp-operator-friendly-profile	Shows a list of all H2QP Operator Friendly Name profiles
h2qp-wan-metrics-profile	Shows a list of all H2QP WAN Metrics profiles
hs2-profile	Shows a list of all Hotspot 2.0 profiles
ht-ssid-profile	Show a list of all high-throughput SSID profiles
rrm-ie-profile	Shows a list of all Radio Resource Management Information Element (RRM IE) profiles
traffic-management-profile	Show a list of all traffic management profiles
tsm-req-profile	Show a list of all Transmit Stream/Category Measurement (TSM) request profiles
virtual-ap	Show a list of all the virtual AP profiles
wmm-traffic-management-profile	Show a list of all WMM traffic management profiles

Example

The output of this command shows that the controller has a single ARM profile, “default”.

```
(host)[mynode] # show profile-list rf arm-profile

Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  2

Total:1
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show provisioning-ap-list

```
show provisioning-ap-list
```

Description

Displays the list of all APs that are in queue to be provisioned by the admin.

Syntax

No parameters.

Example

```
(host) [mynode]# show provisioning-ap-list
Access Points Provisioning List
-------------------------------
Current IP       AP Name  AP Group  Location name  SNMP sysLocation  AP Type  Serial #   AP
State
----------       -------  --------  -------------  ----------------  -------  --------   -----
---
191.191.191.253  ap-215   default   N/A            N/A               215      CK0223282  -
Total APs:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on the Mobility Master

show provisioning-params

```
show provisioning-params
```

Description

Displays the list of parameters and the values used to provision the APs.

Syntax

No parameters.

Example

The output of this command shows list of all provisioning parameters and their values.

```
(host) [mynode]# show provisioning-params
AP provisioning
---------------
Parameter                                                       Value
---------                                                       -----
AP Name                                                         N/A
AP Group                                                        default
Location name                                                   N/A
SNMP sysLocation                                                N/A
Master                                                          N/A
Gateway                                                         N/A
IPv6 Gateway                                                    N/A
Netmask                                                         N/A
IP Addr                                                         N/A
IPv6 Addr                                                       N/A
IPv6 Prefix                                                     64
DNS IP                                                          N/A
DNS IPv6                                                        N/A
Domain Name                                                     N/A
Server Name                                                     N/A
Server IP                                                       N/A
Antenna gain for 802.11a                                        N/A
Antenna gain for 802.11g                                        N/A
Use external antenna                                            No
Antenna for 802.11a                                             both
Antenna for 802.11g                                             both
PKCS12 PASSPHRASE                                               N/A
Single chain mode for Radio 0                                   0
Single chain mode for Radio 1                                   0
External antenna polarization for 5GHz Radio                    0
External antenna polarization for 2.4GHz Radio                  0
TrustAnchor                                                     N/A
IKE PSK                                                         N/A
ikepsk-hex-based                                                No
PAP User Name                                                   N/A
PAP Password                                                    N/A
PPPOE User Name                                                 N/A
PPPOE Password                                                  N/A
PPPOE Service Name                                              N/A
PPPOE CHAP Secret                                               N/A
USB User Name                                                   N/A
USB Password                                                    N/A
USB Device Type                                                 none
USB CSR-Key Storage                                             No
```

```
USB Device Identifier                                                N/A
USB Dial String                                                      N/A
USB Initialization String                                            N/A
USB TTY device data path                                             N/A
USB TTY device control path                                          N/A
USB modeswitch parameters                                            N/A
Uplink VLAN                                                          0
Remote AP                                                            No
OCSP Default                                                         N/A
certificate DN                                                       N/A
Link Priority Ethernet                                               0
Link Priority Cellular                                               0
Cellular modem network preference                                    auto
USB power mode                                                       auto
AP POE Power optimization                                            false
AP2xx prestandard POE detection                                      Disabled
Mesh Role                                                            none
Installation                                                         default
Latitude                                                             N/A
Longitude                                                            N/A
Altitude                                                             N/A
Antenna bearing for 802.11a                                          N/A
Antenna bearing for 802.11g                                          N/A
Antenna tilt angle for 802.11a                                       N/A
Antenna tilt angle for 802.11g                                       N/A
Username of AP so that AP can authenticate to 802.1x using PEAP      N/A
Password of AP so that AP can authenticate to 802.1x using PEAP      N/A
Enable AP to 802.1x using EAP-TLS                                    Disabled
Enable AP to use factory certificates when doing 802.1x EAP-TLS      Disabled
Mesh SAE                                                             sae-disable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show rap-wml

```
show rap-wml [cache <server-name> | servers | wired-mac <bssid>]
```

Description

Displays the name and attributes of a MySQL database or a MySQL server.

Syntax

Parameter	Description
`cache <server-name>`	Displays the cache of all look-ups for a database server.
`servers`	Displays the database server state.
`wired-mac <bssid>`	Displays the wired MAC discovered on traffic through the AP.

Example

The output of this command shows status of all database servers.

```
(host) [mynode] #show rap-wml servers

WML DB Servers
--------------
name  ip  type  user  password  db-name  cache  ageout(sec)  in-service
----  --  ----  ----  --------  -------  -----  -----------  ----------
WML DB Tables
-------------
server  db  table  column  timestamp-column  lookup-time(sec)  delimiter  query-count
------  --  -----  ------  ----------------  ----------------  ---------  -----------
Mesh SAE                        sae-default
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on the Mobility Master

show references aaa alias-group

```
show references aaa
   alias-group <ag_name>
   [page <page>] [start <start>]
```

Description

Shows AAA profile references to an alias group.

Syntax

Parameter	Description
`alias-group <ag_name>`	Shows the references to an Alias group.
`page <page>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <start>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Use this command to show the references to an alias group.

```
(host)[mynode] #show references aaa alias-group alias1
```

Related Commands

Command	Description
aaa alias-group	Configures an AAA alias with set of VLAN derivation rules that could speed up user rule derivation processing for deployments with a very large number of user derivation rules.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa authentication

```
show references aaa authentication
   captive-portal {default | <profile-name>}
   dot1x {default | <profile-name>}
   mac {default | <profile-name>}
   mgmt
   stateful-dot1x
   stateful-kerberos {default | <profile-name>}
   stateful-ntlm {default | <profile-name>}
   via
      auth-profile {default | <profile-name>}
      connection-profile {default | <profile-name>}
      global-config
      web-auth <default>
   vpn {default | <profile-name>}
   wired
   wispr {default | <profile-name>}
   [page <page>] [start <start>]
```

Description

This command shows AAA profile references.

Syntax

Parameter	Description	Default
`captive-portal <profile-name>`	Shows the number of references to a captive-portal profile.	default
`dot1x <profile-name>`	Shows the number of references to a 802.1X authentication profile.	default
`mac <profile-name>`	Shows the number of references to a MAC authentication profile.	default
`mgmt`	Shows the number of references to a management authentication profile.	
`stateful-dot1x <profile-name>`	Shows the number of references to the stateful 802.1X authentication profile.	default
`stateful-kerberos <profile-name>`	Shows references to a Stateful Kerberos authentication profile.	default
`stateful-ntlm <profile-name>`	Shows the number of references to the specified stateful NTLM authentication profile.	default

Parameter	Description	Default
via	Shows the number of references to VIA.	
auth-profile <profile-name>}	Shows references to a VIA authentication profile.	default
connection-profile <profile-name>	Shows references to a VIA connection profile.	default
global-config	Shows references to the VIA global configuration.	
web-auth <default>	Shows references to a VIA web authentication.	default
vpn <profile-name>	Shows the number of references to VPN authentication.	default
wired	Shows the number of references to wired authentication.	
wispr <profile-name>	Shows the number of references to the specified WISPr authentication profile.	default
page <page>	Include this optional parameter to limit output of this command to the specified number of items.	
start <start>	Include this optional parameter to start displaying the output of this command at the specified index number.	

Example

Use this command to show where a specified AAA profile has been applied. The output of the example shown here indicates that the aaa profile **default-dot1x** contains a single reference to the 802.1X authentication profile **default**.

```
(host)[mynode] #show references aaa authentication dot1x default

References to 802.1X Authentication Profile "default"
-----------------------------------------------------
Referrer                                          Count
--------                                          -----
aaa profile "default-dot1x" authentication-dot1x  1
Total References:1
```

Related Commands

Command	Description
aaa authentication captive-portal	Configures a Captive Portal authentication profile.
aaa authentication dot1x	Configures the 802.1X authentication profile.
aaa authentication mac	Configures the MAC authentication profile.
aaa authentication mgmt	Configures authentication for administrative users.
aaa authentication stateful-dot1x	Configures 802.1X authentication for clients on non-Aruba APs.
aaa authentication stateful-kerberos	Configures stateful Kerberos authentication.
aaa authentication stateful-ntlm	Configures stateful NT LAN Manager (NTLM) authentication.
aaa authentication via auth-profile	Configures the VIA authentication profile.
aaa authentication via connection-profile	Configures the VIA connection profile.
aaa authentication via global-config	Allows you to enable SSL fallback mode.
aaa authentication via web-auth	Creates a VIA web authentication profile.
aaa authentication vpn	This command configures VPN authentication settings.
aaa authentication wired	Configures authentication for a client device that is directly connected to a port on the managed device.
aaa authentication wispr	Configures WISPr authentication with WISPr RADIUS server of an ISP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa authentication-server

```
show references aaa authentication-server
   ldap <ldap_server_name>
   radius <rad_server_name>
   tacacs <tacacs_server_name>
   windows <windows_server_name>
   [page <page>] [start <start>]
```

Description

This command displays information about AAA authentication servers.

Syntax

Parameter	Description
`ldap <ldap-server-name>`	Show the number of server groups that include references to the specified LDAP server.
`radius <rad_server_name>`	Show the number of server groups that include references to the specified RADIUS server.
`tacacs <tacacs_server_name>`	Show the number of server groups that include references to the specified TACACS server.
`windows <windows_server_name>`	Show the number of server groups that include references to the specified Windows server.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to show the AAA server groups that include references to the specified server. The example below shows that two server groups, **default** and **rad,** each include a single reference to the RADIUS server **rad01**.

```
(host)[mynode] #show references aaa authentication-server radius rad01

References to RADIUS Server "rad01"
-----------------------------------
Referrer                                Count
--------                                -----
aaa server-group "default" server_group  1
aaa server-group "rad" server_group      1
Total References:2
```

Related Commands

Command	Description
aaa authentication-server ldap	Configures an LDAP server.
aaa authentication-server radius	Configures a RADIUS server.
aaa authentication-server tacacs	Configures a TACACS+ server.
aaa authentication-server windows	Configures a windows server for stateful-NTLM authentication.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa password-policy

```
show references aaa password-policy mgmt
```

Description

This command shows the password policy for locally configured management users.

Syntax

Parameter	Description
`mgmt`	Shows references to the Management Password Policy.

Example

Execute the following command to show the password policy for locally configured management users.

```
(host)[mynode] #show references aaa password-policy mgmt
```

Related Commands

Command	Description
aaa password-policy mgmt	Defines a policy for creating management user passwords.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa profile

```
show references aaa profile <profile-name>
```

Description

This command shows references to an AAA Profile.

Syntax

Parameter	Description
`profile <profile-name>`	Name of an AAA profile for which you want to view references.

Example

Issue this command to show the wlan virtual AP profiles that include references to the specified AAA profile. The example below shows that seven different virtual AP profiles include a single reference to the AAA profile **default**.

```
(host)[mynode] #References to AAA Profile "default"
-----------------------------------
Referrer                                                Count
--------                                                -----
wlan virtual-ap "1.0.0_corporateHQ-wpa2" aaa-profile    1
wlan virtual-ap "110.0.corporateHQ-wpa2" aaa-profile    1
wlan virtual-ap "default" aaa-profile                   1
wlan virtual-ap "corporateHQ-vocera" aaa-profile        1
wlan virtual-ap "corporateHQ-voip-wpa2" aaa-profile     1
wlan virtual-ap "Test123" aaa-profile                   1
wlan virtual-ap "branch12" aaa-profile                  1
Total References:7
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa radius

```
show references aaa
   radius modifier <rad_modifier_name>
   [page <page>] [start <start>]
```

Description

This command shows information about the configuration profiles that reference a specific RADIUS modifier profile.

Syntax

Parameter	Description
`radius modifier <rad_modifier_name>`	Shows references to a RADIUS modifier profile.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number

Example

The following is an example to execute the **show references aaa radius modifier** command:

```
(host) [mynode] #show references aaa radius modifier RADIUSProfile1
```

Related Commands

Command	Description
aaa radius modifier	Configures the RADIUS modifier profile to customize the attributes that are included, excluded, and modified in the RADIUS request before it is sent to the authentication server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa radius-attributes

```
show references aaa
   radius-attributes <node-path>
```

Description

This command shows information about the configuration profiles that reference a specific RADIUS modifier profile.

Syntax

Parameter	Description
`radius-attributes`	Displays references to RADIUS attributes.
`<node-path>`	Displays the path of the configuration node.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following is an example to execute the **show references aaa radius-attributes** command:

```
(host) [mynode] #show references aaa radius-attributes HW-Cluster-1
```

Related Commands

Command	Description
aaa radius-attributes	Configures the RADIUS attributes to statically configure values to be included in RADIUS Access- Requests and Accounting-Requests.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa rfc-3576-server

```
show references aaa
   rfc-3576-server <server_ip>
   [page <page>] [start <start>]
```

Description

This command shows information about the configuration profiles that reference a specific RFC 3576 server.

Syntax

Parameter	Description
`rfc-3576-server <server_ip>`	IP address of an RFC-3576 server.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number

Example

This first example shows that the **default** AAA profile and the AirGroup ClearPass Policy Manager-server AAA profile reference an RFC 3567 Server with the IP address 10.1.1.41.

```
(host)[mynode] #show references aaa rfc-3576-server 10.1.1.41
References to RFC 3576 Server "10.1.1.41"
-----------------------------------------
Referrer                                  Count
--------                                  -----
aaa profile "default" rfc-3576-server     1
airgroup cppm-server aaa rfc-3576-server  1
Total References:2
```

Related Commands

Command	Description
aaa rfc-3576-server	Define RFC 3576 server profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa server-group

```
show references aaa server-group
   <sg_name>
   [page <page>][start <start>]
```

Description

This command shows references to a server group.

Syntax

Parameter	Description
`<sg_name>`	Name of the server group for which you want to show references
`page <number>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to display a list of AAA profiles that include references to the specified server group.

```
(host)[mynode] #show references aaa server-group default

References to Server Group "default"
-----------------------------------
Referrer                                                Count
--------                                                -----
aaa profile "aircorp-office-ssid" mac-server-group      1
aaa profile "amigopod-guest" mac-server-group           1
aaa profile "default" mac-server-group                  1
aaa profile "default-airwave-office" mac-server-group   1
aaa profile "defaultcorporate" mac-server-group         1
aaa profile "defaultcorporate-no-okc" mac-server-group  1
aaa profile "defaultcorporate-okc" mac-server-group     1
aaa profile "default-dot1x" mac-server-group            1
aaa profile "default-India" mac-server-group            1
aaa profile "default-india-hotel" mac-server-group      1
aaa profile "default-India-split" mac-server-group      1
aaa profile "voip-psk" mac-server-group                 1
aaa profile "default-dot1x-psk" mac-server-group        1
aaa profile "default-mac-auth" mac-server-group         1
aaa profile "default-open" mac-server-group             1
aaa profile "default-xml-api" mac-server-group          1
Total References:16
```

Related Commands

Command	Description
aaa server-group	Allows you to add a configured authentication server to an ordered list in a server group, and configure server rules to derive a user role, VLAN ID or VLAN name from attributes returned by the server during authentication.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aaa xml-api server

```
show references aaa
   xml-api server <server-id>
   [page <page>][start <start>]
```

Description

This command shows references to an XML API Server.

Syntax

Parameter	Description
`xml-api server <server-id>`	Shows references to an XML API Server. Specify the IP address of the XML-API server.
`page <number>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references to the specified AML-API server.

```
(host) [mynode] #show references aaa xml-api server 191.1.2.1
```

Related Commands

Command	Description
aaa xml-api	Configures an external XML API server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references activate

```
show references activate
   [page <page>] [start <start>]
```

Description

This command displays Activate service whitelist profile references.

Syntax

Parameter	Description
`activate`	Name of the activate profile for which you want to show references.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of profiles that include references to the activate profile.

```
(host) [mynode] #show references activate
References to activate
--------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Related Commands

Command	Description
activate	Synchronizes a managed device whitelist or remote AP whitelist on Mobility Master with the Activate whitelist database.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references airgroup

```
show references airgroup
   cppm-server aaa
   [page <page>] [start <start>]
```

Description

This command displays information about AAA authentication servers.

Syntax

Parameter	Description
`cppm-server`	Specifies the ClearPass Policy Server information.
`aaa`	Specifies the AAA parameters for AirGroup.
`page <page>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <start>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Use this command to show the AAA server groups that include references to the AirGroup.

```
(host)[mynode] #show reference airgroup
References to Airgroup AAA profile
----------------------------------
Referrer  Count
--------  -----
Total References:0
```

Related Commands

Command	Description
airgroup	configures AirGroup settings.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references airgroupprofile

```
show references airgroupprofile
   activate
   cppm <airgroup-cppm-name>
   domain <airgroup-domain-name>
   ipv6 <ipv6-profile-name>
   service <service-name>
   [page <page>] [start <start>]
```

Description

This command shows the references to the AirGroup profile information.

Syntax

Parameter	Description
`activate`	Displays references to the active AirGroup profile.
`cppm <airgroup-cppm-name>`	Displays references to the AirGroup ClearPass Policy Manager profile.
`domain <airgroup-domain-name>`	Displays references to an AirGroup domain profile.
`ipv6 <ipv6-profile-name>`	Displays references to the AirGroup IPv6 profile.
`service <service-name>`	Displays references to the AirGroup service profile. By default, the following services are available: ■ default-airplay ■ default-airprint ■ default-allowall ■ default-amazontv ■ default-dial ■ default-dlna-media ■ default-dlna-print ■ default-googlecast ■ default-itunes ■ default-remotemgmt ■ default-sharing
`<profile-name>`	Configures an AirGroup profile.
`page <page>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <start>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

Use this command to show the AirGroup domain profiles.

```
(host)[mynode] ##show references airgroupprofile cppm test
```

Related Commands

Command	Description
airgroupprofile	Configures AirGroup profile settings.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references airmatch

```
show references airmatch
   profile
   [page <page>] [start <start>]
```

Description

The show references profile command displays profile references. No other profiles reference the AirMatch profile, so the output of this always displays a reference count of 0.

Syntax

Parameter	Description
`profile`	Shows references to the AirMatch profile
`page <page>`	Include this parameter to limit output of the **show references** command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of the **show references** command at the specified index number.

Example

The **show references <profile>** command displays a list of profiles that include references to the selected profile. No other profiles reference the AirMatch profile, so this table always displays a reference count of 0.

```
(host) [mynode] #show references airmatch profile
References to AirMatch
---------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Related Commands

Related Command	Description
airmatch profile	Configures the AirMatch profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references ap

```
show references ap
   am-filter-profile {default | <profile-name>}
   authorization-profile {default | <profile-name>}
   deploy-profile {page | start}
   enet-link-profile {default | <profile-name>}
   general-profile
   lldp
      med-network-policy-profile
      {default | <profile-name>}
      profile
   mesh-cluster-profile {default | <profile-name>}
   mesh-ht-ssid-profile {default | <profile-name>}
   mesh-radio-profile {default | <profile-name>}
   multizone-profile {default | <profile-name>}
   provisioning-profile {default | <profile-name>}
   regulatory-domain-profile {default | <profile-name>}
   spectrum local-overridead
   system-profile {default | <profile-name>}
   wired-ap-profile {default | <profile-name>}
   wired-port-profile
   [page <page>] [start <start>]
```

Description

This command shows the number of references to a specific AP profile.

Syntax

Parameter	Description	Default
`am-filter-profile <profile-name>`	Shows references to an AM filter.	default
`authorization-profile <profile-name>`	Shows references to an AP Authorization profile.	default
`deploy-profile`	Show references to the AP deploy-profile.	
`enet-link-profile <profile-name>`	Shows AP groups that include a references to this Ethernet link profile.	default
`general-profile`	Shows references to the ap general-profile.	
`lldp`	Shows references to the Link-layer Discovery Protocol profile.	
`med-network-policy-profile <profile-name>`	Shows references to LLDP-MED Network Policy profile of an AP.	
`profile`	Shows references to an AP LLDP profile.	
`mesh-cluster-profile <profile-name>`	Shows AP groups that include a references to this mesh cluster profile.	default

Parameter	Description	Default
`mesh-ht-ssid-profile <profile-name>`	Shows AP groups that include a references to this mesh high-throughput SSID profile.	default
`mesh-radio-profile <profile-name>`	Shows AP groups that include a references to this mesh radio profile.	default
`multizone <profile-name>`	Shows references to an AP multizone profile.	default
`provisioning-profile <profile-name>`	Shows references to a Provisioning profile.	default
`regulatory-domain-profile <profile-name>`	Shows AP groups that include a references to this regulatory domain profile.	default
`spectrum local-override`	Shows references to the Spectrum Local Override Profile.	
`system-profile <profile-name>`	Shows AP groups that include a references to this system profile.	default
`wired-ap-profile <profile-name>`	Shows AP groups that include a references to this wired AP profile.	default
`wired-port-profile <profile-name>`	Shows references to an AP wired port profile	default
`page <page>`	Include this optional parameter to limit output of this command to the specified number of items.	
`start <start>`	Include this optional parameter to start displaying the output of this command at the specified index number.	

Example

The example below shows that 10 different AP groups include links to the AP Ethernet link profile **Default**. These 10 AP groups reference the **Default** Ethernet link profile for both their Ethernet 0 and Ethernet 1 interfaces, for a total of 20 references altogether.

```
(host)[mynode] #show references ap enet-link-profile default

References to AP Ethernet Link profile "default"
------------------------------------------------
Referrer                                    Count
--------                                    -----
ap-group "10.0.0" enet0-profile             1
ap-group "10.0.0" enet1-profile             1
ap-group "corp" enet0-profile               1
ap-group "corp" enet1-profile               1
ap-group "Corp_AM_Ch1" enet0-profile        1
ap-group "Corp_AM_Ch1" enet1-profile        1
ap-group "Corp_AM_Ch6" enet0-profile        1
ap-group "Corp_AM_Ch6" enet1-profile        1
ap-group "corpTest" enet0-profile           1
ap-group "corpTest" enet1-profile           1
ap-group "default" enet0-profile            1
ap-group "default" enet1-profile            1
ap-group "India_Local" enet0-profile        1
```

```
ap-group "India_Local" enet1-profile        1
ap-group "ops" enet0-profile                1
ap-group "ops" enet1-profile                1
ap-group "voip-test" enet0-profile          1
ap-group "voip-test" enet1-profile          1
ap-group "voip-test-nokia" enet0-profile    1
ap-group "voip-test-nokia" enet1-profile    1
Total References:20
```

Related Commands

Command	Description
ap am-filter-profile	Configures an AM filter.
ap authorization-profile	Defines a temporary configuration profile for remote APs that are not yet authorized on the network.
ap deploy-profile	Configures an AP deployment profile.
ap enet-link-profile	Configures an AP Ethernet link profile.
ap general-profile	Configures the general profile of an AP.
ap lldp profile	Defines an LLDP profile that specifies the type-length-value (TLV) elements to be sent in LLDP PDUs.
ap lldp med-network-policy-profile	Defines an LLDP MED network policy profile that defines DSCP values and L2 priority levels for a voice or video application.
ap mesh-cluster-profile	Configures a mesh cluster profile used by mesh nodes.
ap mesh-ht-ssid-profile	Configures a mesh high-throughput SSID profile used by mesh nodes.
ap mesh-radio-profile	Configures a mesh radio profile used by mesh nodes.
ap multizone-profile	Attaches the profile to ap-group or ap-name.
ap provisioning-profile	Defines a provisioning profile for an AP or group of APs.
ap regulatory-domain-profile	Configures an AP regulatory domain profile.
ap spectrum local-override	Converts an AP or AM into a spectrum monitor by adding it to the spectrum local-override list.
ap system-profile	Configures an AP system profile.
ap wired-ap-profile	Configures a wired AP profile.
ap wired-port-profile	Configures a wired port profile.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ap deploy-profile** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ap-group

```
show references
   ap-group {default | <profile-name>}
   [page <page>] [start <start>]
```

Description

This command shows the number of references to a specific AP-group profile.

Syntax

Parameter	Description	Default
`ap-group <profile-name>`	Shows references to an AP-group profile.	default

Example

The following is an example for execution of the **show references ap-group** command:

```
(host) [mynode] #show references ap-group LeftWing
```

Related Commands

Command	Description
ap-group	Configures an AP group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ap-lacp-striping-ip

```
show references
   ap-lacp-striping-ip
   [page <page>] [start <start>]
```

Description

This command shows the references to the AP LACP LMS map information.

Syntax

Parameter	Description
`ap-lacp-striping-ip`	Shows references to AP LACP LMS map information.

Example

The following is an example for execution of the **show references ap-lacp-striping-ip** command:

```
(host) [mynode] #show references ap-lacp-striping-ip
```

Related Commands

Command	Description
ap-lacp-striping-ip	Configures the AP LACP LMS map information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ap-name

```
show references
   ap-name <profile-name>
   [page <page>] [start <start>]
```

Description

This command shows the number of references to a specific AP-group profile.

Syntax

Parameter	Description
`ap-name <profile-name>`	Shows references to an AP name profile.

Example

The following is an example for execution of the **show references ap-name** command:

```
(host) [mynode] #show references ap-name ap228
```

Related Commands

Command	Description
ap-name	Configures a specific AP.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references aruba-central

```
show references
   aruba-central
   [page <page>] [start <start>]
```

Description

This command shows the number of references to Aruba-Central.

Syntax

Parameter	Description
`aruba-central`	Shows references to Aruba-Central.

Example

The following is an example for execution of the **show references aruba-central** command:

```
(host) [mynode] #show references aruba-central
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references bw-contract

```
show references
   bw-contract <name> [revert_cmd]
   [page <page>] [start <start>]
```

Description

This command shows the number of references to bandwidth contract.

Syntax

Parameter	Description
`bw-contract <name>`	Shows references to bandwidth contract. Specify the bandwidth contract name.
`[revert_cmd]`	List of no commands to change the value.

Example

The following is an example for execution of the **show references bw-contract** command:

```
(host) [mynode] #show references bw-contract bwcontract1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references control-plane-security

```
show references
   control-plane-security
   [page <page>] [start <start>]
```

Description

This command shows the number of references to bandwidth contract.

Syntax

Parameter	Description
`control-plane-security`	Shows references to the Control Plane Security Profile.

Example

The following is an example for execution of the **show references control-plane-security** command:

```
(host) [mynode] #show references control-plane-security
```

Related Commands

control-plane-security	Configures the control plane security profile by identifying APs to receive security certificates.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references est profile

```
show references
   est profile {default | <profile-name>}
   [page <page>] [start <start>]
```

Description

This command shows the number of references to bandwidth contract.

Syntax

Parameter	Description
`est profile <profile-name>`	Show references to an EST Profile.

Example

The following is an example for execution of the **show references est profile** command:

```
(host) [mynode] #show references est profile default
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references file syncing profile

```
show references
   file syncing profile
   [page <page>] [start <start>]
```

Description

This command shows references to the file syncing profile.

Syntax

Parameter	Description
`file syncing profile`	Shows references to the file syncing profile.

Example

The following is an example for execution of the **show references file syncing profile** command:

```
(host) [mynode] #show references file syncing profile
```

Related Commands

Command	Description
file syncing profile	Allows the user to configure the file syncing profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references guest-access-email

```
show references
   guest-access-email
   [page <page>] [start <start>]
```

Description

This command shows references to the global guest access email profile.

Syntax

Parameter	Description
`guest-access-email`	Shows references to the guest-access email profile.
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode]#show references guest-access-email

References to Guest-access Email Profile
----------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Related Commands

Command	Description
guest-access-email	Configures the SMTP server which is used to send guest email.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ha

```
show references
   ha group-profile <profile-name>
   [page <page>] [start <start>]
```

Description

This command displays HA group profile references.

Syntax

Parameter	Description
`group-profile <profile-anme>`	Name of the HA group profile for which you want to show references.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <page>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for a specific HA group profile.

```
(host)[mynode](config) #show references ha group-profile newgroup
References to HA group information "newgroup"
-----------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Related Commands

Command	Description
ha	Creates a new high availability group, or define settings for an existing group.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ids

```
show references ids
   ap-classification-rule <rule-name>
   ap-rule-matching
   dos-profile {default | <profile-name>}
   general-profile {default | <profile-name>}
   impersonation-profile {default | <profile-name>}
   management-profile
   profile {default | <profile-name>}
   rap-wml-server-profile <server-name>
   rap-wml-table-profile <table-name>
   rate-thresholds-profile {default | <profile-name>}
   signature-matching-profile {default | <profile-name>}
   signature-profile <profile-name>
   unauthorized-device-profile {default | <profile-name>}
   wms-general-profile
   wms-local-system-profile
```

Description

This command displays IDS profile references.

Syntax

Parameter	Description	Default
`ap-classification-rule <rule-name>`	Shows references to an IDS AP classification rule profile.	
`ap-rule-matching`	Shows references to the IDS Active AP Rules Profile.	
`dos-profile <profile-name>`	Shows references to an IDS Denial of Service (DoS) profile.	default
`general-profile <profile-name>`	Shows references to an IDS general profile.	default
`impersonation-profile <profile-name>`	Shows references to an IDS impersonation profile.	default
`management-profile`	Shows references to the IDS WMS management profile.	
`profile <profile-name>`	Shows references to an IDS profile.	default
`rap-wml-server-profile <server-name>`	Shows references to an IDS remote AP WML server profile.	

Parameter	Description	Default
rap-wml-table-profile <table-name>	Shows references to an IDS remote AP WML table profile	
rate-thresholds-profile <profile-name>	Shows references to an IDS rate thresholds profile.	default
signature-matching-profile <profile-name>	Shows references to an IDS signature matching profile.	default
signature-profile <profile-name>	Shows references to an IDS signature profile.	default
unauthorized-device-profile <profile-name>	Shows references to an unauthorized device profile.	default
wms-general-profile	Shows references to the IDS WMS general profile.	
wms-local-system-profile	Shows references to the IDS WMS local system profile.	

Example

Execute the following command to display a list of references for the default IDS profile.

```
(host) [mynode] #show references ids profile default
References to IDS Profile "default"
-----------------------------------
Referrer                              Count
--------                              -----
ap-group "default" ids-profile        1
ap-group "NoAuthApGroup" ids-profile  1
Total References:2
```

Related Commands

Command	Description
ids ap-classification-rule	Configures the IDS AP classification rule profile.
ids ap-rule-matching	Configures the IDS active AP rules profile by enabling an AP classification rule.
ids dos-profile	Configures traffic anomalies for denial of service (DoS) attacks.
ids general-profile	Configures an IDS general profile.
ids impersonation-profile	Configures anomalies for impersonation attacks.
ids management-profile	Configures the IDS WMS management profile.
ids profile	Defines a set of IDS profiles.

Command	Description
ids rate-thresholds-profile	Configures an IDS rate thresholds profile.
ids signature-matching-profile	Configures an IDS signature matching profile.
ids signature-profile	Configures signatures for wireless intrusion detection.
ids unauthorized-device-profile	Configures detection of unauthorized devices, as well as rogue AP detection and containment.
ids wms-general-profile	configures the IDS WLAN management system (WMS) general profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ifmap cppm

```
show references
   ifmap cppm
   [page <page>] [start <start>]
```

Description

This command displays the ClearPass Policy Manager IF-MAP references.

Syntax

Parameter	Description
`ifmap cppm`	Shows references to the ClearPass Policy Manager IF-MAP profile.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the ClearPass Policy Manager IF-MAP profile.

```
(host) [mynode] #show references ifmap cppm
References to CPPM IF-MAP Profile
---------------------------------
Referrer  Count
--------  -----
Total References:0
```

Related Commands

Command	Description
ifmap	Sends HTTP User Agent Strings and mDNS broadcast information to ClearPass Policy Manager so that it can make more accurate decisions about what types of devices are connecting to the network.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master

show references ip-flow-export-profile

```
show references
   ip-flow-export-profile
   [page <page>] [start <start>]
```

Description

This command shows references to the IP flow collector Profile.

Syntax

Parameter	Description
`ip-flow-export-profile`	Shows references to the IP flow collector profile.
`page <page>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <start>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the IP flow export profile:

```
(host) [mynode] #show references ip-flow-export-profile
```

Related Commands

Command	Description
ip-flow-export-profile	Configures the IP flow collector profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references lc-cluster

```
show references lc-cluster group-profile <profile-name> {page<page> start<start>}
```

Description

Displays Controller Cluster Profile references.

Syntax

Parameter	Description
`group-profile <profile-anme>`	Name of the lc-cluster group profile for which you want to show references.
`page <number>`	Include this parameter to limit output of this command to the specified number of items.
`start <number>`	Include this parameter to start displaying the output of this command at the specified index number.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Managed device

show references license-pool-profile

```
show references
   license-pool-profile
   [page <page>] [start <start>]
```

Description

This command displays references to a License pool profile.

Syntax

Parameter	Description
`license-pool-profile`	Shows references to the license-pool profile.
`page <page>`	Include this parameter to limit output of this command to the specified number of items.
`start <start>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Execute this command to display a list of references for the license-pool profile.

```
(host)[node] #show references license-pool-profile
```

Related Commands

Related Command	Description
license-pool-profile	Creates a local licensing pool and allocate licenses for that licensing pool.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Master.

show references mgmt-server profile

```
show references mgmt-server profile <profile_name>
```

Description

Shows the management server configuration profiles.

Syntax

Parameter	Description
`mgmt-server profile`	Specifies the management profile name.
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode] #show references mgmt-server profile default
References to Mgmt Config profile "default"
-------------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show references papi-security

```
show references papi-security [page <number>] [start <number>]
```

Description

Show references to a PAPI security profile.

Syntax

Parameter	Description
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
            (host)[node]#show references papi-security

References to PAPI Security Profile
-----------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show references rf

```
show references rf
   dot11a-radio-profile <profile-name>
   dot11g-radio-profile <profile-name>
   event-thresholds-prof <profile-name>
   ht-radio-profile <profile-name>
   optimization-profile <profile-name>
```

Description

Show RF profile references.

Syntax

Parameter	Description
`dot11a-radio-profile`	Show references to a 802.11a radio profile
`dot11g-radio-profile`	Show references to a 802.11g radio profile
`event-thresholds-prof`	Show references to an RF Event Thresholds Profile
`ht-radio-profile`	Show references to a High-throughput radio profile
`optimization-profile`	Show references to an RF Optimization Profile

Command History

	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references ucc

```
show references ucc
   facetime
   h323
   ich
   jabber
   noe
   rtpa-config
   sccp
   session-idle-timeout
   sip
   skype4b
   vocera
   wificalling
      page <page>
      start <start>
```

Description

This command displays the UCC ALG references to a profile.

Syntax

Parameter	Description
`facetime`	Show references to the Apple FaceTime ALG configuration.
`h323`	Show references to the H.323 ALG configuration.
`ich`	Show references to the Intelligent Call Handling configuration.
`jabber`	Show references to the Cisco Jabber ALG configuration.
`noe`	Show references to the Alcatel-Lucent New Office Environment (NOE) ALG configuration.
`rtpa-config`	Show references to the Real-Time Analysis configuration.
`sccp`	Show references to the Cisco SCCP ALG configuration.
`session-idle-timeout`	Show references to the UCC Session Idle Timeout configuration.
`sip`	Show references to the SIP ALG configuration.
`skype4b`	Show references to the Microsoft Skype for Business ALG configuration.
`vocera`	Show references to the Vocera ALG configuration.
`wificalling`	Show references to the Wi-Fi Calling configuration.
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode]#show references u skype4b

References to Skype4B ALG Configuration
---------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master

show references upgrade-profile

```
crypto-local
show references upgrade-profile {page<page> start<start>}
```

Description

Displays the upgrade profile references.

Syntax

Parameter	Description
`upgrade-profile`	Shows references to the upgrade profile.
`page <number>`	Include this parameter to limit output of this command to the specified number of items.
`start <number>`	Include this parameter to start displaying the output of this command at the specified index number.

Example

Issue this command to display a list of references for the upgrade profile.

```
(host)[mynode]#show references upgrade-profile
References to Upgrade Profile
-----------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show references user-role

```
show references user-role <role_name>
```

Description

Show access rights for user role.

Syntax

Parameter	Description
<role_name>	The role name assigned to a user.

Example

```
(host)[mynode] #show references user-role guest

References to User Role "guest"
-------------------------------
aaa profile "airwave-office-ssid" mac-default-role
aaa profile "amigopod-guest" mac-default-role
aaa profile "corp1344-voip" mac-default-role
aaa profile "default" mac-default-role
aaa profile "default-airwave-office" mac-default-role
aaa profile "default-corp1344" mac-default-role
aaa profile "default-corp1344-no-okc" mac-default-role
aaa profile "default-corp1344-okc" mac-default-role
aaa profile "default-dot1x" mac-default-role
aaa profile "default-dot1x-psk" mac-default-role
aaa profile "default-dot1x-psk" dot1x-default-role
aaa profile "default-India" mac-default-role
aaa profile "default-india-hotel" mac-default-role
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references web-server

```
show references web-server [page <number>] [start <number>]
```

Description

Show the Web server configuration references.

Syntax

Parameter	Description
`page <number>`	Include this optional parameter to limit output of this command to the specified number of items.
`start <number>`	Include this optional parameter to start displaying the output of this command at the specified index number.

Example

```
(host)[mynode]#show references web-server

References to Web Server Configuration
--------------------------------------
Referrer  Count
--------  -----
Total References:0
```

Command History

	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show references wlan

```
show references wlan
   bcn-rpt-req-profile
   client-wlan-profile
   dot11k-profile <profile-name>
   dot11r-profile <profile-name>
   edca-parameters-profile <profile-name>
   hotspot
      advertisement-profile
      anqp-3gpp-nwk-profile <profile-name>
      anqp-domain-name-profile <profile-name>
      anqp-ip-addr-avail-profile <profile-name>
      anqp-nai-realm-profile <profile-name>
      anqp-nwk-auth-profile <profile-name>
      anqp-roam-cons-profile <profile-name>
      anqp-venue-name-profile <profile-name>
      h2qp-conn-capability-profile <profile-name>
      h2qp-op-cl-profile <profile-name>
      h2qp-operator-friendly-name-profile <profile-name>
      h2qp-wan-metrics-profile <profile-name>
      hs2-profile <profile-name>
   ht-ssid-profile
   rrm-ie-profile
   ssid-profile <profile-name>
   traffic-management-pr <profile-name>
   tsm-req-profile
   virtual-ap <profile-name>
   wmm-traffic-management
```

Description

Show information about the different configuration profiles that reference a specific WLAN profile.

Syntax

Parameter	Description
`bcn-rpt-req-profile`	Shows references to a Beacon Report Request profile.
`client-wlan-profile`	Shows references for the Client WLAN profile.
`dot11k-profile <profile-name>`	Shows references to a 802.11k profile.
`dot11r-profile <profile-name>`	Shows references to a 802.11r profile.
`edca-parameters-profile <profile-name>`	Shows references to an EDCA parameters profile.

Parameter	Description
hotspot	Shows references to one of the following hotspot profile types: ■ advertisement-profile ■ anqp-3gpp-nwk-profile ■ anqp-domain-name-profile ■ anqp-ip-addr-avail-profile ■ anqp-nai-realm-profile ■ anqp-nwk-auth-profile ■ anqp-roam-cons-profile ■ anqp-venue-name-profile ■ h2qp-conn-capability-profile ■ h2qp-op-cl-profile ■ h2qp-operator-friendly-name-profile ■ h2qp-wan-metrics-profile ■ hs2-profile
ht-ssid-profile <profile-name>	Shows references to a high-throughput SSID profile.
rrm-ie-profile	Shows references to an RRM IE profile.
ssid-profile <profile-name>	Shows references to an SSID management profile.
traffic-management-pr <profile-name>	Shows references to a traffic management profile.
virtual-ap <profile-name>	Shows references to a virtual AP profile.
tsm-req-profile	Show references to a TSM Report Request profile.
wmm-traffic-management	Shows references to a WMM Traffic management profile.

Example

The following example shows that two different WLAN hotspot 2.0 profiles reference the **default** WLAN hotspot advertisement profile.

```
(host) [mynode] #show references wlan hotspot advertisement-profile default

References to Advertisement Profile "default"
---------------------------------------------
Referrer                                                    Count
--------                                                    -----
wlan hotspot hs2-profile "deploytest" advertisement-profile  1
wlan hotspot hs2-profile "default" advertisement-profile     1

Total References:2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rf am-scan-profile

```
show rf am-scan-profile [<profile-name>]
```

Description

Display the AM scanning profile list. Optionally display parameter and values of a specified Air Monitor profile.

Syntax

Parameter	Description
<profile-name>	Name of this instance of the profile.

Usage Guidelines

Enter the basic show command to view a list of profiles, the number of profiles and the profile status. For example:

```
(host) [mynode]#show rf am-scan-profile

AM Scanning profile List
------------------------
Name      References  Profile Status
----      ----------  --------------
default   9
north     0

Total:2
```

Example

In the example above, their are two profile names; default and north. The Reference column indicates the number of references to this profile name. The Profile Status column is blank unless the profile is predefined.

Optionally, you can enter a profile name to view the parameters for that profile. For example:

```
(host) [mynode]#show rf am-scan-profile default

AM Scanning profile "default"
-----------------------------
Parameter                                 Value
---------                                 -----
Scan Mode                                 all-reg-domain
Dwell time: Active channels               500
Dwell time: Regulatory Domain channels    250
Dwell time: non-Regulatory Domain channels  200
Dwell time: Rare channels                 100
```

The explanation of the display output is described in the table below.

Parameter	Description
Scan-mode	The scanning mode for the radio
all-reg-domain	Scan channels in all regulatory domain

Parameter	Description
rare	Scan all channels (all regulatory domains and rare channels)
reg-domain	Scan channels in the APs regulatory domain
Dwell time: Active channels	Dwell time (in ms) for channels where there is wireless activity
Dwell time: Regulatory Domain channels	Dwell time (in ms) for AP's Regulatory domain channels
Dwell time: non-Regulatory Domain channels	Dwell time (in ms) for channels not in the APs regulatory domain
Dwell time: Rare channels	Dwell time (in ms) for rare channels

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Requires RFProtect license.	Config mode on Mobility Master

show rf arm-rf-domain-profile

```
show rf arm-rf-domain profile
```

Description

This profile contains a non-editable key defined by Mobility Master, and used to sign over-the air (OTA) ARM updates exchanged between APs.

Syntax

No parameters

Example

The output of this command displays the OTA key defined by Mobility Master.

```
(host)[mynode] #show rf arm-rf-domain-profile

ARM RF domain
-------------
Parameter          Value
---------          -----
ARM RF domain key  27f71ad66f28c374a8904b4a82177e2c
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rf arm-profile

```
show rf arm-profile [<profile>]
```

Description

Show an ARM profile.

Syntax

Parameter	Description
<profile>	Name of an ARM profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire ARM profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured ARM profiles. The **References** column lists the number of other profiles with references to the ARM profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[node] # show rf arm-profile
Adaptive Radio Management (ARM) profile List
-------------------------------------------
Name                    References  Profile Status
----                    ----------  --------------
airwave                 2
default                 4
default-AP85            2
no-scanning             1
Wireless-rf-profile                     1

Total:5.
```

This example displays the configuration settings for the profile **Wireless_rf_profile.**

```
(host)[node] #show rf arm-profile default
Adaptive Radio Management (ARM) profile "Wireless_rf_profile"
-------------------------------------------------------------------------------------------------------
----
Parameter                                                                        Value
---------                                                                        -----
Assignment                                                                       single-band
Allowed bands for 40MHz channels                                                 a-only
80MHz support                                                                    Enabled
160MHz-support                                                                   None
Client Aware                                                                     Enabled
Max Tx EIRP                                                                      127 dBm
Min Tx EIRP                                                                      9 dBm
Rogue AP Aware                                                                   Disabled
Scan Interval                                                                    10 sec
Aggressive scanning                                                              true
Active Scan                                                                      Disabled
ARM Over the Air Updates                                                         Enabled
```

```
Scanning                                                                    Enabled
Multi Band Scan                                                             Enabled
VoIP Aware Scan                                                             Enabled
Power Save Aware Scan                                                       Disabled
Video Aware Scan                                                            Enabled
Ideal Coverage Index                                                        10
Acceptable Coverage Index                                                   4
Free Channel Index                                                          25
Interfering AP Weight                                                       25 %
Backoff Time                                                                240 sec
Error Rate Threshold                                                        50 %
Error Rate Wait Time                                                        30 sec
Channel Quality Aware Arm                                                   Disabled
Channel Quality Threshold                                                   70 %
Channel Quality Wait Time                                                   120 sec
Minimum Scan Time                                                           8
Load aware Scan Threshold                                                   1250000 Bps
Mode Aware Arm                                                              Disabled
Scan Mode                                                                   all-reg-domain
Client Match                                                                Enabled
Client Match report interval (sec)                                          30
Allows Client Match to Automatically Clear Unsteerable Clients after Ageout Enabled
Client Match Unsteerable Client Ageout Interval                             2 Days 0 Hours
Client Match Band Steering G Max Signal (-dBm)                              45
Client Match Band Steering A Min Signal (-dBm)                              75
Client Match Sticky Client Check Interval (sec)                             3
Client Match Sticky Client Check SNR (dB)                                   25
Client Match SNR Delta Bound(dB)                                            10
Client Match Sticky Min Signal                                              70
Client Match Steering Timeout (sec)                                         10
Client Match Load Balancing Threshold (%)                                   20
Client Match IOS Steering Backoff Interval (sec)                            300
Client Match VBR Stale Entry Age (sec)                                      120
Client Match Max Steering Failures                                          2
Client Match Load Balancing Client Threshold                                10
Client Match Load Balancing SNR Threshold (dB)                              77
Client Match Load Balancing Signal Delta Bound (dB)                         5
Client Match 802.11v BSS Transition Management                              Enabled
Dynamic Bandwidth Switch                                                    Enabled
Dynamic Bandwidth Switch Wait Time (sec)                                    30
Dynamic Bandwidth Switch Triggering Indicator CCA ibss Threshold (%)        10
Dynamic Bandwidth Switch Triggering Indicator Beacon Failed Threshold       30
Dynamic Bandwidth Switch Triggering Indicator CCA intf Threshold (%)        30
Dynamic Bandwidth Switch Clear Time (min)                                   30
```

The output of this command includes the following parameters:

Parameter	Description
Assignment	Displays the current ARM channel/power assignment mode.
Allowed bands for 40MHz channels	Shows if 40 MHz mode of operation is allowed on the 5 GHz (802.11a) or 2.4 GHz (802.11b/g) frequency band only, on all frequency bands, or on neither frequency band.
Client Aware	Shows if the client aware feature is enabled or disabled. When enabled, the AP does not change channels when there are active clients.

Parameter	Description
Max Tx Power	The highest transmit power levels for the AP, from 0-30 dBm in 3 dBm increments. Higher power level settings may be constrained by local regulatory requirements and AP capabilities. In the event that an AP is configured for a Max Tx Power setting it cannot support, this value will be reduced to the highest supported power setting.
Min Tx Power	The lowest transmit power levels for the AP, from 0-30 dBm, in 3 dBm increments. Note that power settings will not change if the Assignment option is set to disabled or maintain.
Multi Band Scan	If enabled, single-radio APs will try to scan across bands for rogue AP detection.
Rogue AP Aware	If enabled, Aruba APs may change channels to contain off-channel rogue APs with active clients. This security features allows APs to change channels even if the Client Aware setting is disabled. This setting is disabled by default, and should only be enabled in high-security environments where security requirements are allowed to consume higher levels of network resources. You may prefer to receive Rogue AP alerts via SNMP traps or syslog events.
Scan Interval	If Scanning is enabled, the Scan Interval defines how often the AP will leave its current channel to scan other channels in the band. Off-channel scanning can impact client performance. Typically, the shorter the scan interval, the higher the impact on performance. If you are deploying a large number of new APs on the network, you may want to lower the Scan Interval to help those APs find their optimal settings more quickly. Raise the Scan Interval back to its default setting after the APs are functioning as desired.
Aggressive Scanning	When the aggressive scanning feature is enabled, an AP radio with no clients will scan channels every second.
Active Scan	If enabled, the AP initiates active scanning via probe request. This option elicits more information from nearby APs, but also creates additional management traffic on the network. Active Scan is disabled by default, and should not be enabled except under the direct supervision of Aruba Support.
Scanning	Shows if the AP has enabled or disabled AP scanning of other channels.
Scan Time	The amount of time, in milliseconds, an AP will drift out of the current channel to scan another channel.
VoIP Aware Scan	Shows if Aruba's VoIP Intelligent Call Handling prevents any single AP from becoming congested with voice calls. If Intelligent Call Handling is enabled, you should also enable VoIP Aware Scan in the ARM profile, so the AP will not attempt to scan a different channel if one of its clients has an active VoIP call.
Power Save Aware Scan	When enabled, the AP will not scan if Power Save is active.
Video Aware Scan	If Video Aware Scan is enabled in the ARM profile, the AP will not attempt to scan a different channel if one of its clients has an active video session.
Ideal Coverage Index	The coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.
Acceptable Coverage Index	The minimal coverage that the AP should try to achieve on its channel. The denser the AP deployment, the lower this value should be.

Parameter	Description
Free Channel Index	The difference in the interference index between the new channel and current channel must exceed this value for the AP to move to a new channel. The higher this value, the lower the chance an AP will move to the new channel.
Backoff Time	Time, in seconds, an AP backs off after requesting a new channel or power level.
Error Rate Threshold	The percentage of errors in the channel that triggers a channel change.
Error Rate Wait Time	Time, in seconds, that the error rate has to maintain or surpass the error rate threshold before it triggers a channel change.
Channel Quality Aware Arm	Shows if ARM changes are based upon an internally calculated channel quality metric. When this feature is disabled, ARM initiates channel changes based on thresholds defined in this profile, and chooses the channel based on the calculated interference index value.
Channel Quality Threshold	Displays the channel quality percentage below which ARM initiates a channel change.
Channel Quality Wait Time	If channel quality is below the specified channel quality threshold for this wait time period, ARM initiates a channel change.
Minimum Scan Time	Time, in seconds, that a channel must be scanned before it is considered for assignment.
Load aware Scan Threshold	The traffic throughput level an AP must reach before it stops scanning, in bytes/second. A value of 0 to disables this feature.
Mode Aware Arm	If enabled, ARM will turn APs into AMs if it detects higher coverage levels than necessary. This helps avoid higher levels of interference on the WLAN. Although this setting is disabled by default, you may want to enable this feature if your APs are deployed in close proximity (e.g. less than 60 feet apart).
Scan Mode	This parameter defines the scan mode for the AP. ■ all-reg-domain: The AP scans channels within all regulatory domains. This is the default setting. ■ reg-domain:Limit the AP scans to just the regulatory domain for that AP.
Client Match	The client match feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is enabled by default
Client Match report interval (sec)	This interval defines how often an AP sends an updated client probe report to the controller. Each client probe report contains a list of MAC addresses for clients that have been active in the last two minutes, and the AP radio SNR values seen by those clients.
Client Match Unsteerable Client Ageout Interval	The client entries in an unsteerable client list remain in effect for the interval defined by this parameter before they age out.

Parameter	Description
Client Match Unsteerable Client Ageout	When client match and the client match unsteerable client ageout feature are enabled, the controller periodically sends APs that are not a desired AP match for a client in a list of unsteerable clients. These lists contain a list of MAC addresses for up to 128 clients that should not be steered to that AP.
Client Match Sticky Client Check Interval (sec)	Frequency at which the AP checks for client's received SNR values. If the SNR value drops below the threshold defined by the **cm-sticky-snr** parameter for three consecutive check intervals, that client may be moved to an different AP.
Client Match Sticky Client Check SNR (dB)	If the client's received signal strength indicator (RSSI) is above this signal-to-noise ratio (SNR) threshold, that client will be allowed to stay associated to its current AP. If the client's received signal strength is below this threshold, it may be moved to a different AP.
Client Match SNR threshold(dB)	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the AP radio is stronger than its current radio by the dB level defined by the cm-sticky-snr-thresh parameter, and the candidate radio also has a minimum signal level defined by the cm-sticky-min-signal parameter.
Client Match Sticky Min Signal	A client triggered to move to a different AP may consider an AP radio a better match if the client detects that the signal from the candidate AP radio is at or higher than the minimum signal level defined by this parameter*and* the candidate radio has a higher signal strength than the radio to which the client is currently associated. (The required improvement in signal strength can be defined using the **cm-sticky-snr-delta** command.)
Client Match Restriction timeout (sec)	When a client is steered from one AP to a more desirable AP, the steer timeout feature helps facilitate the move by defining the amount of time that any APs to which the client should NOT associate will not respond to the AP.
Client Match Load Balancing threshold (%)	When the client match feature is enabled, clients may be steered from a highly utilized channel on an AP to a channel with fewer clients. If a channel on an AP radio has this percentage fewer clients than another channel supported by the client, the client match feature may move clients from the busier channel to the channel with fewer clients.
Client Match VBR Stale Entry Age (sec)	The controller can maintains client match data for the maximum number of supported clients for that controller platform, showing the detected SNR values for up to 16 candidate APs per client. This table is periodically updated as APs send client probe reports to the controller. This parameter defines the amount of time that the controller should retain client match data from each client probe report.
Client Match Max Steer Failures	The controller keeps track of the number of times the client match feature failed to steer a client to a different radio, and the reason that each steer attempt was triggered. If the client match feature attempts to steer a client to a new radio multiple consecutive times for the same reason but client steering fails each time, the controller notifies the AP to mark the client as unsteerable for that specific trigger. This parameter defines the maximum allowed number of client match steering fails with the same trigger before the client is marked as unsteerable for that trigger.
Client Match Load Balancing Client Threshold	If an AP radio has fewer clients than the client match load balancing threshold defined by this parameter, the AP will not participate in load balancing.

Parameter	Description
Client Match Load Balancing SNR Threshold (dB)	Clients must detect a SNR from an underutilized AP radio at or above this threshold before the client match feature considers load balancing a client to that radio.
Dynamic Bandwidth Switch	ARM dynamic 80MHz/40MHz bandwidth switch when 80MHz assignment is enabled.
Dynamic Bandwidth Switch Wait Time (sec)	Minimum time in seconds during which dynamic bandwidth switch indicators have to be true to trigger a 80MHz to 40MHz bandwidth change.
Dynamic Bandwidth Switch Triggering Indicator CCA ibss Threshold (%)	Dynamic Bandwidth Switch wait time window starts when load aware scan rejects increases and CCA ibss is below the threshold.
Dynamic Bandwidth Switch Triggering Indicator Beacon Failed Threshold	Dynamic Bandwidth Switch beacon failed indicator is true if beacon failed num is no less than this threshold during the wait time window.
Dynamic Bandwidth Switch Triggering Indicator CCA intf Threshold (%)	Dynamic Bandwidth Switch CCA intf indicator is true if CCA intf is no less than this threshold during the wait time window.
Dynamic Bandwidth Switch Clear Time (min)	Dynamic Bandwidth Switch back to 80MHz channel after the clear time in minutes if currently there is no high volume of traffic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rf dot11a-radio-profile

```
show rf dot11a-radio-profile [<profile>]
```

Description

Show an 802.11a Radio profile.

Syntax

Parameter	Description
<profile>	Name of an 802.11a profile.

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire 802.11a Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured 802.11a Radio profiles. The **References** column lists the number of other profiles with references to the 802.11a Radio profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode]# show rf dot11a-radio-profile
802.11a radio profile List
--------------------------
Name          References  Profile Status
----          ----------  --------------
default       18
default-AP85  1
test          1

Total:3.
```

This example displays the configuration settings for the profile default.

```
(host) # show rf dot11a-radio-profile default
802.11a radio profile "default"
Parameter                                   Value
---------                                   -----
Radio enable                                Enabled
Mode                                        ap-mode
High throughput enable (radio)              Enabled
Very high throughput enable (radio)         Enabled
Channel                                     N/A
Transmit EIRP                               15 dBm
Non-Wi-Fi Interference Immunity             2
Supr Immunity                               0
Enable CSA                                  Disabled
CSA Count                                   4
Spectrum Monitoring                         Enabled
Spectrum Monitoring Profile                 default-a
Advertise 802.11d and 802.11h Capabilities  Disabled
Spectrum Load Balancing                     Disabled
Spectrum Load Balancing Mode                channel
```

```
Spectrum Load Balancing Update Interval (sec)  30 seconds
Spectrum Load Balancing Threshold (%)          20 percent
Spectrum Load Balancing Domain                 N/A
Beacon Period                                  100 msec
Beacon Regulate                                Disabled
Advertized regulatory max EIRP                 0
ARM/WIDS Override                              OFF
Reduce Cell Size (Rx Sensitivity)              0 dB
Energy Detect Threshold Offset                 0 dB
Management Frame Throttle interval             1 sec
Management Frame Throttle Limit                20
Maximum Distance                               0 meters
RX Sensitivity Threshold                       0 dB
RX Sensitivity Tuning Based Channel Reuse      disable
Set to Radar Test Mode                         disabled
Adaptive Radio Management (ARM) Profile        default
High-throughput Radio Profile                  default-a
AM Scanning Profile                            default
Enable frame transmissions                     Enabled
Max Channel Bandwidth                          80MHz
Max EIRP                                       18 dBm
Min EIRP                                       12 dBm
EIRP Offset                                    0 dBm
deploy-hour                                    N/A
```

The output of this command includes the following parameters:

Parameter	Description
Radio enable	Shows if the AP has enabled or disabled transmissions on this radio band.
Mode	Access Point operating mode. Available options are: ■ am-mode: Air Monitor mode ■ ap-mode: Access Point mode ■ apm-mode: Access Point Monitor mode ■ sensor-mode: RFprotect sensor mode
High throughput enable (radio)	Shows if high-throughput (802.11n) is enabled on the radio. A high-throughput profile manages 40 Mhz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.) A high-throughput profile also determines whether an AP radio using the profile will stop using the 40 MHz channels surrounding APs or stations advertise 40 Mhz intolerance. This option is enabled by default.
Very high throughput enable (radio)	Enable or disable support for Very High Throughput (802.11ac) on the radio. This option is enabled by default.
Channel	Channel number for the AP 802.11a, 802.11n, or 802.11ac physical layer.
Transmit EIRP	Maximum transmit power (EIRP) in dBm from 0 to 51 in .5 dBm increments. Further limited by regulatory domain constraints and AP capabilities.

Parameter	Description
Non-Wi-Fi Interference Immunity	Sets a value for 802.11 Interference Immunity. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly "deaf" to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: ■ Level-0: no ANI adaptation. ■ Level-1: noise immunity only. ■ Level-2: noise and spur immunity. This is the default setting ■ Level-3: level 2 and weak OFDM immunity. ■ Level-4: level 3 and FIR immunity.
Spur Immunity	Displays the spur immunity value for 802.11a radio. **NOTE:** This parameter is applicable for 130 Series access points only. The controller ignores this parameter if configured for non-130 Series access points.
Enable CSA	Shows if CSAs are enabled or disabled. CSAs, as defined by IEEE 802.11h, enable an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.
CSA Count	Number of channel switch announcements that must be sent prior to switching to a new channel. The default CSA count is 4 announcements.
Spectrum Monitoring	If enabled, the AP operates as a hybrid AP that can simultaneously serve clients and monitor a single channel for spectrum analysis data.
Spectrum Monitoring Profile	The spectrum monitoring profile referenced by APs using this 802.11a radio profile. For details, see rf spectrum-profile on page 879
Advertise 802.11d and 802.11h Capabilities	If enabled, the radio advertises its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
Spectrum load balancing	The Spectrum load balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP's client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.
Spectrum load balancing mode	SLB Mode allows control over how to balance clients. Channel-based load-balancing balances clients across channels. Radio-based load-balancing distributes clients across radios on the same band, independent of channels.
Spectrum load balancing mode update interval	This parameter specifies how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.

Parameter	Description
Spectrum load balancing threshold	If the spectrum load balancing feature is enabled, this parameter controls the percentage difference between number of clients on a channel channel that triggers load balancing. The default value is 20%, meaning that spectrum load balancing is activated when there are 20% more clients on one channel than on another channel used by the AP radio.
Spectrum load balancing domain	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled ARM scanning and channel assignment. ■ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is *not* defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain *isalso* defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.
Beacon Period	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	If enabled, this option introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. This option is disabled by default.
Advertised Regulatory Max EIRP	Shows if the radio is configured to work around a known issue on Cisco 7921G telephones by capping for a radio's maximum EIRP. When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons. The supported value is1–31 dBm.
ARM/WIDS Override	If enabled, this option disables ARM and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.
Reduce Cell Size (Rx Sensitivity)	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.
Energy Detect Threshold Offset	This parameter can modify the energy detect threshold used by the radio in making transmit decisions. The energy detect threshold is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. A value of 0 indicates the AP is using the default energy detect threshold for this radio. (This value may vary by AP model)

Parameter	Description
Management Frame Throttle Interval	Averaging interval for rate limiting mgmt frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.
Management Frame Throttle Limit	Maximum number of management frames that can come in from this radio in each throttle interval.
Maximum Distance	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km..
RX Sensitivity Threshold	If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (-dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. For example, if the RX sensitivity threshold was set to -65 dBm, the AP would ignore signals with a strength from -1 dBM to -64 dBm. If the value is set to zero, the feature will automatically determine an appropriate threshold.
RX Sensitivity Tuning Based Channel Reuse	Shows if the channel reuse feature's current operating mode, static, dynamic or disable. ■ **Static**: This mode of operation is a coverage-based adaptation of the CCA thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ **Dynamic**: In this mode, the CCA thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ **Disable**: This mode does not support the tuning of the CCA Detect Threshold.
Set to Radar Test Mode	For internal use only.
Adaptive Radio Management (ARM) Profile	Name of an ARM profile associated with this 802.11a profile.
High-throughput Radio Profile	Name of a High Throughput Radio profile associated with this 802.11a profile.
AM Scanning Profile	The AM scanning profile referenced by APs using this 802.11a radio profile. For details, seerf am-scan-profile on page 826
Max Channel Bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Master managed devices.
Min Channel Bandwidth	Sets the minimum channel bandwidth for APs associated to Mobility Master managed devices.

Parameter	Description
Max EIRP	The maximum transmission power level from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.
Min EIRP	The minimum transmission power level (in dBm) to be assigned to the AP radio(s).
EIRP Offset	This parameter is used to manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.
deploy-hour	Specify a number from 0-23 to select the hour during which AirMatch updates are sent to the APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Master, the AirMatch solution will be deployed according to the time zone of the managed device. **NOTE:** If this parameter is set in both the AirMatch profile and radio profile, the setting in the radio profile will take precedence.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **deploy-hour**, **eirp-offset, Energy Detect Threshold Offset** and **Min Channel Bandwidth** parameters are introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show rf dot11g-radio-profile

```
show rf dot11g-radio-profile [<profile>]
```

Description

Show an 802.11g Radio profile.

Syntax

Parameter	Description
<profile>	Name of a 802.11g profile.

Usage Guidelines

Issue this command without the **<profile>**parameter to display the entire 802.11g profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has four configured 802.11g profiles. The **References** column lists the number of other profiles with references to the 802.11g profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host)[mynode] # show rf arm-profile
Adaptive Radio Management (ARM) profile List
--------------------------------------------
Name                    References  Profile Status
----                    ----------  --------------
airwave                 4
default                 4
no-scanning             1
nokia-rf-profile        1

Total:4.
```

This example displays the configuration settings for the profile **default**.

```
(host)[mynode]# show rf dot11g-radio-profile default
802.11g radio profile "default"
-------------------------------
Parameter                                       Value       Set
---------                                       -----       ---
Radio enable                                    Enabled
Mode                                            ap-mode
High throughput enable (radio)                  Enabled
Very high throughput rates enable (256-QAM)     Disabled
Channel                                         N/A
Transmit EIRP                                   15 dBm
Non-Wi-Fi Interference Immunity                 2
Enable CSA                                      Disabled
CSA Count                                       4
Spectrum Monitoring                             Disabled
Spectrum Monitoring Profile                     default-g
Advertise 802.11d and 802.11h Capabilities      Disabled
```

```
Spectrum Load Balancing                          Disabled
Spectrum Load Balancing Mode                     channel
Spectrum Load Balancing Update Interval (sec)    30 seconds
Spectrum Load Balancing Threshold (%)            20 percent
Spectrum Load Balancing Domain                   N/A
Beacon Period                                    100 msec
Beacon Regulate                                  Disabled
Advertised regulatory max EIRP                   0
ARM/WIDS Override                                OFF
Reduce Cell Size (Rx Sensitivity)                0 dB
Energy Detect Threshold Offset                   0 dB
Management Frame Throttle interval               1 sec
Management Frame Throttle Limit                  20
Maximum Distance                                 0 meters
RX Sensitivity Threshold                         0 dB
RX Sensitivity Tuning Based Channel Reuse        disable
Protection for 802.11b Clients                   Enabled
Adaptive Radio Management (ARM) Profile          default-g
High-throughput Radio Profile                    default-g
AM Scanning Profile                              default
Enable frame transmissions                       Enabled
Max Channel Bandwidth                            20MHz
Min Channel Bandwidth                            20MHz
Max EIRP                                         9 dBm
Min EIRP                                         6 dBm
EIRP Offset                                      0 dBm
deploy-hour                                      N/A
```

The output of this command includes the following parameters:

Parameter	Description
Radio enable	Shows if the AP has enabled or disabled transmissions on this radio band.
Mode	Access Point operating mode. Available options are: ■ am-mode: Air Monitor mode ■ ap-mode: Access Point mode ■ apm-mode: Access Point Monitor mode ■ sensor-mode: RFprotect sensor mode
High throughput enable (radio)	Shows if high-throughput (802.11n) is enabled on the radio. A high-throughput profile manages 40 Mhz tolerance settings, and controls whether or not APs using this profile will advertise intolerance of 40 MHz operation. (This option is disabled by default, allowing 40 MHz operation.) A high-throughput profile also determines whether an AP radio using the profile will stop using the 40 MHz channels surrounding APs or stations advertise 40 Mhz intolerance. This option is enabled by default.
Very High Throughput Rates Enable	Enable or disable support for Very High Throughput (802.11ac) on the radio. This option is enabled by default.
Channel	Channel number for the AP 802.11a, 802.11n, or 802.11ac physical layer.
Transmit EIRP	Maximum transmit power (EIRP) in dBm from 0 to 51 in .5 dBm increments. Further limited by regulatory domain constraints and AP capabilities.

Parameter	Description
Non-Wi-Fi Interference Immunity	Sets a value for 802.11 Interference Immunity. The default setting for this parameter is level 2. When performance drops due to interference from non-802.11 interferers (such as DECT or Bluetooth devices), the level can be increased up to level 5 for improved performance. However, increasing the level makes the AP slightly “deaf” to its surroundings, causing the AP to lose a small amount of range. The levels for this parameter are: ■ Level-0: no ANI adaptation. ■ Level-1: noise immunity only. ■ Level-2: noise and spur immunity. This is the default setting ■ Level-3: level 2 and weak OFDM immunity. ■ Level-4: level 3 and FIR immunity.
Enable CSA	Shows if CSAs are enabled or disabled. CSAs, as defined by IEEE 802.11h, enable an AP to announce that it is switching to a new channel before it begins transmitting on that channel. This allows clients that support CSA to transition to the new channel with minimal downtime.
CSA Count	Number of channel switch announcements that must be sent prior to switching to a new channel. The default CSA count is 4 announcements.
Spectrum Monitoring	If enabled, the AP operates as a hybrid AP that can simultaneously serve clients and monitor a single channel for spectrum analysis data.
Spectrum Monitoring Profile	The spectrum monitoring profile referenced by APs using this 802.11a radio profile. For details, see rf spectrum-profile on page 879
Advertise 802.11d and 802.11h Capabilities	If enabled, the radio advertises its 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities.
Spectrum load balancing	The Spectrum load balancing feature helps optimize network resources by balancing clients across channels, regardless of whether the AP or the controller is responding to the wireless clients' probe requests. If enabled, the controller compares whether or not an AP has more clients than its neighboring APs on other channels. If an AP’s client load is at or over a predetermined threshold as compared to its immediate neighbors, or if a neighboring Aruba AP on another channel does not have any clients, load balancing will be enabled on that AP. This feature is disabled by default.
Spectrum load balancing mode	SLB Mode allows control over how to balance clients. Channel-based load-balancing balances clients across channels. Radio-based load-balancing distributes clients across radios on the same band, independent of channels.
Spectrum load balancing mode update interval	This parameter specifies how often spectrum load balancing calculations are made (in seconds). The default value is 30 seconds.

Parameter	Description
Spectrum load balancing threshold	If the spectrum load balancing feature is enabled, this parameter controls the percentage difference between number of clients on a channel channel that triggers load balancing. The default value is 20%, meaning that spectrum load balancing is activated when there are 20% more clients on one channel than on another channel used by the AP radio.
Spectrum load balancing domain	Define a spectrum load balancing domain to manually create RF neighborhoods. Use this option to create RF neighborhood information for networks that have disabled ARM scanning and channel assignment. ■ If spectrum load balancing is enabled in a 802.11a radio profile but the spectrum load balancing domain is *not* defined, ArubaOS uses ARM to calculate RF neighborhoods. ■ If spectrum load balancing is enabled in a 802.11a radio profile and a spectrum load balancing domain *isalso* defined, AP radios belonging to the same spectrum load balancing domain will be considered part of the same RF neighborhood for load balancing, and will not recognize RF neighborhoods defined by ARM.
Beacon Period	Time, in milliseconds, between successive beacon transmissions. The beacon advertises the AP's presence, identity, and radio characteristics to wireless clients.
Beacon Regulate	If enabled, this option introduces randomness in the beacon generation so that multiple APs on the same channel do not send beacons at the same time, which causes collisions over the air. This option is disabled by default.
Advertised Regulatory Max EIRP	Shows if the radio is configured to work around a known issue on Cisco 7921G telephones by capping for a radio's maximum EIRP. When you enable this parameter, even if the regulatory approved maximum for a given channel is higher than this EIRP cap, the AP radio using this profile will advertise only this capped maximum EIRP in its radio beacons. The supported value is1–31 dBm.
ARM/WIDS Override	If enabled, this option disables ARM and Wireless IDS functions and slightly increases packet processing performance. If a radio is configured to operate in Air Monitor mode, then the ARM/WIDS override functions are always enabled, regardless of whether or not this check box is selected.
Reduce Cell Size (Rx Sensitivity)	The cell size reduction feature allows you manage dense deployments and to increase overall system performance and capacity by shrinking an AP's receive coverage area, thereby minimizing co-channel interference and optimizing channel reuse. The possible range of values for this feature is 0-55 dB. The default 0 dB reduction allows the radio to retain its current default Rx sensitivity value.
Energy Detect Threshold Offset	This parameter can modify the energy detect threshold used by the radio in making transmit decisions. The energy detect threshold is a negative value, and the value specified for this parameter (1-12) is the offset from the base value of -59 dBm. For example a value of 1 = -60 dBm, and a value of 10: = -69 dBm. A value of 0 indicates the AP is using the default energy detect threshold for this radio. (This value may vary by AP model).

Parameter	Description
Management Frame Throttle Interval	Averaging interval for rate limiting mgmt frames from this radio, in seconds. A management frame throttle interval of 0 seconds disables rate limiting.
Management Frame Throttle Limit	Maximum number of management frames that can come in from this radio in each throttle interval.
Maximum Distance	Maximum distance between a client and an AP or between a mesh point and a mesh portal, in meters. This value is used to derive ACK and CTS timeout times. A value of 0 specifies default settings for this parameter, where timeouts are only modified for outdoor mesh radios which use a distance of 16km..
RX Sensitivity Threshold	If the Rx Sensitivity Tuning Based Channel reuse feature is set to static mode, this parameter manually sets the AP's Rx sensitivity threshold (-dBm). The AP will filter out and ignore weak signals that are below the channel threshold signal strength. For example, if the RX sensitivity threshold was set to -65 dBm, the AP would ignore signals with a strength from -1 dBM to -64 dBm. If the value is set to zero, the feature will automatically determine an appropriate threshold.
RX Sensitivity Tuning Based Channel Reuse	Shows if the channel reuse feature's current operating mode, static, dynamic or disable. ■ **Static**: This mode of operation is a coverage-based adaptation of the CCA thresholds. In the static mode of operation, the CCA is adjusted according to the configured transmission power level on the AP, so as the AP transmit power decreases as the CCA threshold increases, and vice versa. ■ **Dynamic**: In this mode, the CCA thresholds are based on channel loads, and take into account the location of the associated clients. When you set the Channel Reuse This feature is automatically enabled when the wireless medium around the AP is busy greater than half the time. When this mode is enabled, the CCA threshold adjusts to accommodate transmissions between the AP its most distant associated client. ■ **Disable**: This mode does not support the tuning of the CCA Detect Threshold.
Protection for 802.11b Clients	Shows if the profile has enabled or disabled protection for 802.11b clients.
Adaptive Radio Management (ARM) Profile	Name of an Adaptive Radio Management profile associated with this 802.11a profile.
High-throughput Radio Profile	Name of a High Throughput Radio profile associated with this 802.11a profile.
AM Scanning Profile	The AM scanning profile referenced by APs using this 802.11a radio profile. For details, seerf am-scan-profile on page 826
Max Channel Bandwidth	Sets the maximum channel bandwidth for APs associated to Mobility Mastermanaged devices.
Min Channel Bandwidth	Sets the minimum channel bandwidth for APs associated to Mobility Mastermanaged devices.

Parameter	Description
Max EIRP	Maximum EIRP from 3 to 33 dBm. You may also specify a special value of 127 dBm for regulatory maximum to disable power adjustments for environments such as outdoor mesh links.
Min EIRP	The minimum transmission power level (in dBm) to be assigned to the AP radio(s).
EIRP Offset	This parameter is used to manually adjust EIRP levels selected by the AirMatch algorithm by specifying a value from -6 to 6 dBm.
deploy-hour	The hour during which AirMatch updates are sent to APs (in 24-hour format). If the managed device to which the AP is associated is in a different time zone than Mobility Master, the AirMatch solution will be deployed according to the time zone of the managed device. **NOTE:** If this parameter is set in both the AirMatch profile and the 802.11a radio profile, the setting in the 802.11a radio profile will take precedence.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	The **deploy-hour**, **eirp-offset, Energy Detect Threshold Offset** and **Min Channel Bandwidth** parameters are introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show rf event-thresholds-profile

```
show rf event-thresholds-profile [<profile>]
```

Description

Show an Event Thresholds profile.

Syntax

Parameter	Description
<profile>	name of an Event Thresholds profile

Usage Guidelines

Issue this command without the **<profile>** parameter to display the entire Event Thresholds profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Event Thresholds profiles. The **References** column lists the number of other profiles with references to the Event Thresholds profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host)[mynode]# show rf event-thresholds-profile

RF Event Thresholds Profile List
--------------------------------
Name     References  Profile Status
----     ----------  --------------
default  6
event1           2

Total: 2.
```

This example displays the configuration settings for the profile **default**.

```
(host)[mynode]# show rf event-thresholds-profile default
RF Event Thresholds Profile "default"
-------------------------------------
Parameter                                Value
---------                                -----
Detect Frame Rate Anomalies              Disabled
Bandwidth Rate High Watermark            0 %
Bandwidth Rate Low Watermark             0 %
Frame Error Rate High Watermark          0 %
Frame Error Rate Low Watermark           0 %
Frame Fragmentation Rate High Watermark  16 %
Frame Fragmentation Rate Low Watermark   8 %
Frame Low Speed Rate High Watermark      16 %
Frame Low Speed Rate Low Watermark       8 %
Frame Non Unicast Rate High Watermark    0 %
Frame Non Unicast Rate Low Watermark     0 %
Frame Receive Error Rate High Watermark  16 %
Frame Receive Error Rate Low Watermark   8 %
Frame Retry Rate High Watermark          16 %
```

```
Frame Retry Rate Low Watermark          8 %
```

The output of this command includes the following parameters:

Parameter	Description
Detect Frame Rate Anomalies	Shows of the profile enables or disables detection of frame rate anomalies.
Bandwidth Rate High Watermark	If bandwidth in an AP exceeds this value, it triggers a **bandwidth exceeded condition**. The value represents the percentage of maximum for a given radio. (For 802.11b, the maximum bandwidth is 7 Mbps. For 802.11 a and g, the maximum is 30 Mbps.) The recommended value is 85%.
Bandwidth Rate Low Watermark	If an AP triggers a **bandwidth exceeded** condition, the condition persists until bandwidth drops below this value.
Frame Error Rate High Watermark	If the frame error rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame error rate exceeded** condition.
Frame Error Rate Low Watermark	If an AP triggers a **frame error rate exceeded** condition, the condition persists until the frame error rate drops below this value.
Frame Fragmentation Rate High Watermark	If the frame fragmentation rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame fragmentation rate exceeded** condition.
Frame Fragmentation Rate Low Watermark	If an AP triggers a **frame fragmentation rate exceeded** condition, the condition persists until the frame fragmentation rate drops below this value.
Frame Low Speed Rate High Watermark	If the rate of low-speed frames (as a percentage of total frames in an AP) exceeds this value, it triggers a **low-speed rate exceeded** condition.
Frame Low Speed Rate Low Watermark	After a **low-speed rate exceeded condition** exists, the condition persists until the percentage of low-speed frames drops below this value.
Frame Non Unicast Rate High Watermark	If the non-unicast rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **non-unicast rate exceeded** condition. This value depends upon the applications used on the network.
Frame Non Unicast Rate Low Watermark	If an AP triggers a **non-unicast rate exceeded** condition, the condition persists until the non-unicast rate drops below this value.
Frame Receive Error Rate High Watermark	If the frame receive error rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame receive error rate exceeded** condition.
Frame Receive Error Rate Low Watermark	If an AP triggers a **frame receive error rate exceeded** condition, the condition persists until the frame receive error rate drops below this value.
Frame Retry Rate High Watermark	If the frame retry rate (as a percentage of total frames in an AP) exceeds this value, it triggers a **frame retry rate exceeded** condition.
Frame Retry Rate Low Watermark	If an AP triggers a **frame retry rate exceeded** condition exists, the condition persists until the frame retry rate drops below this value.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rf ht-radio-profile

```
show rf ht-radio-profile [<profile>]
```

Description

Show a High-throughput Radio profile.

Syntax

Parameter	Description
<profile>	Name of a High-throughput Radio profile.

Usage Guidelines

Issue this command without the **<profile>**parameter to display the entire High-throughput Radio profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has five configured High-throughput Radio profiles. The **References** column lists the number of other profiles with references to the High-throughput Radio profile, and the **Profile Status** column indicates whether the profile is predefined and editable, and if that predefined profile has been changed from its default settings. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode]# show rf ht-radio-profile
High-throughput radio profile List
----------------------------------
Name            References  Profile Status
----            ----------  --------------
default         0
default-a       8           Predefined (editable)
default-g       3           Predefined (changed)
legacystation   1
test            1

Total:5
```

This example displays the configuration settings for the predefined profile **default-a**.

```
(host) #show rf ht-radio-profile default-a
High-throughput radio profile "default-a" (Predefined (editable))
------------------------------------------------------------------
Parameter                       Value
---------                       -----
40 MHz intolerance              Disabled
Honor 40 MHz intolerance        Enabled
Diversity spreading workaround  Disabled
```

The output of this command includes the following parameters:

Parameter	Description
40 MHz intolerance	Shows whether or not APs using this radio profile will advertise intolerance of 40 MHz operation. By default, 40 MHz operation is allowed.
Honor 40 MHz intolerance	If this parameter is enabled, the radio will stop using the 40 MHz channels if the 40 MHz intolerance indication is received from another AP or station.
Diversity Spreading Workaround	When this feature is enabled, all legacy transmissions will be sent using a single antenna. This enables interoperability for legacy or high-throughput stations that cannot decode 802.11n cyclic shift diversity data. This feature is disabled by default and should be kept disabled unless necessary.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rf optimization-profile

```
show rf optimization-profile [<profile>]
```

Description

Show an Optimization profile.

Syntax

Parameter	Description
<profile>	name of an ARM profile

Usage Guidelines

Issue this command without the **<profile>**parameter to display the entire Optimization profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Optimization profiles. The **References** column lists the number of other profiles with references to the Optimization profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode]# show rf optimization-profile
RF Optimization Profile List
----------------------------
Name     References  Profile Status
----     ----------  --------------
default  6
profile2 1

Total:2
```

This example displays the configuration settings for the profile **profile2**.

```
(host)[mynode]#show rf optimization-profile profile2
RF Optimization Profile "profile2"
----------------------------------
Parameter                           Value
---------                           -----
Station Handoff Assist              Disabled
Detect Association Failure          Disabled
Coverage Hole Detection             Disabled
Hole Good RSSI Threshold            20
Hole Good Station Ageout            30 sec
Hole Detection Interval             180 sec
Hole Idle Station Ageout            90 sec
Hole Poor RSSI Threshold            10
Detect interference                 Disabled
Interference Threshold              90 %
Interference Threshold Exceed Time  25 sec
Interference Baseline Time          25 sec
RSSI Falloff Wait Time              4
Low RSSI Threshold                  10
RSSI Check Frequency                3 sec
```

The output of this command includes the following parameters:

Parameter	Description
Station Handoff Assist	If enabled, this parameter allows the controller to force a client off an AP when the RSSI drops below a defined minimum threshold.
Detect Association Failure	Shows if the profile enables or disables STA association failure detection.
Coverage Hole Detection	Shows if the profile enables or disables coverage hole detection.
Hole Good RSSI Threshold	Time, in seconds, after a coverage hole is detected until a coverage hole event notification is generated. This parameter requires the RF Protect license.
Hole Good Station Ageout	Stations with signal strength above this value are considered to have good coverage. This parameter requires the RF Protect license.
Hole Detection Interval	Time, in seconds, after which a station with good coverage is aged out. This parameter requires the RF Protect license.
Hole Idle Station Ageout	Time, in seconds, after which a station in a poor coverage area is aged out. This parameter requires the RF Protect license.
Hole Poor RSSI Threshold	Stations with signal strength below this value will trigger detection of a coverage hole. This parameter requires the RF Protect license.
Detect interference	Enables or disables interference detection.
Interference Threshold	Percentage increase in the frame retry rate or frame receive error rate before interference monitoring begins on a given channel.
Interference Threshold Exceed Time	Time, in seconds, the FRR or FRER exceeds the threshold before interference is reported.
Interference Baseline Time	Time, in seconds, the air monitor should learn the state of the link between the AP and client to create frame retry rate and frame receive error rate baselines.
RSSI Falloff Wait Time	Number of times the detected client RSSI level must fall below the minimum RSSI threshold the before the AP sends a deauthorization message to the client. The maximum value is 8 times.
Low RSSI Threshold	Minimum RSSI above which deauthorization messages should never be sent.
RSSI Check Frequency	Interval, in seconds, to sample RSSI.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rf spectrum-profile

```
rf spectrum-profile <profile-name>
```

Description

Show a spectrum profile used by the spectrum analysis feature.

Syntax

Parameter	Description
`<profile>`	Name of a spectrum profile.

Usage Guidelines

Issue this command without the **<profile>**parameter to display the entire spectrum profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three configured spectrum profiles. The **References** column lists the number of other profiles with references to the spectrum profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)[mynode]#show rf spectrum-profile

Spectrum profile List
---------------------
Name        References  Profile Status
----        ----------  --------------
spectrum1   1
default-a   2           Predefined (editable)
default-g   2           Predefined (editable)
```

This example displays the configuration settings for the profile spectrum1.

```
(host)[mynode]#show rf spectrum-profile default

Spectrum profile "default"
--------------------------
Parameter                                 Value
---------                                 -----
Age Out: WIFI                             600 sec
Age Out: Generic Interferer               30 sec
Age Out: Microwave                        15 sec
Age Out: Microwave (Inverter type)        15 sec
Age Out: Video Device                     60 sec
Age Out: Audio Device                     10 sec
Age Out: Cordless Phone Fixed Frequency   10 sec
Age Out: Generic Fixed Frequency          10 sec
Age Out: Bluetooth                        25 sec
Age Out: Xbox                             25 sec
Age Out: Cordless Network Frequency Hopper  60 sec
Age Out: Cordless Base Frequency Hopper   240 sec
Age Out: Generic Frequency Hopper         25 sec
```

The output of this command includes the following information:

Parameter	Description
`Age Out: WIFI`	The number of seconds for which a wifi device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 600 seconds.
`Age Out: Generic Interferer`	The number of seconds for which an unknown device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 30 seconds.
`Age Out: Microwave`	The number of seconds for which a microwave device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 15 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
`Age Out: Microwave (inverter type)`	The number of seconds for which an inverter microwave must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 15 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
`Age Out: Video Device`	The number of seconds for which a video device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 60 seconds.
`Age Out: Audio Device`	The number of seconds for which an audio device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Cordless Phone Fixed Frequency`	The number of seconds for which a fixed frequency cordless phone must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Generic Fixed Frequency`	The number of seconds for which a generic fixed frequency device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 10 seconds.
`Age Out: Xbox`	The number of seconds for which an Xbox device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.

Parameter	Description
`Age Out: Bluetooth`	The number of seconds for which a bluetooth device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds. Note that this parameter is applicable to 2.4GHz spectrum monitor radios only.
`Age Out: Cordless Network Frequency Hopper`	The number of seconds for which a frequency-hopping cordless network device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 60 seconds.
`Age Out: Cordless Base Frequency Hopper`	The number of seconds for which a frequency-hopping cordless phone base must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 240 seconds.
`Age Out: Generic Frequency Hopper`	The number of seconds for which a generic frequency-hopping device must stop sending a signal before the spectrum monitor considers that device no longer active on the network. The default value is 25 seconds.

Related Commands

Command	Description
rf spectrum-profile	RF spectrum profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show rft profile

```
show rft profile {all|ht-link-quality|link-quality|raw}
```

Description

Show parameters for the predefined RF test profiles.

Syntax

Parameter	Description
`all`	Show all predefined profiles.
`ht-link-quality`	Show configured parameters for the predefined **HT Link Quality** test profile.
`link-quality`	Show configured parameters for the predefined **Link Quality** test profile.
`raw`	Show configured parameters for the predefined **RAW** test profile.

Usage guidelines

The rft command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support. Issue the **show rft profile** command to view the profiles used for these RF tests.

Example

The following example shows the testing parameters for the predefined link-quality RF test profile.

```
(host) #show rft profile link-quality

Profile LinkQuality: Built-in profile
-------------------------------------
Parameter    Value
---------    -----
Antenna      1 and/or 2
Frame Type   Null Data
Num Packets  100 for each data-rate
Packet Size  1500
Num Retries  0
Data Rate    All rates are tried
```

Related Commands

Command	Description
show rft result	Shows the results of an RF test.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **ht-link-quality** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed device.

show rft result

```
show rft result all|{trans-id <trans-id>}
```

Description

Show the results of an RF test.

Syntax

Parameter	Description
`all`	Show the most recent test result for each test type (antenna-connectivity, link-quality or raw).
`trans-id <trans-id>`	Each RF test is assigned a transaction ID. Include the **trans-id <trans-id>** parameters to show the test result for a specific transaction ID.

Usage guidelines

The rft command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support.

Related Commands

Command	Description
show rft transactions	Shows the most recent transaction IDs for each test type.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed device.

show rft transactions

```
show rft transactions
```

Description

Show transaction IDs of RF tests.

Syntax

No parameters.

Usage guidelines

The rft command is used for RF troubleshooting, and should only be used under the supervision of Aruba technical support. Issue the **show rft transaction** command to view the transaction IDs for the most recent test of each test type.

Example

The following example shows the transaction IDs for the latest RAW, link-quality and antenna-connectivity tests.

```
(host) [mynode] #show rft transactions

RF troubleshooting transactions
-------------------------------
Profile              Transaction ID
-------              --------------
RAW                  2001
LinkQuality          2101
AntennaConnectivity  1801
```

Related Commands

Use transaction IDs with the command to view results for individual RF tests.

Related Commands

Command	Description
show rft result	Use transaction IDs with this command to view results for individual RF tests.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed device.

show rights

```
show rights [<name-of-a-role>]
```

Description

Displays the list of user roles in the roles table with high level details of role policies. To view role policies of a specific role specify the role name.

Syntax

Parameter	Description
`name-of-a-role`	Enter the role name to view its policy details.

Example

The output of this command shows the list of roles in the role table.

```
(host) [mynode]# show rights

RoleTable
---------
Name              ACL  Bandwidth                 ACL List                                Type
----              ---  ---------                 --------                                ----
ap-role           4    Up: No Limit,Dn: No Limit control/,ap-acl/                        System
authenticated     39   Up: No Limit,Dn: No Limit allowall/,v6-allowall/                  User
default-vpn-role  37   Up: No Limit,Dn: No Limit allowall/,v6-allowall/                  User
guest             3    Up: No Limit,Dn: No Limit http-acl/,https-acl/,dhcp-acl/         User
guest-logon       6    Up: No Limit,Dn: No Limit logon-control/,captiveportal/          User
logon             1    Up: No Limit,Dn: No Limit logon-control/,captiveportal/          User
stateful-dot1x    5    Up: No Limit,Dn: No Limit                                       System
voice             38   Up: No Limit,Dn: No Limit sip-acl/,noe-acl/,svp-acl/,vocera-acl/ User
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show roleinfo

```
show roleinfo
```

Description

Displays the role of the controller.

Syntax

No parameters.

Example

The output of this command shows the role of the controller.

```
(host) [mynode] # show roleinfo
switchrole:master
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed device.

show route-access-list

```
show route-access-list
```

Description

This command displays information about ACLs for PBR.

Syntax

No parameters.

Usage Guidelines

Policy-based routing is an optional feature that allows packets to be routed based on ACLs configured by the administrator. By default, when a managed device receives a packet for routing, it looks up the destination IP in the routing table and forwards the packet to the next hop router. If policy-based routing is configured, the next hop device can be chosen based on a defined access control list.

In a typical deployment scenario with multiple uplinks, the default route only uses one of the uplink next-hops for forwarding packets. If a next hop becomes unreachable, the packets will not reach their destination. If your deployment uses policy-based routing based on a next hop list, any of the uplink next hops could be used for forwarding traffic. This requires a valid ARP entry (Route-cache) in the system for all the policy-based routing next hops.

Example

The following command displays a list of configured routing access lists.

```
(host) [mynode] #show route-access-list

Router Access list table
------------------------
Name       Use Count  Roles
----       ---------  -----
attempt1   0
pbr        0
name       1          test
Tuesday    0
```

The output of this command includes the following parameters:

Parameter	Description
`Name`	Name of the access list.
`Use Count`	Number of VLANs associated with this routing access list.
`Roles`	User role associated with the routing access list.

Related Commands

Command	Description
ip access-list route	Configures an ACL for PBR.
ip nexthop-list	Defines a next-hop list for a routing policy.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license	Enable or Config mode on Mobility Master

show rrm dot11k admission-capacity

```
show rrm dot11k admission-capacity
```

Description

Displays the available admission capacity for voice traffic on an AP.

Syntax

No parameters.

Example

The output of this command shows the available admission capacity for voice traffic on all APs.

```
(host) # show rrm dot11k admission-capacity

802.11K Available Admission Capacity for Voice
----------------------------------------------

Flags: B: Bandwidth based CAC, C: Call-count based CAC
       D: CAC Disabled,        E: CAC Enabled

AP Name    IP Address    Freq Band  Chan  Total  Available  Flags
-------    ----------    ---------  ----  -----  ---------  -----
r-wing-94  10.16.12.247  5 GHz      40    31250  0          EC
r-wing-94  10.16.12.247  2.4 GHz    11    31250  0          EC

Num APs:2
```

Command History

This command was available in ArubaOS 3.4

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show rrm dot11k ap-channel-report

```
show rrm dot11k ap-channel-report [ap-name <name-of-an-ap> |
   bssid <bssid-of-an-ap> | ip-addr <ip-address-of-an-ap> | ip6-addr <ip-addr> | essid
   <essid>]
```

Description

Displays the channel information gathered by the AP. You can either specify an ap-name, bssid or ip-address of an AP to see more details.

Syntax

Parameter	Description
`ap-name`	Enter the name of the AP.
`bssid`	Enter the BSSID address of the AP.
`ip-addr`	Enter the IP address of the AP.
`ip6-addr`	Enter the IPv6 address of the AP
`essid`	Entries in the IPv4 user-table that are associated to the specified ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.

Example

The output of this command shows the channel information for r-wing-94:94.

```
(host) [mynode]# show rrm dot11k ap-channel-report ap-name r-wing-94

802.11K AP Channel Report Details
---------------------------------
Freq Band  Channel List
---------  ------------
2.4 GHz    11,
5 GHz      36, 40, 157, 161, 165,

Num Entries:2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show rrm dot11k beacon-report

```
show rrm dot11k beacon-report
```

Description

Displays the beacon report information sent by a client to its AP.

Syntax

No parameters.

Example

The output of this command shows the beacon report for the client 00:1f:6c:7a:d4:fd.

```
(host) [mynode]# show rrm dot11k beacon-report station-mac 00:1f:6c:7a:d4:fd

802.11K Beacon Report Details

-----------------------------------------------

Channel     BSSID              Reg Class     Antenna ID      Meas. Mode
----------  -------            ------------  -------------   ----------------
1           00:0b:86:6d:3e:40  0             1               Bcn Table

Num Elements:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show rrm dot11k neighbor-report

```
show rrm dot11k neighbor-report [ap-name |
   bssid <bssid-of-an-ap> | ip-addr <ip-address-of-an-ap>]
```

Description

Displays the neighbor information for a particular AP. If the AP name or the AP's IP address is specified, the user should specify the ESSID to get the neighbor information. If the ESSID is not specified, the command will display the neighbor information for all the Virtual AP's configured on the AP.

Syntax

Parameter	Description
`ap-name`	Identify the AP for which you want to view information.
`<name-of-an-ap>`	Name of an AP.
`<essid>`	ESSID of the AP. If the ESSID includes spaces, you must enclose it in quotation marks.
`bssid`	Enter the BSSID address of the AP.
`ip-addr`	Enter the IP address of the AP.

Example

The output of this command shows the neighbor information for r-wing-94.

```
(host) [mynode]# show rrm dot11k neighbor-report ap-name r-wing-94

802.11K Neighbor Report Details
-------------------------------

Flags: S: Spectrum Management, Q: QoS, A: APSD, R: Radio Measurement

ESSID         BSSID              Channel  Reachability  Security  Authenticator  Preference
Flags
-----         -----              -------  ------------  --------  -------------  ----------  -
----
r-wing-voice  00:0b:86:6d:3e:30  165      Reachable     Same      Same           1
SR
r-wing-voice  00:0b:86:6d:3e:20  1        Reachable     Same      Same           1
SR
r-wing-data   00:0b:86:6d:3e:40  6        Reachable     Same      Same           1
SR
r-wing-data   00:0b:86:6d:4e:41  153      Reachable     Same      Same           1
SR

Num Entries:4
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show rrm dot11k transmit-stream-report station-mac

```
show rrm dot11k transmit-stream-report station-mac <mac-addr>
```

Description

This is a diagnostic option for quick verification of received transmit stream measurement reports. Displays the contents of the transmit stream measurement reports received from a client.

Syntax

Parameter	Description
`mac-addr`	MAC address of the client.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show running-config

```
show running-config
```

Description

Displays the current Mobility Master configuration, including all pending changes that are yet to be saved.

Syntax

No parameters.

Usage Guidelines

Use this command to see the complete running and pending configuration on the Mobility Master.

Example

The output of this command shows the running configuration on the controller.

```
(host) [mynode] #show running-config
Building Configuration...

version 8.0
hostname "host"
clock timezone PST -8
!
location "Building1.floor1"
controller config 59
crypto-local pki ServerCert default-self-signed default-self-signed
crypto-local pki PublicCert master-ssh-pub-cert master-ssh-pub-cert
ip NAT pool dynamic-srcnat 0.0.0.0 0.0.0.0
ip access-list eth name2
!
ip access-list mac name
!
ip access-list eth etherypte
deny 0x0
!
ip access-list eth validuserethacl
permit any
...
...
...
snmp-server enable trap
snmp-server trap source 0.0.0.0

process monitor log
nbapi_publish
end
```

The output of this command shows the running configuration of the management server profiles.

```
(host) [mynode] #show running-config | include mgmt
Building Configuration...
interface mgmt
mgmt-server  primary-server 40.40.40.1 profile default-amp transport udp  secure
mgmt-server  primary-server 2001::2 profile default-amp transport udp  secure
mgmt-server  primary-server 10.1.1.11 profile default-amp transport udp
mgmt-server  primary-server 20.16.11.1 profile default-ale transport udp
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.1.0.0	Listed primary servers with IPv6 address.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show sapm-bucketmap

```
show sapm-bucketmap [essid <essid>]
```

Description

Displays the bucketmap information of the AP.

Syntax

Parameter	Description
essid	Enter the ESSID of the AP.

Example

The output of this command shows bucketmap information of the AP on the Mobility Master.

```
(host)[mynode](config) #show sapm-bucketmap essid Zone1TestEssid
SAPM Bucketmap
--------------
Item                  Value
----                  -----
Essid                 Zone1TestEssid
Generation Number     1
Read Timestamp        Fri Jul 1 19:46:33 2016 (2d:14h:55m:51s ago)
Stats                 GSM_ADD events=6 GSM Lookups=0 Deletes=0
UAC 0                 10.10.2.3
UAC 1                 10.10.2.4
UAC 2                 10.10.2.5
UAC 3                 10.10.2.6
Active Map [0-31]     00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03
Active Map [32-63]    00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03
Active Map [64-95]    00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03
Active Map [96-127]   00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 02 03
Active Map [128-159]  00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03 00 01 02 03
00 01 02 03 00 01 03 00
Active Map [160-191]  01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00
01 03 00 01 03 00 01 03
Active Map [192-223]  00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03 00 01 03
00 01 03 00 01 03 00 01
Active Map [224-255]  00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01
00 01 00 01 00 01 00 01
Num ESSIDs:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on managed devices.

show sapm cluster nodestate

```
show sapm cluster nodestate [verbose]
```

Description

Displays the state of the cluster nodes.

Syntax

No parameters.

Example

The output of this command shows slot details on the managed device.

```
(host)(cluster) (config)# show sapm cluster nodestate

Cluster Nodelist (Gen Num 124)
------------------------------
Index  Node IP address
-----  ---------------
1      10.17.65.35
2      10.17.65.34
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on managed devices.

show scheduler-profile

```
show scheduler-profile <map-name>
```

Description

Displays details of the scheduler profile that associates priorities to four uplink queues.

Syntax

Command	Description
`map-name`	Displays the scheduler map name.

Examples

The following example displays the priority map of the default scheduler profile.

```
(host) [mynode] #show scheduler-profile default
scheduler profile "default"
---------------------------
Queue     Weight   Priority-map
-----     ------   ------------
Queue 0   0        6 7
Queue 1   0        4 5
Queue 2   0        2 3
Queue 3   0        0 1
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master

show scp

```
show scp
```

Description

Execute this command to view the status of the SCP server functionality of the controller or managed device.

Syntax

No parameters

Example

To view if the SCP server functionality on the controller or managed device is enabled or not, execute the following command:

```
(host) [mynode] #show scp
```

Related Commands

Command	Description
service	Use this command to enable the SCP server functionality on the controller or managed device.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on controller or managed device

show serial console redirect

```
show serial console redirect
```

Description

Displays the status of Serial Console Redirect.

Examples

The following example displays the status of the serial console redirect.

```
(host) [mynode] #show serial console redirect
Serial Console Redirect : Enabled
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system.	Available in Config or Enable mode on Mobility Master

show session-acl-list

```
show session-acl-list
```

Description

Displays the list of configured session ACLs in the controller.

Syntax

No parameters.

Example

The output of this command shows the session ACLs in the controller.

```
(host)[mynode] # show session-access-list
v6-icmp-acl
allow-diskservices
control
validuser
v6-https-acl
vocera-acl
icmp-acl
v6-dhcp-acl
captiveportal
v6-dns-acl
allowall
test
sip-acl
https-acl
...
...
...
v6-http-acl
dhcp-acl
http-acl
stateful-dot1x
ap-acl
svp-acl
noe-acl
stateful-kerberos
v6-logon-control
h323-acl
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show slots

```
show slots
```

Description

Displays the list of slots in the managed device, including the status and card type.

Syntax

No parameters.

Example

The output of this command shows slot details on the managed device.

```
(host)[mynode] # show slots

Slots
------
Slot  Status   Card Type
----  ------   ---------
1     Present  A2400
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on Mobility Master and managed devices.

show snmp community

```
show snmp community
```

Description

Displays the SNMP community string details.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show snmp community

SNMP COMMUNITIES
----------------
COMMUNITY  ACCESS     VERSION
---------  ------     -------
 public    READ_ONLY  V1, V2c
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show snmp inform

```
show snmp inform
```

Description

Displays the length of SNMP inform queue.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show snmp inform stats

Inform queue size is 100

SNMP INFORM STATS
-----------------
HOST   PORT   INFORMS-INQUEUE   OVERFLOW   TOTAL INFORMS
----   ----   ---------------   --------   -------------
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show snmp trap-hosts

```
show snmp trap-hosts
```

Description

Displays the configured SNMP trap hosts.

Syntax

No parameters.

Example

The output of this command shows details of a SNMP trap host.

```
(host) # show snmp trap-hosts

SNMP TRAP HOSTS
---------------
HOST           VERSION     SECURITY NAME   PORT    TYPE   TIMEOUT   RETRY
----           -------     -------------   ----    ----   -------   -----
 10.16.14.1     SNMPv2c     public          162     Trap   N/A       N/A
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show snmp trap-list

```
show snmp trap-list
```

Description

Displays the list of SNMP traps.

Syntax

No parameters.

Example

The output of this command shows the list of SNMP traps and the status.

```
(host) # show snmp trap-list

SNMP TRAP LIST
--------------
TRAP-NAME                                 CONFIGURABLE  ENABLE-STATE
---------                                 ------------  ------------
authenticationFailure                     Yes           Enabled
coldStart                                 Yes           Enabled
linkDown                                  Yes           Enabled
linkUp                                    Yes           Enabled
warmStart                                 Yes           Enabled
wlsxAPBssidEntryChanged                   Yes           Enabled
wlsxAPEntryChanged                        Yes           Enabled
wlsxAPImpersonation                       Yes           Enabled
wlsxAPInterferenceCleared                 Yes           Enabled
wlsxAPInterferenceDetected                Yes           Enabled
wlsxAPRadioAttributesChanged              Yes           Enabled
wlsxAPRadioEntryChanged                   Yes           Enabled
wlsxAccessPointIsDown                     Yes           Enabled
wlsxAccessPointIsUp                       Yes           Enabled
wlsxAdhocNetwork                          Yes           Enabled
wlsxAdhocNetworkBridgeDetected            Yes           Enabled
wlsxAdhocNetworkBridgeDetectedAP          Yes           Enabled
...
...
...
...
wlsxFanOK                                 Yes           Enabled
wlsxFanTrayInserted                       Yes           Enabled
--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show snmp trap-queue

```
show snmp trap-queue
```

Description

Displays the list of SNMP traps in queue.

Syntax

No parameters.

Example

The output of this command shows the list of SNMP traps sent to host.

```
(host) # show snmp trap-queue

a)wlsxMgmtUserAuthenticationFailed
The trap indicates that a management user authentication failed.
2013-10-29 08:08:10 Management user authentication failed for user commonuser1 with IP address
10.20.102.79 usermac 00:00:00:00:00:00 server name CiscoACS-2 serverip 10.15.28.41
b)wlsxNUserAuthenticationFailed :
The trap indicates that a user authentication has failed.
2013-10-29 07:47:07 User Authentication failed for user commonuser1 userip 0.0.0.0 usermac
00:5f:12:00:00:00 servername CiscoACS-1 serverip 10.15.28.40 bssid 00:d2:5d:80:00:08 apname
v5rapsim_000_000
c)wlsxNAuthServerReqTimeOut:
The trap indicates that the authentication server req timeout
2013-10-29 07:44:58 Authentication request timed out for server CiscoACS-1 serveip 10.15.28.4
username commonuser1 userip 0.0.0.0 usermac 00:5f:12:00:00:00 bssid 00:d2:5d:80:00:08 apname
v5rapsim_000_000
d)wlsxNAuthServerTimeOut :
The trap indicates the server taken out of service.
2013-10-29 07:45:48 Authentication server CiscoACS-1 serverip 10.15.28.4  timed out. Time out
value is 1383012948 for user commonuser1 ip 0.0.0.0 mac 00:5f:12:00:00:00 bssid
00:d2:5d:80:00:08 apname v5rapsim_000_000
e)wlsNAuthServerIsDown
The trap indicates that an authentication server is down.
2013-10-29 07:44:11 Authentication Server CiscoACS-1 with ip 10.15.28.4 is down.
f)wlsNAuthServerUp
The trap indicates that an authentication server is up.
2013-10-29 07:45:48 Authentication server CiscoACS-1 with ip 10.15.28.4 is up
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show snmp user-table

```
show snmp user-table [user <username> auth-prot [sha | md5] <value> priv-prot [aes | des]
<value>]
```

Description

Displays the list of SNMP user profile for a specified username.

Syntax

Parameter	Description
`auth-prot`	Authentication protocol for the user, either HMAC-MD5-98 Digest Authentication Protocol (MD5) or HMAC-SHA-98 Digest Authentication Protocol (SHA), and the password for use with the designated protocol.
`priv-prot`	Privacy protocol for the user, either AES or CBC-DES, and the password for use with the designated protocol.

Example

The output of this command shows the list of SNMP traps sent to host.

```
(host) # show snmp user-table

SNMP USER TABLE
---------------
USER     AUTHPROTOCOL  PRIVACYPROTOCOL  FLAGS
----     ------------  ---------------  -----
 Sam     SHA           AES
 fire    SHA           AES
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show spanning-tree

```
show spanning-tree
   <interface [gigabitethernet <slot/module/port> | port-channel id]
   <vlan vlan-id>
```

Description

View the RSTP and PVST+ configuration.

Syntax

Parameter	Description
interface	Enter the keyword **interface** followed by the interface and slot/module/port or port-channel id: ■ For Gigabit Ethernet enter the keyword **gigabitethernet** followed by the <slot/module/port> ■ For Port Channel enter the keyword **port-channel** followed by an id number Range: 0 to 7
vlan	Enter the keyword **vlan** follow by the VLAN ID. Range: 1 to 4094 Default: 1

Example—show spanning-tree

```
(host) # show spanning-tree

Spanning tree instance for vlan 10
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 2 days, 0 hours, 31 mins, 21 secs

Spanning tree instance for vlan 20
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 3 hello 2, max age 20, forward delay 15
Timers: hello 0, notification 0
Last topology change: 1 days, 0 hours, 3 mins, 2 secs
```

Example—show spanning-tree vlan

```
(host) # show spanning-tree vlan 2
Spanning Tree is executing the IEEE compatible Rapid Spanning Tree protocol
Bridge Identifier has priority 32768, address 00:0b:86:f0:20:00
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag is not set, detected flag not set, changes 1
Times: hold 1, topology change 35 hello 2, max age 20, forward delay 15
```

```
Timers: hello 0, notification 0
Last topology change: 2 days, 0 hours, 31 mins, 21 secs
```

Example—show spanning-tree interface gigabitethernet

```
(host) (config-if)#show spanning-tree interface gigabitethernet 0/0/1

Interface FE 1/1 (port 2) in Spanning tree is FORWARDING
Port path cost 19, Port priority 128 Role DISNIGNATED
PortFast DISABLED P-to-P ENABLED
Designated root has priority 0 address 00:01:e8:d5:a3:6d
Designated bridge has priority 32768 address 00:0b:86:50:58:30
Designated port is 2, path cost 0
Timers:  message age 0, forward delay 20, hold 0
Counts:  BPDUs received 0, sent 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show spantree

```
show spantree
   <blocking> | <enable> | <forwarding> | <off> | <vlan>
```

Description

View the global RSTP and PVST+ topology.

Syntax

Parameter	Description
blocking	View the spanning tree ports in the Blocking state.
enable	View the spanning tree ports in the Enable state.
forwarding	View the spanning tree ports in the Forwarding state.
off	View the ports with spanning tree disabled
vlan	View the spanning tree instance for the VLAN.

Example

```
(host) # show spantree

Spanning tree instance    vlan 1
Designated Root MAC       00:0b:86:6b:57:80
Designated Root Priority  32768
Root Cost                 20000
Root Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Bridge MAC                00:1a:1e:00:89:b8
Bridge Priority           32768
Configured Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Rapid Spanning Tree port configuration
--------------------------------------
Port      State       Cost     Prio  PortFast  BpduGuard  P-to-P  Role
----      -----       ----     ----  --------  ---------  ------  ----
GE 0/0/0  Forwarding  20000    128   Disable   Disable    Enable  Root
GE 0/0/1  Discarding  20000    128   Disable   Disable    Enable  Disabled
GE 0/0/2  Discarding  2000     128   Disable   Disable    Enable  Disabled
GE 0/0/3  Discarding  2000     128   Disable   Disable    Enable  Disabled
GE 0/0/4  Discarding  2000     128   Disable   Enable     Enable  Disabled
GE 0/0/5  Discarding  2000     128   Disable   Disable    Enable  Disabled
Pc 0      Discarding  2000000  128   Disable   Disable    Enable  Disabled
Pc 1      Discarding  2000000  128   Disable   Disable    Enable  Disabled
Pc 2      Discarding  2000000  128   Disable   Disable    Enable  Disabled
Pc 3      Discarding  2000000  128   Disable   Disable    Enable  Disabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show ssh

```
show ssh
```

Description

Displays the SSH configuration details.

Syntax

No parameters.

Example

The output of this command shows SSH configuration details.

```
(host) # show ssh
SSH Settings:
-------------
DSA Enabled
Mgmt User Authentication Method username/password public-key
Ciphers aes128-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha1,hmac-sha1-96
(shash_65.100) #
(shash_65.100) #show running-config | include ssh
ssh disable-ciphers aes-cbc
ssh disable-mac hmac-sha1-96
```

Related Commands

Command	Description
ssh	Configures SSH access to a Mobility Master.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.3.0.0	The **ssh disable-ciphers** and **ssh disable-mac** parameters were introduced to the output of this command.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show sso idp-profile

```
show sso idp-profile
```

Description

Displays all SSO IDP profiles.

Syntax

No parameters.

Example

The output of this command lists all SSO IDP profiles on the controller.

```
((host) (config) #show sso idp-profile
SSO Profile List
----------------
Name         References  Profile Status
----         ----------  --------------
sso-example 0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show startup-config

```
show startup-config
```

Description

Displays the configuration which will be used the next time the controller is rebooted. It contains all the options last saved using the write memory command. Any unsaved changes are not included.

Syntax

No parameters.

Example

The output of this command shows slot details on the controller.

```
(host) # show startup-config

version 3.4
enable secret "608265290155fb924578f15b12670a75a37045cbdf62fb0d3a"
telnet cli
telnet soe
loginsession timeout 30
hostname "FirstFloor2400"
clock timezone PST -8
location "Building1.floor1"
mms config 0
controller config 22

ip access-list eth validuserethacl
  permit any
!
netservice svc-snmp-trap udp 162
netservice svc-dhcp udp 67 68
netservice svc-smb-tcp tcp 445
netservice svc-https tcp 443
netservice svc-ike udp 500
netservice svc-l2tp udp 1701
netservice svc-syslog udp 514
...
...
...
netservice svc-msrpc-udp udp 135 139
netservice svc-ssh tcp 22
netservice svc-http-proxy1 tcp 3128
--More-- (q) quit (u) pageup (/) search (n) repeat
```

Command History

This command was available in ArubaOS 3.0

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Available in Enable and Config modes on Mobility Master and managed devices.

show station-table

```
show station-table [mac <mac_address> | verbose ]
```

Description

Displays the internal station table entries and also details of a station table entry.

Syntax

Parameter	Description
`mac <mac_address>`	Displays the details of the AP that matches the specified MAC address.
`verbose`	Displays the details of all the APs in a table format.

Example

The output of this command shows details of an entry in the station table.

```
(host) # show station-table mac 00:1f:6c:7a:d4:fd

Association Table
-----------------
     BSSID              IP         Essid   AP name  Phy  Age
---------------    -----------   -------  -------  ---  ---
00:0b:86:6d:3e:30  10.15.20.252  sam      -        a    01:03:41
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show stm

```
show stm
   aruba-deauth-reasons
   mon-update-queue {stats | threshold}
```

Description

This command is used to display the deauthentication reasons and the monitoring update queue information from the station management module.

Syntax

Parameter	Description
aruba-deauth-reasons	Displays the Aruba deauthentication reasons
mon-update-queue	Displays the STM monitoring update queue information
stats	Displays the STM update queue statistics
threshold	Displays the STM monitoring update queue threshold

Example

The following command displays the STM deauthentication reasons:

```
(host) [mynode] #show stm aruba-deauth-reasons
   Aruba Deauth Reasons
   --------------------
   Code  Reason
   ----  ------
   1     Unspecified Failure
   2     Prior authentication is not valid
   3     STA has left and is deauthenticated
   4     Inactive Timer expired and STA was disassociated
   5     Disassociated due to insufficient resources at AP
   6     Class 2 frames from non authenticated STA
   7     Class 3 frames from non associated STA
   8     STA has left and is disassociated
   9     STA Requesting Association without authentication
   ...
   ...
   ..
```

The following command displays the STM monitoring queue update statistics:

```
(host) [mynode] #show stm mon-update-queue stats
   (host) [mynode] #show stm mon-update-queue stats
   Stm mon update queue statistics
   Mon queue size:0
   AP Devices Queued
   -----------------
   Add  Info Update  Delete  Stats Update
   ---  -----------  ------  ------------
   0    0            0       0
   AP Devices Dropped
   ------------------
   Add  Info Update  Delete  Stats Update
   ---  -----------  ------  ------------
```

```
0    0            0       0
RADIO Devices Queued
--------------------
Add  Info Update  Delete  Stats Update
---  -----------  ------  ------------
0    0            0       0
...
...
```

The following command displays the monitoring update queue threshold value:

```
(host) [mynode] #show stm mon-update-queue threshold
  Stm mon udpate queue limit:83328
```

Related Commands

Command	Description
stm	This command is used to manually disconnect a client from an AP or control the blacklisting of clients.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config or Enable mode on Mobility Master.

show storage

```
show storage
```

Description

Displays the storage information on the controller.

Syntax

No parameters.

Example

The output of this command shows the storage details on the controller.

```
(host) # show storage
Filesystem                Size      Used Available Use% Mounted on
/dev/root                57.0M     54.6M      2.3M  96% /
none                     70.0M      2.0M     68.0M   3% /tmp
/dev/hda3               149.7M      9.3M    132.6M   7% /flash
/dev/usb/flash3           1.5G    168.6M      1.3G  12% /flash
/dev/usbdisk/2            3.5G     71.4M      3.2G   2% /mnt/usbdisk/2
/dev/usbdisk/1            3.9G    131.0M      3.8G   3% /mnt/usbdisk/1
```

The number at the end of the USB device's name is the partition. Unlike the controller's flash, the USB device has more than two partitions; not just 0 and 1. When copying a file from a USB device, you must know which partition the target file is on.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show switch ip

```
show switch ip
```

Description

Displays the IP address of the controller and VLAN ID.

Syntax

No parameters.

Example

The output of this command shows the IP address and VLAN ID of the controller.

```
(host) # show switch ip

Switch IP Address: 10.16.15.1

Switch IP is from Vlan Interface: 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show switch software

```
show switch software
```

Description

Displays the details of the software running in the controller.

Syntax

No parameters.

Example

The output of this command shows the details of software running in the controller.

```
(host) # show switch software

Aruba Operating System Software.
ArubaOS (MODEL: Aruba6000-US), Version 6.2.0.0
Website: http://www.arubanetworks.com
Copyright (c) 2002-2012, Aruba Networks, Inc.
Compiled on 2012-11-28 at 23:35:56 PST (build 36322) by p4build
ROM: System Bootstrap, Version CPBoot 1.3.0.1 (build 28907)
Built: 2011-06-24 13:46:21
Built by: p4build@re_client_28907
Switch uptime is 15 hours 11 minutes 48 seconds
Reboot Cause: Datapath timeout.
Supervisor Card
Processor XLR 732 (revision C4) with 2015M bytes of memory.
32K bytes of non-volatile configuration memory.
512M bytes of Supervisor Card System flash (model=CF 512MB).
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show switches

```
show switches [all | regulatory | state {complete | incomplete | inprogress | required} |
summary ]
```

Description

Displays the details of managed device connected to the Mobility Master, including the Mobility Master itself.

Syntax

Parameter	Description
`all`	List of all managed devices.
`regulatory`	Displays information about the currently active regulatory file.
`state`	Configuration status of all managed devices.
`summary`	Status of all managed devices connected to the Mobility Master.

Example

The output of this command shows that there is a single managed device connected to the Mobility Master.

```
(host) # show switches all
All Switches
------------
IP Address  Name         Location          Type    Version        Status  Configuration State
Config Sync Time (sec)
----------  ----         --------          ----    -------        ------  -------------------
----------------------
10.16.12.1  r-wing-94    Building1.floor1  master  6.0.0.0_13782  up      UPDATE SUCCESSFUL
0192.0.2.12  CorpA2400    Building1.floor1  master  6.0.0.0_13782  up      UPDATE SUCCESSFUL
 0
```

Execute the **show switches regulatory** command to check if the regulatory file is active on the managed device.

```
(host) #show switches regulatory

All Switches
------------
IP Address    Name  Location          Type    Model      File Version    File Build
----------    ----  --------          ----    -----      ------------    ----------
172.16.0.254  host  Building1.floor1  master  7210       1.0_43859       21/4/2014
```

Execute the **show switches state complete** command to check the progress of the configuration update.

```
(host)[mynode] #show switches state [incomplete|incomplete|inprogress|required]
(host) [mynode] (config) #show switches state complete
All Switches
------------
IP Address  IPv6 Address  Name             Location          Type  Model         Version

----------  ------------  ----             --------          ----  -----         -------

1.1.1.1     2002::1       abhi_vmc_61.122  Building1.floor1  LC    VMC-TACTICAL  8.0.0.0-svcs-
ctrl_0000
```

```
Status       Configuration State  Config Sync Time (sec)  Config ID
----------  --------------------  ----------------------  ---------
up          UPDATE SUCCESSFUL    0                       22
Total Switches:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show switchinfo

```
show switchinfo
```

Description

Displays the latest and complete summary of managed device details including role, last configuration change, hostname, reason for last reboot.

Syntax

No parameters.

Example

The output of this command lists all managed devices connected to Mobility Master including the Mobility Master server.

```
(host) # show switchinfo
Hostname is Techpubs
Console Baudrate: 115200
Location not configured
System Time:Tue Nov 27 16:22:14 PST 2012
            Aruba Operating System Software.

            ArubaOS (MODEL: Aruba7220-US), Version 6.2.0.0
            Website: http://www.arubanetworks.com
            Copyright (c) 2002-2012, Aruba Networks, Inc.

Compiled on 2012-11-26 at 17:06:31 PST (build 36290) by p4build
ROM: System Bootstrap, Version CPBoot 1.2.0.9 (build 35873)
Built: 2012-10-24 13:51:09
Built by: p4build@re_client_35873
Switch uptime is 9 hours 34 minutes 3 seconds
Reboot Cause: User reboot.
Built: 2012-10-24 13:51:0
Built by: p4build@re_client_35873

Internet address is 172.16.0.254  255.255.255.0
Routing interface is enable, Forwarding mode is enable
Directed broadcast is disabled
Encapsulation 802, loopback not set
Last clearing of "show interface" counters 0 day 9 hr 34 min 3 sec
link status last changed 0 day 9 hr 34 min 3 sec
Proxy Arp is disabled for the Interface
switchrole:master
Configuration unchanged since last save
Crash information available.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show syscontact

```
show syscontact
```

Description

Displays the contact information for support.

Syntax

No parameters.

Example

The output of this command shows the contact information for technical support.

```
(host) # show syscontact

admin@mycompany.com
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show syslocation

```
show syslocation
```

Description

Displays the location details of the controller.

Syntax

No parameters.

Example

The output of this command location of the controller.

```
(host) # show syslocation

Building 1, Floor 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show tech-support

```
show tech-support
<filename>
user
```

Description

Displays all information about the controller required for technical support purposes.

Syntax

Parameter	Description
`<filename>`	Stores the output in specified file name. Maximum length of the file name is 127 characters
`user`	Run a user specific tech-support command.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show telnet

```
show telnet
```

Description

Displays the status of telnet access using the CLI or Serial over Ethernet (SOE) to the controller.

Syntax

No parameters.

Example

The output of this command shows the status of CLI and SOE access to the controller.

```
(host) # show telnet

telnet cli is enabled
telnet soe is enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show threshold

```
show threshold
   all|controlpath-cpu|controlpath-memory|datapath-cpu|
   no-of-aps|no-of-locals|total-tunnel-capacity|user-capacity|
```

Description

This command shows managed device capacity thresholds which, when exceeded, will trigger alerts.

Syntax

Parameter	Description
`all`	Display all alert thresholds.
`controlpath-cpu`	Display the alert threshold for controlpath CPU capacity. The output of this command shows the percentage of the total controlpath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 45%.
`controlpath-memory`	Display the alert threshold for controlpath memory consumption. The output of this command shows the percentage of the total memory capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 85%.
`datapath-cpu`	Display the alert threshold for datapath CPU capacity. The output of this command shows the percentage of the total datapath CPU capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 30%.
`no-of-APs`	The maximum number of APs that can be connected to a managed device is determined by that managed device's model type and installed licenses. This threshold triggers an alert when the number of APs currently connected to the managed device exceeds a specific percentage of its total AP capacity. The default threshold for this parameter is 80%.
`no-of-locals`	Display the alert threshold for Mobility Master's capacity to support managed devices. Mobility Master can support a combined total of 256 managed devices. The output of this command shows the percentage of the total Mobility Master capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.
`total-tunnel-capacity`	Display the alert threshold for the managed device's tunnel capacity. The output of this command shows the percentage of the managed device's total tunnel capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%
`user-capacity`	Display the alert threshold for the managed device's user capacity. The output of this command shows the percentage of the total resource capacity that must be exceeded before the alert is sent. The default threshold for this parameter is 80%.

Usage Guidelines

The managed device will send a *wlsxThresholdAbove* SNMP trap and a syslog error message when the managed device has exceeded a set percentage of the total capacity for that resource. A *wlsxThresholdBelow* SNMP trap

and error message will be triggered if the resource usage drops below the threshold once again.

Example

```
(host) (config) #show threshold all
Controller Capacity Threshold Values
------------------------------------
RESOURCE                THRESHOLD(%)
--------                ------------
Datapath-Cpu            30 %
Controlpath-Cpu         80 %
Controlpath-Memory      85 %
Total-Tunnel-Capacity   80 %
Ap-Tunnel-Capacity      80 %
User-Capacity           80 %
No-of-APs               80 %
No-of-locals            80 %
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show threshold-limits

```
show threshold-limits
   controlpath-memory|fan-speed|no-of-aps|no-of-locals|total-tunnel-capacity|user-capacity
```

Description

This command shows current values of the different resources monitored by the managed device.

Syntax

Parameter	Description
`controlpath-memory`	The output of this command displays the default memory threshold which, when exceeded, will trigger an alert, the current configured threshold, the total memory (in MB) and the currently available memory (in MB).
`fan-speed`	The output of this command displays the fan alert threshold. This parameter is only available for managed devices with fans, such as the 7200 Series.
`no-of-aps`	The output of this command displays the following values: ■ The default threshold for the number of APs, which, when exceeded, will trigger an alert ■ The current configured threshold. ■ The maximum number of APs supported by the managed device, ■ The number of available licenses for campus and remote APs, ■ The total number of APs, and the current number of campus, remote and virtual APs.
`no-of-locals`	The output of this command displays the default threshold for the number of managed devices which, when exceeded, will trigger an alert, and the current configured threshold. The output also displays the maximum number of managed devices that can be connected to this Mobility Master, and the number of managed devices currently connected.
`total-tunnel-capacity`	The output of this command displays the default tunnel capacity threshold which, when exceeded, will trigger an alert, as well as the current configured tunnel threshold. The output also includes the maximum number of tunnels supported by the managed device, as well as the number of tunnels currently used by the managed device.
`user-capacity`	The output of this command displays the default user capacity threshold which, when exceeded, will trigger an alert, as well as the current configured user threshold. The output also includes the maximum number of users supported by the managed device, as well as the number of users currently associated with the managed device.

Usage Guidelines

The managed device will send a *wlsxThresholdAbove* SNMP trap and a syslog error message when the managed device has exceeded a set percentage of the total capacity for that resource. A *wlsxThresholdBelow* SNMP trap and error message will be triggered if the resource usage drops below the threshold once again.

Example

The following command shows the current alert thresholds for controlpath memory resources:

```
[host](node)(config) #show threshold-limits controlpath-memory
```

```
Threshold Values For Controlpath Memory
---------------------------------------
Default(%)  Current(%)  Total Memory (MB)  Available Memory (MB)
----------  ----------  -----------------  ---------------------
85                  77                679                    225
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show time-range

```
show time-range [<name>|summary]
```

Description

Displays the list of time range configured in the system and rules affected by the time range.

Syntax

No parameters.

Example

The output of this command shows the absolute time range details.

```
(host) # show time-range

Time-Range monitoring, Absolute
-------------------------------
StartDate  Start-time  EndDate    End-time  Applied
---------  ----------  -------    --------  -------
4/29/2009  23:00       4/30/2009  12:00     No
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show timer debug statistics app-name

```
show ipc statistics app-name <name>
```

Description

Displaytimer debugging statistics for a specific application.

Syntax

Parameter	Description	
`<name>`	One of the following application names: ■ **aaa**: Administrator Authentication ■ **ads**: Anomaly Detection ■ **authmgr**: User Authentication ■ **certmgr**: Certificate Manager ■ **cfgm**: Config Manager ■ **cpsec**: Control-Plane Security Manager ■ **cts**: Transport Service ■ **dbsync**: Database Synchronization ■ **dhcp**: DHCP Server ■ **esi**: Server Load Balancing ■ **fpapps**: Layer 2,3 control ■ **ha_mgr**: HA manager ■ **httpd**: HTTPD ■ **ike**: IKE Daemon ■ **l2tp**: L2TP ■ **licensemgr**: License Manager ■ **mdns**: AirGroup mdns ■ **mobileip**: Mobile IP	■ **ntp**: NTP Daemon ■ **ospf**: OSPF ■ **pim**: Protocol Independent Multicast ■ **pktfilter**: Packet Filter ■ **pptp**: PPTP ■ **profmgr**: Profile Manager ■ **publisher**: Publish subscribe service ■ **resolver**: Resolver ■ **snmp**: SNMP agent ■ **stm**: Station Management ■ **syslogd**: Syslog Manager ■ **userdb**: User Database Server ■ **wms**: Wireless Management

Example

The following example shows IPC statistics for the **STM** process.

```
(host) #show timer debug statistics app-name stm

Granularity=100
Wheel Size=512
Tick Count=5744522
Spoke Index=394
Active timers=21
Expired timers=886374
Hiwater mark=49
Started timers=109893
Cancelled timers=4425
Timer info
SI      TV      RC      Recurring       RT      Callback        FN
0     3600000 30      Yes             1575400 0x2ad41c84      PAPI_Init_Prio:1245
0     3600000 30      Yes             1575400 0x2ad4a200      PAPI_Init_Prio:1249
0     3600000 30      Yes             1575400 0x2ad41c84      PAPI_Init_Prio:1245
0     3600000 30      Yes             1575400 0x2ad4a200      PAPI_Init_Prio:1249
0     3600000 30      Yes             1575400 0x2ad41c84      PAPI_Init_Prio:1245
0     3600000 30      Yes             1575400 0x2ad4a200      PAPI_Init_Prio:1249
0     3600000 30      Yes             1575400 0x2ad41c84      PAPI_Init_Prio:1245
0     3600000 30      Yes             1575400 0x2ad4a200      PAPI_Init_Prio:1249
```

```
0      3600000 30      Yes             1575400 0x2ad41c84      PAPI_Init_Prio:1245
0      3600000 30      Yes             1575400 0x2ad4a200      PAPI_Init_Prio:1249
360    300000  0       Yes             3400    0x57d564        sapm_ap_mgmt_init:831
360    60000   0       Yes             3400    0x46942c        addservicetomonitor:169
360    60000   0       Yes             3400    0x2b230730      Nanny_Start_Processing:98
360    60000   0       Yes             3400    0x54e8a4        voip_ucm_init:255
380    60000   0       No              1400    0x646fb8        mon_mgr_set_coll_stats_timer:48
402    1000    0       Yes             800     0x42a068        main:1104
410    300000  1       Yes             52800   0x5b599c        sapm_gap_read_db:3409
422    5000    0       Yes             2800    0x2b2544a0      boc_licusage_init:115
447    8085    0       No              5300    0x478660        mux_heartbeat:1017
472    10000   0       Yes             7800    0x41ce70        wifi_auth_reg_timer_init:7539
492    60000   0       No              9800    0x42a820        stm_set_net_stats_update_timer:
SI: Spoke Index TV: Timer Value RC: Rotation Count
RT: Remaining Time      FN: Function:Line Number
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show trunk

```
show trunk
```

Description

Displays the list of trunk ports on the controller.

Syntax

No parameters.

Example

The output of this command shows details of a trunk port.

```
(host) # show trunk

Trunk Port Table
-----------------
Port    Vlans Allowed                          Vlans Active                           Native
Vlan
----    -------------                          ------------                           --------
---
FE2/12  1,613,615-617,632-633,636-640,667-668  1,613,615-617,632-633,636-640,667-668  1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show tunnel-group

```
show tunnel-group <tunnel-group-name>
```

Description

Displays the operational status of the tunnel-groups configured on the controller.

Syntax

Parameter	Description
`<tunnel-group-name>`	Displays the operational status of the specified tunnel-group.

Example

The output of this command shows the status of the configured tunnel-groups:

```
(host) #show tunnel-group

Tunnel-Group Table Entries
--------------------------
Tunnel Group Type Tunnel Group Id Preemptive Failover  Active Tunnel Id Tunnel Members
------------ ---- --------------- -------------------- ---------------- --------------
tgroup1      L3   16385           enabled              10               10 20
tgroup2      L2   16387           enabled              10               10 20 40
```

The output of the following command shows the status of the specified tunnel-group:

```
(host) #show tunnel-group tgroup1

Tunnel-Group Table Entries
--------------------------
Tunnel Group Type Tunnel Group Id Preemptive Failover  Active Tunnel Id Tunnel Members
------------ ---- --------------- -------------------- ---------------- --------------
tgroup1      L3   16385           enabled              10               10 20
```

The output of the following command shows the datapath Tunnel-Group table entries:

```
(host) #show datapath tunnel-group

Datapath Tunnel-Group Table Entries
-----------------------------------
Tunnel-Group Active Tunnel Members
------------ ------------- ---------
16385        10            10 20
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show tunneled-node

```
show tunneled-node {config|state|database}
```

Description

Displays the wired tunneled node configuration details, the state of the tunneled node, and lists all the tunneled nodes in the database.

Syntax

Parameter	Description
`config`	Displays the wired tunneled node configuration details.
`state`	Displays the state of the tunneled node.
`database`	Displays all the tunneled nodes in the database.

Example

The output of this command shows the tunneled node state.

```
(host) [mynode]# show tunneled-node state

Tunneled Node State
---------
IP MAC s/p state vlan tunnel inactive-time
-- --- --- ----- ---- ------ -------------
192.168.123.14 00:0b:86:40:32:40 1/23 complete 10 9 1
192.168.123.14 00:0b:86:40:32:40 1/22 complete 10 10 1
192.168.123.14 00:0b:86:40:32:40 1/20 complete 10 11 1
```

On the tunneled node client:

```
(host) #show tunneled-node state
Tunneled Node State
-------------------
IP              MAC               s/p   state     vlan  tunnel  inactive-time
--              ---               ---   -----     ----  ------  -------------
192.168.123.16  00:0b:86:40:32:40  1/23  complete  10    21      0
192.168.123.16  00:0b:86:40:32:40  1/22  complete  10    9       0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show tunneled-node-mgr

```
show tunneled-node-mgr
```

Description

Displays the tunneled node configuration details, the state of the tunneled node, and lists all the tunneled nodes in the database.

Syntax

Parameter	Description
`cluster-bucket-map`	Displays the cluster bucket map details.
`cluster-node-list`	Displays the cluster node list information.
`gsm-counters`	Displays the GSM counters details.
`node-heartbeat-table`	Displays node heartbeat table related information.
`stats`	Displays the tunneled node manager statistics.
`trace-buf`	Displays contents of trace buffer.
`tunnel-vlan-user-map`	Displays Information on user count on each Tunnel VLAN pair.
`tunneled-nodes`	Displays all the information on tunneled nodes.
`tunneled-users`	Displays all the information on tunneled users.
`user-tunnel-table`	Displays i Information on user tunnel tables.

Example

You can use the following show command to check if the Per-User Tunnel Node is configured and is working as expected

```
(host) [mynode]# show tunneled-node-mgr stats

  Message stats
  -------------------------------------------------------------------------------------------------
  --
  Switch bootstrap
  ----------------
  switch_bootstrap_req: 2
  switch_bootstrap_req_fail_mandatory_param_absent: 0
  switch_bootstrap_req_fail_invalid_key: 0
  switch_bootstrap_req_fail_actv_req_on_stby_ctrl: 0
  switch_bootstrap_req_fail_stby_req_on_actv_ctrl: 0
  switch_bootstrap_req_fail_not_actv_or_stby: 0
  switch_bootstrap_req_fail_hbt_tunnel_creation_fail: 0
  switch_bootstrap_req_fail_wait_for_license_response: 1
  switch_bootstrap_req_fail_license_not_received: 0
  switch_bootstrap_req_fail_platform_limit_reached: 0
  switch_bootstrap_ack_fail_bmap_not_present: 0
  switch_bootstrap_ack: 1
  switch_bootstrap_nack: 0
```

```
Switch unbootstrap
------------------
switch_unbootstrap_msg: 0
switch_unbootstrap_msg_fail_switch_not_found: 0
switch_unbootstrap_msg_fail_not_actv_or_stby: 0
switch_unbootstrap_ack: 0
switch_unbootstrap_nack: 0

Switch failover
------------------
switch_failover_msg: 0
switch_failover_msg_fail_mandatory_param_absent: 0
switch_failover_msg_fail_switch_not_found: 0
switch_failover_msg_fail_switch_actv: 0
switch_failover_msg_fail_ctrl_not_stby: 0
switch_failover_ack: 0
switch_failover_nack: 0

User bootstrap
------------------
user_bootstrap_req: 3
user_bootstrap_req_fail_mandatory_param_absent: 0
user_bootstrap_mac_move_switch_mac_differs: 0
user_bootstrap_mac_move_user_key_differs: 0
user_bootstrap_req_fail_invalid_key: 0
user_bootstrap_req_fail_bmap_mismatch: 0
user_bootstrap_req_fail_tunnel_creation_fail: 0
user_bootstrap_req_fail_auth_entry_creation_fail: 0
user_bootstrap_ack: 3
user_bootstrap_nack: 0

User unbootstrap
------------------
user_unbootstrap_msg: 1
user_unbootstrap_msg_fail_mandatory_param_absent: 0
user_unbootstrap_msg_fail_switch_mismatch: 0
user_unbootstrap_msg_fail_key_mismatch: 0
user_unbootstrap_msg_fail_user_not_found: 0
user_unbootstrap_msg_fail_switch_not_found: 0
user_unbootstrap_ack: 1
user_unbootstrap_nack: 0

Switch keepalive
------------------
switch_keep_alive: 0
switch_keep_alive_fail_switch_not_found: 0
switch_keep_alive_ack: 0
switch_keep_alive_nack: 0

Nodelist message
------------------
node_list_send_fail_switch_bootstrap_not_acked: 0
node_list_send_fail_switch_max_attempt: 0
node_list_message: 4
node_list_ack_switch_not_found: 0
node_list_ack_invalid_seq_num: 0
node_list_ack: 4
node_list_resend: 0

Bucketmap message
------------------
```

```
bucket_map_send_fail_switch_bootstrap_not_acked: 1
bucket_map_send_fail_switch_max_attempt: 0
bucket_map_message: 1
bucket_map_ack_switch_not_found: 0
bucket_map_ack_invalid_seq_num: 0
bucket_map_ack: 1
bucket_map_resend: 0

Cluster stats
-------------------------------------------------------------------------------------------------
--
Cluster object
--------------------
no_slot_for_new_node: 0
cluster_object_add: 4
cluster_object_disconnect: 6
down_node_not_found: 6
cluster_disable_events: 0

Cluster sac
--------------------
stby_sac_removements: 0
inform_switch_sac_down: 0
ignore_sby_sac_switch_not_found: 0
skip_sby_sac_on_sby: 0
sby_sac_updates_sent: 1

Bucketmap
--------------------
bmap_event_but_cluster_disabled: 0
bmap_create_events: 1
bmap_update_events: 1
bmap_errors: 0
bmap_del_mapped_dormant_sta: 0
bmap_del: 0
self_not_in_bmap: 0

User activation
--------------------
activations: 0
activation_errors: 0
sta_not_dormant: 0
uac_down_activate_bmap: 0
activation_fail_down_uac_not_in_bmap: 0
activation_fail_self_not_in_bmap: 0

User dormant creation
--------------------
sta_dormant_add_switch_not_found: 0
sta_dormant_add_sta_creation_failed: 0
sta_dormant_add_sta_add_to_bucket: 0
sta_dormant_add_tunnel_updated: 0
sta_dormant_add_tunnel_creation_failed: 0

User dormant deletion
--------------------
dormant_del: 0
dormant_del_sta_not_active: 0
dormant_del_sta_not_dormant: 0
station_not_found: 0

Add standby switch to ndoelist
```

```
-------------------
stby_sac_switch_add: 0
stby_sac_switch_del: 0

In memory
-------------------------------------------------------------------------------------------------
--
add_switch: 1
del_sta_from_sta_hash: 1
add_sta: 0
add_dormant_sta_to_switch: 0
add_sta_to_switch: 3
sta_hash_not_found_in_switch: 0
sta_removed_from_switch: 1
deauth_sta: 1
deauth_all_sta: 0
delete_switch: 0
```

Command History

Release	Modification
ArubaOS 8.1.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config modes on managed devices.

show uap-blacklist

```
show uap-blacklist [mac-address|page|start]
```

Description

This command configures a UAP blacklist database entry. You can add, delete, or modify AP MAC addresses and description to the blacklist database. If you enable the blacklist policy in the AP deploy profile, the policy is applied to the APs included in this list.

Syntax

Parameter	Description
`mac-address <name>`	Shows MAC address of the AP.
`page`	Shows specific page (50 records per page).
`start`	Shows <start> records into the database

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The following commands lists all the AP MAC addresses in the UAP blacklist table:

```
(host) [mynode] #show uap-blacklist
UAP Blacklist Details
---------------------
MAC-Address         Description
-----------         -----------
11:11:11:11:11:11   AP-test2
11:11:11:11:11:12   Ap-test1
11:11:11:11:11:01   AP-test3
```

Related Commands

Command	Description
uap-blacklist	This command allows you to create or purges the UAP blacklist database by adding, deleting, or modifying AP MAC address entries.

Command History

Release	Modification
ArubaOS8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on master Mobility Master

show ucc call-info cdrs

```
show ucc call-info cdrs
   ap <ap_name>
      [app [facetime | h323 | jabber | noe | sccp | sip | skype4b | svp | vocera | WiFi-
     Calling]]
   app
      {h323 [detail] | jabber [detail] | noe [detail] | sccp [detail] | sip [detail] | skype4b
      [detail] | svp [detail] | vocera [detail] | WiFi-Calling [detail]}
   cid <cid>
   detail
```

Description

This command displays the Call Detailed Records (CDR) statistics for Unified Communication and Collaboration (UCC).

When VoIP calls are prioritized using media classification, the **UCC Call ID**, **Client Name**, **Called to**, **Dir** (direction of the call), **End-to-End Delay(ms)/Jitter(ms)/PktLoss(%)**, **Codec**, **MOS**, and **MOS-Band** values are not available.

Syntax

Parameter	Description
`ap <ap_name>`	Displays the CDR statistics of an AP for a specific Application Layer Gateway (ALG).
`app`	Displays the CDR statistics based on a specific ALG.
`cid <cid>`	Displays CDR statistics for a specific CDR-ID.
`detail`	Displays detailed CDR statistics.

Example

The following command displays the CDR statistics:

```
(host) [mynode] #show ucc call-info cdrs

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP

CDRS:
-----
CDR ID  UCC Call ID  Client IP     Client MAC         Client Name  ALG           Dir
------  -----------  ---------     ----------         -----------  ---           ---
43      12           192.0.2.22    00:23:33:41:c8:b8  Alex         skype4b       IC
42      12           192.0.2.26    24:77:03:9a:6c:dc  John         skype4b       OG
1       NA           10.15.132.86  fc:c2:de:6c:01:9c  NA           WiFi-Calling  NA

Called to   Dur(sec)   Orig Time         Status  Reason      Call Type        Client Health
---------   --------   ---------         ------  ------      ---------        -------------
Joe         50         Jan  8 06:18:27   SUCC    Terminated  Video/Conf Call  81
Mike        50         Jan  8 06:18:27   SUCC    Terminated  Voice            82
NA          88         Jun  4 06:41:40   ACTIVE  NA          Voice            93

UCC Score[C]   UCC- Score[A]   MOS          Server(IP)
------------   -------------   ---          ----------
81.52/Good     79.18/Good      4.17/Good
79.53/Good     76.24/Good      4.15/Good
NA             NA              NA           T-Mobile
```

```
Total Entries:3
```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. **NOTE:** This column is not populated for WiFi-Calling ALG.
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client. **NOTE:** This column is not populated for WiFi-Calling ALG.
ALG	Displays the VoIP protocol used by the VoIP client.
Dir	Displays the direction of the call. Possible values are: ■ **OG**—Outgoing ■ **IC**—Incoming **NOTE:** This column is not populated for WiFi-Calling ALG.
Called to	Displays the username of the VoIP client being called. **NOTE:** This column is not populated for WiFi-Calling ALG.
Dur(sec)	Displays the duration of the VoIP call in seconds.
Orig Time	Displays the time at which the VoIP call originated.
Status	Displays the status of the VoIP call. Possible values are: ■ **SUCCESS** ■ **FAILED** ■ **ABORTED** ■ **BLOCKED** ■ **FORWARDED** ■ **ALERTING** ■ **HOLD** ■ **ACTIVE**

Column	Description
Reason	Displays the reason code for call termination. Possible values are: ■ **NA** ■ **Capacity Reached** ■ **401 unauthorized** ■ **487 request timeout** ■ **Request timeout** ■ **Request canceled** ■ **Request terminated** ■ **Session timeout** ■ **Session timer expired** ■ **Session expired - request timeout** ■ **Aborted** ■ **Terminated** ■ **Forwarded** ■ **Transferred** ■ **Inactivity** ■ **Wrong number** ■ **Peer reset** ■ **Client reset** ■ **No answer** ■ **Missed** ■ **Parked** ■ **Invalid number** ■ **Tunnel down** ■ **Moved temporarily** ■ **4xx error** ■ **5xx error** ■ **Call leg does not exist** ■ **DELTS request** ■ **TCLAS flow deleted** ■ **No reason**
Call Type	Displays the type of VoIP call or session. Possible values are: ■ **Not Available** ■ **Voice** ■ **Video** ■ **Desktop Sharing** ■ **File Transfer** ■ **Voice/Conf Call** ■ **Video/Conf Call** ■ **Desktop-Sharing/Conf Call** ■ **File-Transfer/Conf Call**
Client Health	Displays the ratio of ideal air time required for transmitting a packet from an AP to a client to the actual air time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.
UCC Score[C]	Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device. **NOTE:** This column is not populated for WiFi-Calling ALG.
UCC Score[A]	Displays the UCC score based on the quality of the voice call or desktop sharing session. This is the metric calculated at the AP. **NOTE:** This column is not populated for WiFi-Calling ALG.

Column	Description
MOS	Displays the Mean Opinion Score (MOS) of the VoIP call. **NOTE:** This column is not populated for WiFi-Calling ALG.
Server(IP)	Displays the name of the service provider for WiFi-calling ALG

The following command displays the CDR statistics for an AP.

```
(host) [mynode] #show ucc call-info cdrs ap AP225-1

CDR-AP:
-------
CDR ID  UCC Call ID  AP Name  Re-Assoc  ICH-Denied  Utilization(%)  Codec     Quality  Delay
(msec)
------  -----------  -------  --------  ----------  --------------  -----     -------  -------
----
18      7            AP225-1  0         No          37              G711      Good     0.74
17      7            AP225-1  0         No          37              G711      Fair     19.00
16      6            AP225-1  1         No          34              NA        Good     0.55

Jitter(msec)  Packet Loss(%)  Orig WMM-AC
------------  --------------  -----------
0.21          0.00            NA
0.37          14.93           0
0.05          0.00            0

Max Concurrent Calls: 3 At Jan 14 03:54:15
Total Entries:3
```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. **NOTE:** This column is not populated for WiFi-Calling ALG
AP Name	Displays the name that uniquely identifies the AP.
Re-Assoc	Displays the number of times the client re-associated while on an active call.
ICH-Denied	Displays the status of the Intelligent Call Handling (ICH). Possible values are: ■ **Yes**—Call prioritized ■ **No**—Call not prioritized
Utilization(%)	Displays the channel utilization of the AP during the call.
Codec	Displays the compression protocol used for voice and video calls, desktop sharing, or file transfer session. **NOTE:** This column is not populated for WiFi-Calling ALG

Column	Description
Quality	Displays the quality of the VoIP call based on the UCC score. Possible values are: ■ **Good** ■ **Fair** ■ **Poor** ■ **NA** **NOTE:** This column is not populated for WiFi-Calling ALG.
Delay(msec)	Displays the average delay in milliseconds. **NOTE:** This column is not populated for WiFi-Calling ALG.
Jitter(msec)	Displays the average jitter in milliseconds. **NOTE:** This column is not populated for WiFi-Calling ALG.
Packet Loss(%)	Displays the loss of packet in percentage. **NOTE:** This column is not populated for WiFi-Calling ALG.
Orig WMM-AC	Displays the original client value of the Wi-Fi Multimedia Access Category.

The following command displays detailed CDR statistics.

```
(host) [mynode] #show ucc call-info cdrs detail

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP
      [E] - Metric calculated End-to-End
       D - Delay in milliseconds
       J - Jitter in milliseconds
       PL - Packet Loss in percent

CDR-Detail:
------------
CDR ID  UCC Call ID  AP Name  Re-Assoc  UCC Score[C]  D(ms)/J(ms)/PL(%)[C]
------  -----------  -------  --------  ---------     --------------------
29      11           AP135-1  0         82.70         0.57/0.01/0.42
22      9            AP135-1  0         83.93         0.30/0.00/0.00
21      9            AP135-1  0         85.07         0.33/0.00/0.64

UCC Score[A] D(ms)/J(ms)/PL(%)[A] SNR  Avg Tx Rate(Mbps)  Tx Drop(%)  Tx Retry(%)
------------ -------------------- ---  -----------------  ----------  -----------
81.34        0.68/0.01/0.53       48   45.19              0.27        23.99
82.01        0.45/0.00/0.10       46   532.39             0.00        1.42
84.76        0.52/0.00/0.79       53   58.79              57.52       10.30

Avg Rx Rate(Mbps)  Rx Retry(%)  MOS   D(ms)/J(ms)/PL(%)[E]  Controller-IP
-----------------  -----------  ---   --------------------  -------------
53.70                           3.50  12.58/05.70/05.16     192.0.2.1
355.00             0.01         2.64  10.16/03.81/03.24     192.0.2.1
107.92             0.01         4.07  11.24/04.92/04.18     192.0.2.1

Total Entries:3
```

The output of this command includes the following information:

Column	Description
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session. **NOTE:** This column is not populated for WiFi-Calling ALG.
AP Name	Displays the name that uniquely identifies the AP.
Re-Assoc	Displays the number of times the client re-associated while on an active call.
UCC Score[C]	Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.
D(ms)/J(ms)/PL(%)[C]	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the managed device.
UCC Score[A]	Displays the UCC score based on the quality of the voice call or desktop sharing. This is the metric calculated at the AP. **NOTE:** This column is not populated for WiFi-Calling ALG.
D(ms)/J(ms)/PL(%)[A]	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the AP.
SNR	Displays the Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
Avg Tx Rate(Mbps)	Displays the average transmission rate in Mbps.
Tx Drop(%)	Displays the transmission packet drop in percentage.
Tx Retry(%)	Displays the transmission retry in percentage.
Avg Rx Rate(Mbps)	Displays the average receive rate in Mbps.
Rx Retry(%)	Displays the receive retry in percentage.
MOS	Displays the MOS value of the VoIP call. This is an end-to-end score (wired and wireless) of the VoIP call. **NOTE:** This column is not populated for WiFi-Calling ALG.
D(ms)/J(ms)/PL(%)[E	Displays the end-to-end delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This field takes the wired and wireless network QoS parameters into consideration.
Controller-IP	Displays the IP address of the managed device.

Command History

Release	Modification
ArubaOS 8.2.0.0	Column **Server(IP)** is added to output of command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc client-info

```
show ucc client-info
   app
      {h323 [detail]|jabber [detail]|noe [detail]|sccp [detail]|sip [detail]|skype4b [detail]
      |svp [detail] | vocera [detail]|WiFi-Calling [detail]}
   detail
   sta <mac>
```

Description

This command displays the UCC client status and CDR statistics.

When VoIP calls are prioritized using media classification, the **Client Name** value is not available.

Syntax

Parameter	Description
`app`	Displays the UCC client status and CDR statistics based on a specific ALG.
`detail`	Displays UCC client status details.
`sta <mac>`	Displays the detailed record for a specific client based on its MAC address.

Example

The following command displays the UCC client status and record:

```
(host) [mynode] #show ucc client-info

Client Status:
--------------
Client IP     Client MAC         Client Name  ALG      Server(IP)  Registration State  Call
Status
---------     ----------         -----------  -----    ----------  ------------------  -------
----
192.0.2.22    00:23:33:41:c8:b8  Alex         SIP      192.0.2.1   REGISTERED          Idle

192.0.2.26    24:77:03:9a:6c:dc  John         Jabber   192.0.2.3   REGISTERED          Idle


AP Name  Flags  Device Type  Home Agent    Foreign Agent
-------  -----  -----------  ----------    -------------
AP-105          OS X         192.0.2.25    NA
AP-135          Win 7        192.0.2.25    NA

Total Client Entries:2
Flags: V - Visitor, A - Away, W - Wired, R - Remote, E - External
```

The output of this command includes the following information:

Column	Description
`Client IP`	Displays the IP address of the VoIP client.

Column	Description
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client.
ALG	Displays the Application Layer Gateway protocol used by the VoIP client.
Server(IP)	Displays the IP address of call server the client is registered to.
Registration State	Displays the registration status of the VoIP call. Possible values are: ■ **Challenged** ■ **Registered** ■ **Registering** ■ **Unregistered** ■ **Rejected** ■ **Unknown**
Call Status	Displays the VoIP call status of the client. Possible values are: ■ **Idle** ■ **In-Call**
AP Name	Displays the name of the AP to which the VoIP client is associated.
Flags	Displays if the client is a visitor, away, wired, remote, or external.
Device Type	Displays the device type identification of the client.
Home Agent	Displays the IP address of the managed device to which the client is connected or the home agent of the client if mobile IP is enabled.
Foreign Agent	Displayed if the client has roamed to another managed device when mobile IP is enabled.

The following command displays the UCC client status details:

```
(host) [mynode] #show ucc client-info detail

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP
      [E] - Metric calculated End-to-End
       D - Delay in milliseconds
       J - Jitter in milliseconds
       PL - Packet Loss in percent

Client Status Details(Average):
-------------------------------
Client IP     Client MAC         Client Name  Controller Delay(ms)/Jitter(ms)/PktLoss(%)
---------     ----------         -----------  ----------------------------------------
192.0.2.22    00:23:33:41:c8:b8  Alex         1.33/0.15/1.99
192.0.2.26    24:77:03:9a:6c:dc  John         0.82/0.17/0.05

AP Delay(ms)/Jitter(ms)/PktLoss(%)  End-to-End Delay(ms)/Jitter(ms)/PktLoss(%)  Call-Dur(sec)
TxRate(Mbps)  RxRate(Mbps)
----------------------------------  ----------------------------------------  -------------
------------  ------------
1.04/0.09/2.26                      79.00/3.23/1.72                           1114
84.42         130.56
1.12/0.15/2.63                      10.36/3.55/0.07                           584
27.02         30.12

ICH Denied  ALG
```

```
----------  ---
0           SIP
0           Jabber

Total Client Entries:2
```

The output of this command includes the following information:

Column	Description
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client.
Controller Delay(ms)/ Jitter(ms)/PktLoss(%)	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the managed device.
AP Delay(ms)/ Jitter(ms)/PktLoss(%)	Displays the WLAN delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This is the metric calculated at the AP.
End-to-End Delay(ms)/ Jitter(ms)/PktLoss(%)	Displays the end-to-end delay (in milliseconds), jitter (in milliseconds), and packet loss (in percentage). This field takes the wired and wireless network QoS parameters into consideration.
Call-Dur(sec)	Displays the average call duration in seconds.
TxRate(Mbps)	Displays the average transmission rate in Mbps.
RxRate(Mbps)	Displays the average receive rate in Mbps.
ICH Denied	Displays the number of calls that were not prioritized due to channel utilization threshold exceeding on the AP radio.
ALG	Displays the Application Layer Gateway protocol used by the VoIP client.

The following command displays a detailed record for a specific client MAC address:

```
(host) [mynode] #show ucc client-info sta 00:21:6a:b9:5f:34

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP

Station Report:
---------------
Client IP     Client MAC         AP-Name  SNR  Avg Tx Rate(Mbps)
---------     ----------         -------  ---  -----------------
10.15.88.245  00:21:6a:b9:5f:34  AP-135-1  45   54.56

Tx Drop(%)  Tx Retry(%)  Avg Rx Rate(Mbps)  Rx Retry(%)  Un-steerable (reason)
----------  -----------  -----------------  -----------  ---------------------
1.06        24.06        43.16              0.41         NA

Active Calls:
-------------
CDR ID  UCC Call ID  Client IP     Client Name  ALG     Dir  Called To  Dur(sec)  Orig-Time
------  -----------  ---------     -----------  ---     ---  ---------  --------  ---------
116     12           10.15.88.245  Alex         skype4b OG   Joe        421       Jan 20
01:36:08
```

```
Status  Call Type  Client Health  UCC Score[C]  UCC Score[A]   MOS
------  ---------  -------------  ------------  ------------   ---
ACTIVE  Voice      62             81.52/Good    83/01Good      4.17/Good

Call History:
-------------
CDR ID  UCC Call ID  Client IP     Client Name  ALG     Dir  Called To  Dur(sec)  Orig-Time
------  -----------  ---------     -----------  ---     ---  ---------  --------  ---------
54      23           10.15.88.245  Alex         skype4b OG   Mike       847       Jan 16
02:45:22
53      22           10.15.88.245  Alex         skype4b OG   Ken        789       Jan 14
06:53:41

Status  Reason      Call Type        Client Health  UCC Score[C]  UCC Score[A]  MOS
------  ------      ---------        -------------  ------------  ------------  ---
SUCC    Terminated  Voice            49             71.72/Good    73.99/Good    3.85/Good
SUCC    Terminated  Voice/Conf Call  44             77.22/Good    79.01/Good    4.13/Good
```

The output of this command includes the following information:

Column	Description
Station Report	
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Client Name	Displays the username of the VoIP client.
AP-Name	Displays the name of the AP handling the VoIP call.
SNR	Displays the Signal-to-noise (SNR) ratio. SNR is the power ratio between an information signal and the level of background noise.
Avg Tx Rate(Mbps)	Displays the average transmission rate in Mbps.
Tx Drop(%)	Displays the transmission packet drop in percentage.
Tx Retry(%)	Displays the transmission retry in percentage.
Avg Rx Rate(Mbps)	Displays the average receive rate in Mbps.
Rx Retry(%)	Displays the receive retry in percentage.
Un-steerable (reason)	Displays the reason for steering/not steering the client to another band. Possible values are: ■ **Sticky** ■ **Load Balance** ■ **Band Steer** ■ **Band Balance** ■ **Administrator Added** ■ **(IOS)** ■ **NA**
Active Calls	
CDR ID	Displays the Call Detail Record ID of a particular voice and video calls, desktop sharing, or file transfer session.

Column	Description
UCC Call ID	Displays the unique identifier for all call legs of a particular voice and video calls, desktop sharing, or file transfer session.
Client IP	Displays the IP address of the VoIP client.
Client Name	Displays the username of the VoIP client.
ALG	Displays the Application Layer Gateway protocol used by the VoIP client.
Dir	Displays the direction of the call. Possible values are: ■ **OG**—Outgoing ■ **IG**—Incoming
Called To	Displays the username of the VoIP client being called.
Dur(sec)	Displays the duration of the VoIP call in seconds.
Orig-Time	Displays the time at which the VoIP call originated.
Status	Displays the status of the VoIP call. Possible values are: ■ **SUCCESS** ■ **FAILED** ■ **ABORTED** ■ **BLOCKED** ■ **FORWARDED** ■ **ALERTING** ■ **HOLD** ■ **ACTIVE**
Call Type	Displays the type of VoIP call or session. Possible values are: ■ **Not Available** ■ **Voice** ■ **Video** ■ **Desktop Sharing** ■ **File Transfer** ■ **Voice/Conf Call** ■ **Video/Conf Call** ■ **Desktop-Sharing/Conf Call** ■ **File-Transfer/Conf Call**
Client Health	Displays the ratio of ideal air time required for transmitting a packet from an AP to a client to the actual air time taken for the packet transmission in percentage. Ideal air time assumes highest data rate without any retransmission.
UCC Score[C]	Displays the UCC score based on the quality of the voice call. This is the metric calculated at the managed device.
UCC Score[A]	Displays the UCC score based on the quality of the voice call or desktop sharing session. This is the metric calculated at the AP.
MOS	Displays the Mean Opinion Score of the VoIP call.
Call History	

Column	Description
Reason	Displays the reason code for call termination. Possible values are: ■ **NA** ■ **Capacity Reached** ■ **401 unauthorized** ■ **487 request timeout** ■ **Request timeout** ■ **Request canceled** ■ **Request terminated** ■ **Session timeout** ■ **Session timer expired** ■ **Session expired - request timeout** ■ **Aborted** ■ **Terminated** ■ **Forwarded** ■ **Transferred** ■ **Inactivity** ■ **Wrong number** ■ **Peer reset** ■ **Client reset** ■ **No answer** ■ **Missed** ■ **Parked** ■ **Invalid number** ■ **Tunnel down** ■ **Moved temporarily** ■ **4xx error** ■ **5xx error** ■ **Call leg does not exist** ■ **DELTS request** ■ **TCLAS flow deleted** ■ **No reason**
NOTE: For information on additional field descriptions, refer the field descriptions under the **Active Calls** heading.	

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc dns-ip-learning

```
show ucc dns-ip-learning
```

Description

This command displays the carrier's evolved Packet Data Gateway (ePDG) IP address learned by the managed device. This command is specific for Wi-Fi calling clients.

Syntax

No parameters.

Example

The following command displays the carrier's evolved Packet Data Gateway (ePDG) IP address learned by the managed device:

```
((host) [mynode] #show ucc dns-ip-learning

DNS IP Learning:
----------------
IP Address      Service Provider
----------      ----------------
208.54.85.108   T-Mobile
208.54.73.77    T-Mobile
208.54.70.110   T-Mobile
208.54.77.253   T-Mobile
208.54.75.2     T-Mobile
208.54.85.64    T-Mobile
208.54.73.76    T-Mobile
208.54.83.96    T-Mobile
208.54.85.111   T-Mobile

Total Entries:9
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc facetime

```
show ucc facetime
```

Description

This command displays the Apple Facetime ALG configuration.

Syntax

No parameters.

Example

The following command displays the Apple Facetime ALG configuration:

```
(host) [mynode] #show ucc facetime

FaceTime ALG Configuration
--------------------------
Parameter              Value    Set
---------              -----    ---
FaceTime ALG Support   Enabled
video priority         34
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc h323

```
show ucc h323
```

Description

This command displays the H.323 ALG configuration.

Syntax

No parameters.

Example

The following command displays the H.323 ALG configuration:

```
(host) [mynode] #show ucc h323

H323 ALG Configuration
----------------------
Parameter          Value    Set
---------          -----    ---
H323 ALG Support   Enabled
voice priority     46
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc ich

```
show ucc ich
```

Description

This command displays the Intelligent Call Handling configuration.

Syntax

No parameters.

Example

The following command displays the Intelligent Call Handling configuration:

```
(host) [mynode] #show ucc ich

Intelligent Call Handling Configuration
---------------------------------------
Parameter                      Value    Set
---------                      -----    ---
Intelligent Call Handling      Enabled
Channel Utilization Threshold  90
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc internal-state

```
show ucc internal-state
```

Description

This command displays the number of CDRs, flows, and voice clients created. This is a debug command.

Syntax

No parameters.

Example

The following command displays the UCM internal state statistics:

```
(host) [mynode] #show ucc internal-state

UCM Internal State Statistics
-----------------------------
Clients  Active CDRs  Ended CDRs  Flows Installed  Flows Agedout  VC creation failed
-------  -----------  ----------  ---------------  -------------  ------------------
3        0            43          140              13             0

Clients (Last)  Flows Installed (Last)  Flows AgedOut (Last)  VC creation failed (Last)
--------------  ----------------------  --------------------  -------------------------
0               0                       0                     0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc jabber

```
show ucc jabber
```

Description

This command displays the Cisco Jabber ALG configuration.

Syntax

No parameters.

Example

The following command displays the Cisco Jabber ALG configuration:

```
(host) [mynode] #show ucc jabber

Jabber ALG Configuration
------------------------
Parameter              Value        Set
---------              -----        ---
Jabber ALG Support     Enabled
Jabber server ip       192.0.2.2
Jabber server ip       192.0.2.3
voice priority         46
video priority         34
app-sharing priority   34
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc noe

```
show ucc noe
```

Description

This command displays the Alcatel-Lucent New Office Environment (NOE) ALG configuration.

Syntax

No parameters.

Example

The following command displays the Alcatel-Lucent NOE ALG configuration:

```
(host) [mynode] #show ucc noe

NOE ALG Configuration
---------------------
Parameter         Value    Set
---------         -----    ---
NOE ALG Support   Enabled
voice priority    46
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc rtpa-config

```
show ucc rtpa-config
```

Description

This command displays the real-time analysis configuration.

Syntax

No parameters.

Example

The following command displays the real-time analysis configuration:

```
(host) [mynode] #show ucc rtpa-config

Real-Time Analysis Configuration
--------------------------------
Parameter                                   Value    Set
---------                                   -----    ---
Real-Time Analysis of VoIP calls            Enabled
Upstream Real-Time Analysis of VoIP calls   Enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc rtpa-report

```
show ucc rtpa-report
```

Description

This command displays the real-time analysis report.

Syntax

No parameters.

Example

The following command displays the real-time analysis report:

```
(host) [mynode] #show ucc rtpa-report

Help: [C] - Metric calculated at the Controller
      [A] - Metric calculated at the AP
      [E] - Metric calculated End-to-End

Real-Time Analysis Call Quality Report
--------------------------------------
Client(IP)       Client(MAC)        Client(Name)   ALG  Jitter(usec)[C]  Pkt-loss(%)[C]  Delay
(usec)[C]
----------       -----------        ------------   ---  ---------------  --------------  ------
--------
192.168.201.240  f0:7b:cb:3b:65:5c  1002           SIP  23.700           0.000
101.800
192.168.201.246  00:24:d7:40:a8:58  1003           SIP  30.912           0.000
257.140

UCC Score[C]  Jitter(usec)[A]  Pkt-loss(%)[A]  Delay(usec)[A]  UCC Score[A]  Forward mode
------------  ---------------  --------------  --------------  ------------  ------------
68.366        0.000            0.499           316.400         84.119        decrypt-tunnel
82.551        0.000            0.000           327.478         85.999        decrypt-tunnel

Num Records:2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc sccp

```
show ucc sccp
```

Description

This command displays the Cisco Skinny Client Control Protocol (SCCP) ALG configuration.

Syntax

No parameters.

Example

The following command displays the Cisco SCCP ALG configuration:

```
(host) [mynode] #show ucc sccp

SCCP ALG Configuration
----------------------
Parameter          Value    Set
---------          -----    ---
SCCP ALG Support   Enabled
voice priority     46
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc session-idle-timeout

```
show ucc session-idle-timeout
```

Description

This command displays the UCC session idle timeout configuration.

Syntax

No parameters.

Example

The following command displays the UCC session idle timeout configuration:

```
(host) [mynode] #show ucc session-idle-timeout

UCC Session Idle Timeout Configuration
--------------------------------------
Parameter                 Value  Set
---------                 -----  ---
UCC Session Idle Timeout  35
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc sip

```
show ucc sip
```

Description

This command displays the SIP ALG configuration.

Syntax

No parameters.

Example

The following command displays the SIP ALG configuration:

```
(host) [mynode] #show ucc sip

SIP ALG Configuration
---------------------
Parameter                     Value     Set
---------                     -----     ---
SIP ALG Support               Enabled
SIP Midcall request timeout   Disabled
RTCP Inactivity               Disabled
voice priority                46
video priority                34
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc skype4b

```
show ucc skype4b
```

Description

This command displays the Skype4B ALG configuration.

Syntax

No parameters.

Example

The following command displays the Skype4B ALG configuration:

```
(host) [mynode] #show ucc skype4b

Skype4B ALG Configuration
-------------------------
Parameter                    Value    Set
---------                    -----    ---
Skype4B ALG Support          Enabled
Skype4B SDN Over http/https  https
voice priority               46
video priority               34
app-sharing priority         34
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc statistics

```
show ucc statistics counter call
   client [app {h323|jabber|noe|sccp|sip|skype4b|svp|vocera|WiFi-Calling}]
   global [app {h323|jabber|noe|sccp|sip|skype4b|svp|vocera|WiFi-Calling}]
```

Description

This command displays the UCC call statistics.

Syntax

Parameter	Description
`client`	Displays per client call statistics counter.
`global`	Displays system-wide call statistics counter.

Example

The following command displays the global call counters:

```
(host) [mynode] #show ucc statistics counter call global

System-wide Call Counters:
--------------------------
Call Originated  Call Terminated  Active  Success  Failed  Blocked
---------------  ---------------  ------  -------  ------  -------
6                37               0       12       29      0

Aborted  Forwarded  WMM AC-VI  WMM AC-VO  WMM-BK  WMM-BE
-------  ---------  ---------  ---------  ------  ------
2        0          6          0          0       8

Device Type Allocations:
------------------------
Device Type  WMM AC-VI  WMM AC-VO  WMM-BK  WMM-BE
-----------  ---------  ---------  ------  ------
Win 7        0          0          0       6
Apple        3          0          0       0
OS X         3          0          0       0

WMM (VI, VO, BK, BE):total calls with received priority
```

The following command displays the client call counters:

```
(host) [mynode] #show ucc statistics counter call client

Per Client Call Counters:
-------------------------
Client IP     Client MAC         Call Originated  Call Terminated  Active  Success  Failed
---------     ----------         ---------------  ---------------  ------  -------  ------
10.15.88.216  10:40:f3:82:91:04  0                32               0       3        29
10.15.88.217  10:40:f3:82:c1:48  3                0                0       3        0
10.15.88.245  00:26:c6:52:6b:7c  2                4                0       4        0
10.15.88.218  00:21:6a:b9:5f:34  1                1                0       2        0

Blocked  Aborted  Forwarded  WMM AC-VI  WMM AC-VO  WMM-BK  WMM-BE
-------  -------  ---------  ---------  ---------  ------  ------
0        0        0          3          0          0       0
0        0        0          3          0          0       0
0        2        0          0          0          0       6
```

```
0          0          0          0          0          0          2

WMM (VI, VO, BK, BE):total calls with received priority
```

The output of this command includes the following information:

Column	Description
Client IP	Displays the IP address of the VoIP client.
Client MAC	Displays the MAC address of the VoIP client.
Call Originated	Displays the number of times a call originated from the VoIP client.
Call Terminated	Displays the number of times a call terminated on the VoIP client.
Active	Displays the number of active calls on the VoIP client.
Success	Displays the number of successful calls.
Failed	Displays the number of failed call setup calls.
Blocked	Displays the number of blocked calls due to CAC.
Aborted	Displays the number of terminated calls due to inactivity.
Forwarded	Displays the number of times a call is forwarded for a VoIP client.
WMM AC-VI	Displays the number of calls where the client sent RTP with WMM AC set to Video (VI).
WMM AC-VO	Displays the number of calls where the client sent RTP with WMM AC set to Voice (VO).
WMM-BK	Displays the number of calls where the client sent RTP with WMM AC set to Background (BK).
WMM-BE	Displays the number of calls where the client sent RTP with WMM AC set to Best Effort (BE).

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc trace-buffer

```
show ucc trace-buffer
   jabber [count <0-65535>]
   sccp [count <0-65535>]
   sip [count <0-65535>]
   skype4b[count <0-65535>]
```

Description

This command displays the UCC call message trace buffer for Cisco Jabber, Cisco SCCP, SIP, and Microsoft Skype for Business ALGs. Call signaling events such as establishing voice, video, desktop sharing, and file transfer are recorded.

Syntax

Parameter	Description
`jabber [count <0-65535>]`	Displays the Jabber call message trace buffer.
`sccp [count <0-65535>]`	Displays the SCCP call message trace buffer.
`sip [count <0-65535>]`	Displays the SIP call message trace buffer.
`skype4b [count <0-65535>]`	Displays the Skype4b call message trace buffer.

Example

The following command displays Skype4b call message trace buffer:

```
(host) #show ucc trace-buffer skype4b

Skype4b Voice Client(s) Message Trace
-------------------------------------
Client IP     Client MAC         Client Name  Direction  Event Time       BSSID
---------     ----------         -----------  ---------  ----------       -----
192.0.2.22    00:23:33:41:c8:b8  Alex         OG         Jan  3 11:24:34  9c:1c:12:8a:b5:50
192.0.2.26    24:77:03:9a:6c:dc  John         OG         Jan  3 11:24:34  9c:1c:12:8a:b5:50
192.0.2.29    00:22:90:ea:9e:f1  Steve        OG         Jan  3 11:24:08  9c:1c:12:8a:b5:50

Called To  Media Type   AP Name  Src Port     Dest Port    Call Status
---------  ----------   -------  --------     ---------    -----------
Joe        Voice/Video  AP-225   50030/58008  50032/58006  Start of call
Mike       Voice/Video  AP-225   50032/58006  50030/58008  InCallQuality Update
Ken        Voice        AP-225   50026        50038        Call Quality Update

Num of Rows:3
```

The output of this command includes the following information:

Column	Description
`Client IP`	Displays the IP address of the VoIP client.
`Client MAC`	Displays the MAC address of the VoIP client.
`Client Name`	Displays the user name of the VoIP client.

Column	Description
Direction	Displays the call direction. ■ **OG** — Outgoing ■ **IC** — Incoming
Event Time	Displays the time stamp when the VoIP call originated.
BSSID	Displays the BSSID of the AP to which the VoIP client is connected.
Called To	Displays the user name of the VoIP client being called.
Media Type	Displays the type of Skype4b call. This can be one of the following: ■ **Desktop-sharing** ■ **File-transfer** ■ **Video** ■ **Voice**
AP Name	Displays the name of the access point receiving calls.
Src Port	Displays the source port for the media session.
Dest Port	Displays the destination port of the particular media session.
Call Status	Displays if the Skype4b client is in any one of the following call status: ■ **Start of call** ■ **End of call** ■ **Before call update** ■ **Call Quality Update** ■ **InCallQuality Update** ■ **After call update**

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc vocera

```
show ucc vocera
```

Description

This command displays the Vocera ALG configuration.

Syntax

No parameters.

Example

The following command displays the Vocera ALG configuration:

```
(host) [mynode] #show ucc vocera

Vocera ALG Configuration
------------------------
Parameter           Value    Set
---------           -----    ---
Vocera ALG Support  Enabled
voice priority      46
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show ucc wificalling

```
show ucc wificalling
```

Description

This command displays the Wi-Fi calling configuration.

Syntax

No parameters.

Example

The following command displays the Wi-Fi calling configuration:

```
(host) [mynode] #show ucc wificalling

WiFiCalling Configuration
-------------------------
Parameter             Value    Set
---------             -----    ---
WiFiCalling Support   Enabled
voice priority        46
dns pattern           N/A
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	PEFNG license	Config or Enable mode on Mobility Master

show upgrade internal

```
show upgrade internal managed-devices status
      copy list <mac-list>
      reboot list <mac-list>
      summary list <mac-list>
```

Description

This command displays the status of the upgrade of the managed devices.

Syntax

Parameter	Description
`copy list <mac-list>`	Copy status of managed devices based on MAC address. Specify multiple MAC addresses separated by commas.
`reboot list <mac-list>`	Reboot status of managed devices based on MAC address. Specify multiple MAC addresses separated by commas.
`summary list <mac-list>`	Status summary of managed devices based on MAC address. Specify multiple MAC addresses separated by commas.

Example

```
(host) [mynode] #show upgrade internal managed-devices status summary list 00:0b:23:b0:81:d0

upgrade managed-node status summary
-----------------------------------
LC MAC  Config Path  Host Name  IP Addr  LC Model  Current Ver  Last Cmd  Last Cmd Status
------  -----------  ---------  -------  --------  -----------  --------  ---------------
00:0b:23:b0:81:d0  /md/IND/70XXS  A7010-HA2-FIFTEEN  192.168.5.15  A7010  8.0.0.0-svcs-ctrl_
55616  Not initialized  Not initialized
```

The output of this command includes the following information:

Parameter	Description
`LC MAC`	MAC address of the managed device.
`Config Path`	Config node path of the managed device.
`Host Name`	Name of the Mobility Master.
`IP Addr`	IP address of the managed device.
`LC Model`	Model number of the managed device.
`Current Ver`	Version of ArubaOS currently running on the managed device.
`Last Cmd`	Last command issued on the managed device.
`Last Cmd Status`	Status of the last command issued on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show upgrade managed-devices

```
show upgrade managed-devices status
      copy
         all
         path <node-path>
         single <mac-addr>
      reboot
         all
         path <node-path>
         single <mac-addr>
      summary
         all
         path <node-path>
         single <mac-addr>
```

Description

This command displays the status of the upgrade of the managed devices.

Syntax

Parameter	Description
copy	Copy status of managed device.
all	Copy status of all managed devices under the respective node path.
path <node-path>	Copy status of all managed devices under the specific node path.
copy single <mac-addr>	Copy status of a specific managed device based on MAC address.
reboot	Reboot status of managed device.
all	Reboot status of all managed devices under the respective node path.
path	Reboot status of all managed devices under a specific node path.
single	Reboot status of a specific managed device based on MAC address.
Summary	Status summary of the managed device .
all	Status summary of all managed device under the respective node path.
path	Status summary ofl managed devices under a specific node path.
single	Status Summary of a specific managed device based on MAC address.

Example

```
(host) [mynode] #show upgrade managed-devices status summary single 00:0b:23:b0:81:d0
-----------------------------------
LC MAC  Config Path  Host Name  IP Addr  LC Model  Current Ver  Last Cmd  Last Cmd Status
------  -----------  ---------  -------  --------  -----------  --------  ---------------
00:0b:23:b0:81:d0  /md/IND/IPV6-NODES  A7005-BKLMS_TWENTY  2002:dead:face:5::20  A7005
8.0.0.0-svcs-ctrl_55616  Not initialized  Not initialized
```

The output of this command includes the following information:

Parameter	Description
LC MAC	MAC address of the managed device.
Config Path	Config node path of the managed device.
Host Name	Name of the Mobility Master.
IP Addr	IP address of the managed device.
LC Model	Model number of the managed device.
Current Ver	Version of ArubaOS currently running on the managed device.
Last Cmd	Last command issued on the managed device.
Last Cmd Status	Status of the last command issued on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

show upgrade-profile

Description

The settings in the centralized image upgrade profile uses ArubaOS images to upgrade the managed devices with the ArubaOS images hosted on an image server. When an upgrade action command is executed on the Mobility Master, the **upgrademgr** process running on Mobility Master sends an upgrade request to **upgrademgr** process running on corresponding managed devices. The managed devices then connect to the image server and download the appropriate image file after verifying the validity of the image file, before upgrading to the downloaded image file.

Syntax

No parameters.

Usage Guidelines

The centralized image upgrade feature is enabled and configured on managed devices only, and supports up to 100 simultaneous image downloads.

Example

```
(host) (config) # show upgrade-profile

Upgrade Profile
---------------
Parameter                Value
---------                 -----
Server IP address         N/A
Server IPv4/IPv6 address  2000:192:168:28::59
Username                  root
Password                  ********
Protocol                  scp
File path                 Builds
```

The output of this command includes the following information:

Parameter	Description	Range	Default
`serverip`	The IPv4 address of the image server. This parameter is only used by managed devices running versions prior to ArubaOS 8.2 and accepts only IPv4 address. **NOTE:** For FTP or SCP protocol, specify the username and password.	-	-
`serveraddr`	The IPv4 or IPv6 address of the image server. This parameter is only used by managed devices running ArubaOS 8.2. **NOTE:** For FTP or SCP protocol, specify the username and password.	-	-
`Username`	If the **protocol** parameter is set to **FTP** or **SCP**, this parameter displays the user name that ArubaOS uses to connect to the image server.	-	-

Parameter	Description	Range	Default
`Password`	If the **protocol** parameter is set to **FTP** or **SCP**, this parameter displays the password that ArubaOS will use to connect to the image server.	-	-
`Protocol`	Specify the protocol used to send the software to the managed device. ■ TFTP ■ FTP ■ SCP	-	TFTP
`File path`	File path to the location on the image server where the image file(s) reside.	-	-

Command History

Release	Modification
ArubaOS 8.2.0.0	The **serveraddr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show uplink

```
show uplink [config|{connection <link_id>}|signal|{stats <link_id}]
```

Description

Displays uplink manager configuration details.

Syntax

Parameter	Description
`config`	Enter the keyword **config** to display the uplink manager, the default wired priority and default cellular priority
`connection`	Enter the keyword **connection** followed by the uplink ID number to display the connection details.
`signal`	Enter the keyword **signal** to display the cellular uplink signal strength.
`stats`	Enter the keyword **stats** followed by the uplink ID number to display the statistical information on the designated uplink.

Example

The output of this command displays the managed device uplink status . For a managed device, the health status of these uplink connections is also displayed in the **Status** section of the **Dashboard>WAN** page of the managed device WebUI.

```
(host) #show uplink
Uplink Manager: Disabled
Uplink Health-check: Enabled
Uplink Health-check IP/FQDN: 192.0.2.14
Uplink Management Table
-----------------------
Id  Uplink Type  Properties     Priority  State      Status      Reachability
--  -----------  ----------     --------  -----      ------      ------------
1   Wired        vlan 4094      200       Connected  Active      Reachable
2   Cellular     Novatel_U727   100       Standby    Ready       Reachable
```

Related Commands

Command	Description
ip probe default	This command configures WAN health-check ping-probes for measuring WAN availability and latency on managed device uplinks.
uplink	Manage and configure the uplink network connection.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show usb

```
show usb
   cellular
   ports [<address>]
   test <address>
   usb-modeswitch
   verbose
```

Description

Display detailed USB device information on a stand-alone controller or managed device.

Syntax

Parameter	Description
`cellular`	Enter the keyword **cellular** to display cellular devices.
`ports`	Enter the keyword **ports** to display detailed TTY port information such as signal strength.
`test`	Enter the keyword **test** to test the USB TTY ports. **NOTE:** Testing an invalid modem port may cause the stand-alone controller or managed device to “hang”. To resolve this, unplug and re-plug the modem.
`usb-modeswitch`	USB mode switch utility log.
`verbose`	Enter the keyword **verbose** to display detailed USB information including serial number and USB type.

Usage Guideline

This command should be executed from the managed device only.

Examples

The USB Device table, in the example below, displays the USB port is in the 'Device Ready' state, meaning that the port has passed the diagnostic test and is ready to send and receive data.

```
(host-md) #show usb

USB Device Table
----------------
Address  Product                Vendor  ProdID  Serial           Type      Profile    State
Bus
-------  -------                ------  ------  ------           ----      -------    -----
--
18       Novatel Wireless CDMA  1410    4100    091087843891000  Cellular  new_modem  Device
ready
```

Below is an example of the **show usb verbose** display output (partial).

```
(host-md) #show usb verbose
...
T: Bus=01 Lev=02 Prnt=02 Port=00 Cnt=01 Dev#= 3 Spd=12 MxCh= 0
D: Ver= 1.10 Cls=00(>ifc ) Sub=00 Prot=00 MxPS=64 #Cfgs= 1
P: Vendor=1410 ProdID=4100 Rev= 0.00
```

```
S: Manufacturer=Novatel Wireless Inc.
S: Product=Novatel Wireless CDMA
S: SerialNumber=091087843891000
C:* #Ifs= 5 Cfg#= 1 Atr=a0 MxPwr=500mA
...
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show user

```
show user
   ap-group <ap-group>
   ap-name <ap-name>
   authentication-method dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web
   bssid <A:B:C:D:E:F>
   devtype <device>
   essid <STRING>
   internal
   ip <A.B.C.D> [log]
   location b.f.l
   mac <A:B:C:D:E:F> [log]
   mobile {[bindings][visitors]}
   name <STRING>
   phy-type {[a]|[b]}
   role <STRING>
   rows <NUMBER> <NUMBER>
```

Description

Displays detailed information about user in terms of AP group, authentication method, role and so on.

Syntax

Parameter	Description
`ap-group <ap-group>`	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
`ap-name <ap-name>`	Filter the output of this command by showing users connected to an AP with the specified AP name.
`authentication-method`	Filter the output of this command by the authentication method used for the device:
`dot1x`	Show data for devices using 802.1X authentication.
`mac`	Show data for devices using MAC authentication.
`opensystem`	Show data for devices using open (no) authentication.
`psk`	Show data for devices that do not use authentication but use a pre-shared key for encryption.
`stateful-dot1x`	Show data for devices using stateful 802.1X authentication.
`via-vpn`	Show data for devices that authenticate using Aruba VIA.
`vpn`	Show data for devices using VPN authentication.
`web`	Show data for devices using captive portal authentication.
`bssid <A:B:C:D:E:F>`	Show user data for a specific device BSSID.
`devtype <device>`	Show output for a specified device type, if identified. If the device name includes spaces, you must enclose it in quotation marks.

Parameter	Description
`essid <STRING>`	Show user data for a specific ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
`internal`	Display internal user entries only. Include the **rows** options to filter the output of this command by specifying the number of rows from the end of the output and the total number of rows to display/
`ip <A.B.C.D>`	Show user data for a specific IP address .
`log`	If per-user logging is enabled using the aaa log command, include the optional **log** parameter to display authentication log files for a user with the specified MAC address.
`mac <A:B:C:D:E:F>`	Show user data for a specific MAC address
`log`	If per-user logging is enabled using the aaa log command, include the optional **log** parameter to display authentication log files for a user with the specified MAC address.
`mobile`	Filter the output of this command to show data for Mobile users.
`bindings`	Show data for users that have moved away from their home network.
`visitors`	Show data for mobility users that are visiting the network.
`name <STRING>`	User's name.
`phy-type`	801.11 type
`a`	Matches PHY type a.
`g`	Matches PHY type b or g.
`role <STRING>`	User role such as employee, visitor and so on.
`rows <NUMBER> <NUMBER>`	Filter the output of the show user command by specifying the number of rows from the end of the output and the total number of rows to display/

Usage Guidelines

Use the **show user** command to show detailed user statistics and roles.

Example

```
(host) #show user
Users
-----
IP           MAC       Name   Role  Age(d:h:m)  Auth  VPN link  AP name  Roaming
Essid/Bssid/Phy  Profile  Forward mode  Type  Host Name
----------  ------------  ------  ----  ----------  ----  --------  -------  -------  --------
-------  -------  ------------  ----  ---------
User Entries: 0/0
Curr/Cum Alloc:0/0 Free:0/0 Dyn:0 AllocErr:0 FreeErr:0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show user-table

```
show user-table
   ap-group <ap-group>
   ap-name <ap-name>
   authentication-method dot1x|mac|opensystem|psk|stateful-dot1x|via-vpn|vpn|web
   bssid <A:B:C:D:E:F>
   devtype <device>
   debug
   essid <STRING>
   internal
   ip <A.B.C.D> [log]|[detail]
   mac <A:B:C:D:E:F> [log]
   mobile {[bindings][visitors]}
   name <STRING>
   phy-type {[a]|[b]}
   role <STRING>
   rows <NUMBER> <NUMBER>
   standby [ipv4]|[ipv6]|[log]|[mac]
   station
   summary
   unique
   verbose
```

Description

Displays detailed information about the controller's connection to a user device, in regards to mobility state and statistics, authentication statistics, VLAN assignment method, AP datapath tunnel info, radius accounting statistics, user name, user-role derivation method, datapath session flow entries, and 802.11 association state and statistics. The **show user** command allows you to filter specific information by parameter.

Syntax

Parameter	Description
`ap-group <ap-group>`	Filter the output of this command by showing users connected to APs that belong to the specified AP group.
`ap-name <ap-name>`	Filter the output of this command by showing users connected to an AP with the specified AP name.
`authentication-method`	Filter the output of this command by the authentication method used for the device:
`dot1x`	Show data for devices using 802.1X authentication.
`mac`	Show data for devices using MAC authentication.
`opensystem`	Show data for devices using open (no) authentication.
`psk`	Show data for devices that do not use authentication but use a pre-shared key for encryption.
`stateful-dot1x`	Show data for devices using stateful 802.1X authentication.
`via-vpn`	Show data for devices that authenticate using Aruba VIA.

Parameter	Description
vpn	Show data for devices using VPN authentication.
web	Show data for devices using captive portal authentication.
bssid <A:B:C:D:E:F>	Show user data for a specific device BSSID.
debug	Show all user data for debugging purposes.
devtype <device>	Show output for a specified device type, if identified. If the device name includes spaces, you must enclose it in quotation marks.
essid <STRING>	Show user data for a specific ESSID. If the ESSID includes spaces, you must enclose it in quotation marks.
internal	Display internal user entries only. Include the **rows** options to filter the output of this command by specifying the number of rows from the end of the output and the total number of rows to display/
ip <A.B.C.D>	Show user data for a specific IP address .
log	If per-user logging is enabled using the aaa log command, include the optional **log** parameter to display authentication log files for a user with the specified MAC address.
detail	Show detailed user data for a specific IP address including role-derivation.
mac <A:B:C:D:E:F>	Show user data for a specific MAC address
log	If per-user logging is enabled using the aaa log command, include the optional **log** parameter to display authentication log files for a user with the specified MAC address.
mobile	Filter the output of this command to show data for Mobile users.
bindings	Show data for users that have moved away from their home network.
visitors	Show data for mobility users that are visiting the network.
name <STRING>	User's name.
phy-type	801.11 type
a	Matches PHY type a.
g	Matches PHY type b or g.
role <STRING>	User role such as employee, visitor and so on.
rows <NUMBER> <NUMBER>	Filter the output of the show user command by specifying the number of rows from the end of the output and the total number of rows to display/
standby	User standby entries
ipv4	User standby entires for the IPv4 address specified.
ipv6	User standby entires for the IPv6 address specified.

Parameter	Description
log	Debug log of the specified user.
mac	User standby entires for the MAC address specified.
station	For internal use only.
summary	Shows the authentication and encryption type used by wired or wireless clients.
unique	Displays only information for users with a valid IP address.
verbose	Displays all information about the user table.

Usage Guidelines

Use the **show user-table** command to show detailed user statistics which includes the entire output of the user-table, mobility state and statics, authentication statistics, VLAN assignment method, AP datapath tunnel information, radius accounting statistics, user-role derivation method, datapath session flow entries and 802.11 association state and statistics.

Examples

This example displays users currently in the **employee** role. The output of this command is split into two tables in this document, however it appears in one table in the CLI.

```
(host) [mynode] (config) show user role employee
Users
-----
    IP               MAC             Name            Role      Age(d:h:m)  Auth     VPN link  AP
name
----------      ------------       ------          ----      ----------  ----     --------  ----
---
192.168.160.1   00:23:6c:80:3d:bc  madisonl        employee  01:05:50    802.1X             1263
10.100.105.100  00:05:4e:45:5e:c8  CORP1NETWORKS   employee  00:02:22    802.1X
wlan-qa-cage
10.100.105.102  00:14:a5:30:c2:7f  pdedhia         employee  01:20:09    802.1X             2198
10.100.105.97   00:1b:77:c4:a2:fa  CORP1NETWORKS   employee  00:02:18    802.1X             2198
10.100.105.109  00:21:5c:02:16:bb  myao            employee  00:05:40    802.1X             1109


Users
-----
Roaming     Essid/Bssid/Phy                            Profile    Forward mode    Type
 -------     ---------------                            -------   ------------    ----
Associated  ethersphere-wpa2/00:1a:1e:85:d3:b1/a-HT  default    tunnel
Associated  ethersphere-wpa2/00:1a:1e:6f:e5:51/a     default    tunnel
Associated  ethersphere-wpa2/00:1a:1e:87:ef:f1/a     default    tunnel
Associated  ethersphere-wpa2/00:1a:1e:87:ef:f1/a     default    tunnel
Associated  ethersphere-wpa2/00:1a:1e:85:c2:11/a-HT  default    tunnel          ipad
```

The output of the **show user mac <mac-addr>** and **show user ip <ip-addr>** commands include the following information.

```
(host) [mynode]) # show user-table ip 5.5.5.2
Name: 98:0c:82:45:d6:7b, IP: 5.5.5.2, MAC: 98:0c:82:45:d6:7b, Role: mac-role, ACL: 54/0/0,
Age: 00:00:07
Authentication: Yes, status: started, method: MAC, protocol: PAP, server: Internal
Bandwidth = No Limit
```

```
Bandwidth = No Limit
Role Derivation: default for authentication type MAC
VLAN Derivation: unknown
Idle timeouts: 0, Valid ARP: 0
Mobility state: Wireless, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 L3 Mob: 0
Flags: internal=0, trusted_ap=0, l3auth=0, mba=1, vpnflags=0, u_stm_ageout=1
Flags: innerip=0, outerip=0, vpn_outer_ind:0, guest=0, download=1, wispr=0
Auth fails: 0, phy_type: g-HT, reauth: 0, BW Contract: up:0 down:0, user-how: 14
Vlan default: 3, Assigned: 5, Current: 5 vlan-how: 0 DP assigned vlan:0
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, Flags=0x0
Tunnel=0, SlotPort=0x2000, Port=0x1000d (tunnel 13)
Role assigment - L3 assigned role: n/a, VPN role: n/a, Dot1x cached role: n/a
Current Role name: mac-role, role-how: 1, L2-role: mac-role, L3-role: mac-role
Essid: 1_wlan_135, Bssid: d8:c7:c8:38:f4:a0 AP name/group: d8:c7:c8:cb:8f:4a-135/groupfor135
Phy-type: g-HT
RadAcct sessionID:n/a
RadAcct Traffic In 4/216 Out 2/420 (0:4/0:0:0:216,0:2/0:0:0:420)
Timers: reauth 0
Profiles AAA:1_wlan_135-aaa_prof, dot1x:dot1x_prof-rwv10, mac:pMac CP: def-role:'logon' sip-
role:'' via-auth-profile:''
ncfg flags udr 0, mac 1, dot1x 1, RADIUS interim accounting 0
IP Born: 1354560806 (Mon Dec  3 10:53:26 2012)
Core User Born: 1354560805 (Mon Dec  3 10:53:25 2012)
Upstream AP ID: 0, Downstream AP ID: 0
Device Type: Dalvik/1.4.0 (Linux; U; Android 2.3.6; SAMSUNG-SGH-I777 Build/GINGERBREAD)
Session Timeout from Radius: No, Session Timeout Value:0
Address is from DHCP: yes
```

The **role-how** and **vlan-how** parameters in the output of this command display a code that corresponds to the following values:

Role Derivation Code	Description
1	AAA profile default role
2	Role derived from user rules
3	Role derived from UDR
4	Default role for authentication type
5	Role derived from server rules
6	Aruba vendor-specific attribute (VSA)
7	Dot1X profile role
8	Dot1X server derived role
9	Dot1X role derived from Aruba VSA
10	Dot1X role derived from ClearPass Policy Manager VSA
11	Role derived from DHCP option
12	Change of authorization role
13	Forced role set by ESI

Role Derivation Code	Description
14	Role derived from mobility
15	Role assigned by external/internal captive portal
16	Role assigned by SIP
17	SDR derived role during L3 authentication
18	VSA derived role during L3 authentication
19	ClearPass Policy Manager VSA derived role during L3 authentication
20	Authentication type VPN role (VIA, VPN, or Transport VPN)
21	Authentication type role (BTLM, Kerb, GIS, or so on)
22	System assigned AP role

VLAN Derivation Code	Description
1	Default VLAN
2	Initial role contained
3	User rule role contained
4	Matched user rule
5	DHCP Option 77 role contained
6	Matched DHCP Option 77
7	MBA role contained
8	MBA server rule role contained
9	MBA server rule
10	MBA Aruba VSA role contained
11	MBA Aruba VSA
12	MBA MSFT attributes
13	User Dot1X role contained
14	Dot1X server rule role contained
15	Dot1X server rule
16	Dot1X Aruba VSA role contained
17	Dot1X Aruba VSA

VLAN Derivation Code	Description
18	Dot1X MSFT attributes
19	VLAN from pmk-cache
20	DHCP options user rule role contained
21	DHCP options user rule
30	Adaptive DHCP VLAN

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show util_proc

```
show util_proc guest-email counters
```

Description

Show counters for the guest email process.

Syntax

No parameters.

Usage Guidelines

As part of guest provisioning, the guest access email feature allows you to define the SMTP port and server that processes guest provisioning email. This server sends email to the guest or the sponsor when a guest user manually sends email from the Guest Provisioning page, or when a user creates a guest account.

Example

The output of this command shows the numbers of guest emails received, sent and dropped since the controller was last reset

```
(host) #show util_proc guest-email counters

Guest Email Counters
--------------------
Name             Value
----             -----
Email Received   14
Email Sent       3
Email Dropped    0.
```

Related Commands

To configure SMTP servers and server ports for guest email, use the command guest-access-email.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show valid-network-oui-profile

```
show valid-network-oui-profile
```

Description

This command displays the Valid Equipment OUI Profile table

Syntax

No parameters

Usage Guidelines

If you used the valid-networkoui-profile to add a new OUI to the controller, issue the show valid-network-oui-profile command to see a list of current OUIs.

Example

```
(Host) (config) #show valid-network-oui-profile

Valid Equipment OUI profile
---------------------------
Parameter  Value
---------  -----
OUI        00:1A:1E
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show version

```
show version
```

Description

Show the system software version.

Syntax

No parameters.

Example

```
(host) #show version
Aruba Operating System Software.
ArubaOS (MODEL: Dell Networking W-650 Controller-US), Version 6.1.0.0
Website: http://www.dell.com
Copyright (c) 2002-2011, Aruba Networks, Inc.
Compiled on 2011-04-28 at 00:18:36 PDT (build 28106) by p4build

ROM: System Bootstrap, Version CPBoot 1.0.0.0 (build 23274)
Built: 2010-01-19 11:11:41
Built by: p4build@re_client_23274

Switch uptime is 1 days 6 hours 2 minutes 4 seconds
Reboot Cause: User reboot.
Supervisor Card
Processor XLS 408 (revision B1) with 890M bytes of memory.
32K bytes of non-volatile configuration memory.
256M bytes of Supervisor Card System flash (model=NAND 256MB)
```

The output of this command includes the following information

Parameter	Description
Model	Controller model type.
Version	Version of ArubaOS software.
ROM	System bootstrap version.
Switch Uptime	Switch uptime (time elapsed since the last controller reset.
Reboot Cause	Reason the controller was last rebooted.
Supervisor Card	Details for the controller's internal supervisor card.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show via

```
show via
   version
   websessions
```

Description

Displays VIA version and web session details.

Syntax

Parameter	Description	Range	Default
`version`	Displays the version of VIA client available on the controller.	—	—
`websessions`	Displays the list of users connected to the VIA controller using the VIA client.	—	—

Example

The following example displays the version of VIA client available on the controller.

```
(host) # show via version(host) (VIA Client WLAN Profile "example") #show  via version
Default VIA Installer:
----------------------
<aruba>
        <via>
                <platform>win32</platform>
                <version>1.0.0.23373</version>
        </via>
</aruba>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan

```
show vlan <id>
```

Description

This command shows a configured VLAN interface number, description and associated ports.

Syntax

Parameter	Description	Range	Default
<id>	Identification number for the VLAN.	1-4094	1

Usage Guidelines

Issue this command to show the selected VLAN configuration. The **VLAN** column lists the VLAN ID. The **Description** column provides the VLAN name or number and the **Ports** column shows the VLAN's associated ports. The **AAA Profile column** shows if a wired AAA profile has been assigned to a VLAN, enabling role-based access for wired clients connected to an untrusted VLAN or port on the controller.

```
(host) #show vlan

VLAN CONFIGURATION
------------------
VLAN  Description     Ports                          AAA Profile
----  -----------     -----                          -----------
1     Default         GE0/3-7 GE0/9 XG0/10-11 Pc0-7  N/A
10    VLAN0010        GE0/8                          N/A
20    RAP_VLAN                                       N/A
25    VLAN0025        GE0/0                          mac-auth-aaa-prof
30    VLAN0030                                       N/A
56    VLAN0056                                       default
57    VLAN0057                                       default
58    VLAN0058                                       default
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan-assignment

```
show vlan-assignment
```

Description

This command shows the number of clients assigned to a VLAN.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the number of clients that are assigned to a VLAN.

```
(host) [mynode]#show vlan-assignment

VLAN Assignment
---------------
VLAN   #CLIENTS
----   --------
10     0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan-assignment-auth

```
show vlan-assignment-auth
```

Description

This command shows the VLAN usage in the user authentication module.

Syntax

No parameters.

Usage Guidelines

Issue this command to view all the VLAN IDs that are configured along with the current client count that uses that VLAN ID.

```
(host) #show vlan-assignment-auth

Vlan usage in AUTH
------------------
VLAN ID  Usage
-------  -----
10       0
```

Related Commands

```
(host) [mynode] (config) #vlan
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan mapping

```
show vlan mapping
```

Description

This command shows a configured VLAN name, its pool status, assignment type and the VLAN IDs assigned to the pool.

Syntax

Parameter	Description	Range	Default
<id>	Identification number for the VLAN.	1-4094	1

Usage Guidelines

Issue this command to show the selected VLAN configuration. The **VLAN Name** column displays the name of the VLAN pool. The **VLAN IDs** column lists the VLANs that are part of the pool.

```
(host) #show vlan mapping

Vlan Mapping Table
------------------
VLAN Name         Assignment Type  VLAN IDs
---------         ---------------  --------
mygroup           Hash             62,94
newpoolgroup      Even
vlannametest      Even             62,1511
yourvlan          N/A              62
```

Related Commands

```
(host) [mynode] (config) #vlan
(host) [mynode] (config) #vlan-name
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan status

```
show vlan status <id>
```

Description

This command shows the current status of all VLANs on the controller.

Syntax

No parameters.

Usage Guidelines

Issue this command to show the status of VLANs on the controller. The **VLANID** column displays the VLAN ID name or number. The **IP Address** column provides the VLAN's IP address. The **Adminstate** column indicates if the VLAN is enabled or disabled. The **Operstate** column indicates if the VLAN is currently up and running. The **PortCount** column shows how many ports are associated with the VLAN. The **Nat Inside** column displays whether source Nat is enabled for the VLAN interface. If Nat is enabled, all the traffic passing through this VLAN interface is the source natted to the outgoing interface's IP address.

```
(host) #show vlan status

Vlan Status
-----------
VlanId  IPAddress                    Adminstate  Operstate  PortCount  Nat Inside  Mode
Ports                                       AAA Profile
------  ---------                    ----------  ---------  ---------  ----------  ----     -
----                                          ------------
1       unassigned/unassigned        Enabled     Up         9          Disabled    Regular
GE1/0 GE1/2 GE1/5-9 XG1/10-11 Pc0 Pc2-5 Pc7   N/A
2       N/A                          N/A         N/A        3          Disabled    Regular
GE1/7-9                                     N/A
10      172.20.10.202/255.255.255.0  Enabled     Up         4          Disabled    Regular
GE1/7-9 Pc6                                 N/A
21      172.20.21.202/255.255.255.0  Disabled    Down       4          Disabled    Regular
GE1/7-9                                     N/A
24      172.20.24.202/255.255.255.0  Disabled    Down       3          Disabled    Regular
GE1/7-9                                     N/A
29      172.20.29.202/255.255.255.0  Enabled     Up         4          Disabled    Regular
GE1/7-9 Pc6                                 N/A
101     172.102.1.202/255.255.255.0  Enabled     Down       3          Disabled    Regular
GE1/7-9                                     N/A
102     172.102.2.202/255.255.255.0  Enabled     Down       3          Disabled    Regular
GE1/7-9                                     N/A
```

Related Commands

```
(host) [mynode] (config) #vlan
(host) [mynode] (config) #vlan-name
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan summary

```
show vlan summary
```

Description

This command shows the number of existing VLANs.

Syntax

Parameter	Description
`Number of existing VLANs`	The number of existing VLANs on the controller.

Usage Guidelines

Issue this command to show the number of existing VLANs on the controller.

```
(host) #show vlan summary

Number of existing VLANs                :13
```

Related Commands

```
(host) (config) #vlan
(host) (config) #vlan-name
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show vlan-bwcontract-explist

```
show vlan-bwcontract-explist [internal]
```

Description

Show entries in the VLAN bandwidth contracts MAC exception lists.

Syntax

Parameter	Description
`internal`	Include the optional **internal** parameter to display the MAC addresses in the internal, preconfigured VLAN bandwidth contracts MAC exception list.

Example

The following command displays the MAC addresses in the internal MAC exception list.

```
(host) (config) #show vlan-bwcontract-explist internal

VLAN BW Contracts Internal MAC Exception List
-----------------------------------------
MAC address
-----------
01:80:C2:00:00:00
01:00:0C:CC:CC:CD
01:80:C2:00:00:02
01:00:5E:00:82:11
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show vpdn l2tp configuration

```
show vpdn l2tp configuration
```

Description

Displays the VPN L2TP tunnel configuration.

Syntax

No parameters.

Example

The output of this command shows the L2TP tunnel configuration.

```
(host) # show vpdn l2tp configuration

Enabled
Hello timeout: 30 seconds
DNS primary server: 10.16.15.1
DNS secondary server: 10.16.14.1
WINS primary server: 0.0.0.0
WINS secondary server: 0.0.0.0
PPP client authentication methods:
         PAP
IP LOCAL POOLS:
         vpnpool: 10.16.15.150 - 10.16.15.160
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show vpdn pptp configuration

```
show vpdn pptp configuration
```

Description

Displays the PPTP configuration on the controller.

Syntax

No parameters.

Example

The output of this command shows the L2TP tunnel configuration.

```
(host) # show vpdn pptp configuration

Enabled
Hello timeout: 30 seconds
DNS primary server: 10.15.1.1
DNS secondary server: 10.15.1.200
WINS primary server: 0.0.0.0
WINS secondary server: 0.0.0.0
PPP client authentication methods:
         MSCHAP
         MSCHAPv2
MPPE Configuration
         128 bit encryption enabled
IP LOCAL POOLS
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show vpdn pptp local pool

```
show vpdn pptp local pool <pool_name>
```

Description

Displays the IP address pool for VPN users using Point-to-Point Tunneling Protocol.

Syntax

No parameters.

Example

The output of this command shows the all IP address pools for VPN users.

```
(host) # show vpdn pptp local pool

IP addresses used in pool localgroup
0 IPs used - 11 IPs free - 11 IPs configured
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show vpn-dialer

```
show vpn-dialer <dialer_name>
```

Description

Displays the VPN dialer configuration for users using VPN dialers.

Syntax

No parameters.

Example

The output of this command shows the VPN dialer configuration for remote Users.

```
(host) # show vpn-dialer remoteUser

remoteUser
----------
Attribute           Value
---------           -----
PPTP                disabled
L2TP                enabled
DNETCLEAR           disabled
WIREDNOWIFI         disabled
PAP                 enabled
CHAP                enabled
MSCHAP              enabled
MSCHAPV2            enabled
CACHE-SECURID       disabled
IKESECS             4000
IKEENC              3DES
IKEGROUP            ONE
IKEHASH             MD5
IKEAUTH             PRE-SHARE
IKEPASSWD           ********
IPSECSECS           4000
IPSECGROUP          GROUP1
IPSECENC            ESP-3DES
IPSECAUTH           ESP-MD5-HMAC
SECURID_NEWPINMODE  disabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show vrrp

```
show vrrp {{<vrid>[statistics]}|ipv6{<vrid>|stats[all]}|stats[all]|summary}
```

Description

Displays the list of all VRRP configuration on the managed device. To view a specific VRRP configuration, specify the VRID number.

Syntax

Parameter	Description	Range	Default
`<vrid>`	Displays the Virtual Router Id.	1-255	—
`ipv6`	Display VRRP information for IPv6 address.	—	—
`stats`	Displays the operational statistics of the VRRP.	—	—
`summary`	Displays the number of vrrp instances for IPv4 and IPv6.	—	—

Example

The output of the following command shows the VRRP IPv4 instance with vrid 1.

```
(host) [mynode] #show vrrp
Virtual Router 1:
Description
Admin State UP, VR State BACKUP
IP Address 0.0.0.0, MAC Address 00:00:5e:00:01:01, vlan 99
Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
Hold time 45 sec
Auth type NONE ********
tracking is not enabled
```

The output of the following command shows the statistics for IPv4 vrrp instance with vrid 10.

```
(host) [mynode] # show vrrp 10 statistics
Virtual Router 10:
Admin State UP, VR State MASTER
Advertisements:
Sent:                            249562   Received:                          475
Zero priority sent:                   0   Zero priority received:              0
Lower IP address received           475   Lower Priority received              3
Tracking priority overflow:           0
Advertisements received errors:
Interval mismatch                     0   Invalid TTL                          0
Invalid packet type                   0   Authentication failure               0
Invalid auth type                     0   Mismatch auth type                   0
Invalid VRRP IP address               0   Invalid packet length                0
VRRP Up timestamp:                        Fri Aug 23 15:49:27 2013
Master Up timestamp:                      Mon Aug 26 11:59:44 2013
Last advertisement sent timestamp:        Mon Aug 26 16:38:55 2013
Last advertisement received timestamp:    Mon Aug 26 11:59:44 2013
Current time:                             Mon Aug 26 16:38:55 2013
Number times became VRRP Master:      2
```

The output of the following command provides information about IPv6 VRRP instances.

```
(host) [mynode] # show vrrp ipv6
```

```
Virtual Router 1:
   Description
   Admin State DOWN, VR State INIT
   IPv6 Address ::
   MAC Address 00:00:5e:00:02:01, vlan 0
   Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
   tracking is not enabled
Virtual Router 23:
   Description
   Admin State DOWN, VR State INIT
   IPv6 Address ::
   MAC Address 00:00:5e:00:02:17, vlan 0
   Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
   tracking is not enabled
Virtual Router 255:
   Description
   Admin State UP, VR State MASTER
   IPv6 Address 2006::25
   MAC Address 00:00:5e:00:02:ff, vlan 521
   Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
   tracking is not enabled
```

The output of the following command shows the statistics for IPv6 VRRP instances.

```
(host) [mynode] #show vrrp ipv6 stats all
Virtual Router 1:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                                 0   Received:                         0
Zero priority sent:                   0   Zero priority received:           0
Lower IP address received             0   Lower Priority received           0
Tracking priority overflow:           0
Advertisements received errors:
Interval mismatch                     0   Invalid TTL                       0
Invalid packet type                   0
Invalid VRRP IP address               0   Invalid packet length             0
VRRP Up timestamp:                    N/A, DOWN
Master Up timestamp:                  N/A, not MASTER
Last advertisement sent timestamp:    never
Last advertisement received timestamp:   never
Current time:                         Wed Sep 25 19:40:42 2013
Number times became VRRP Master:      0
Virtual Router 23:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                                 0   Received:                         0
Zero priority sent:                   0   Zero priority received:           0
Lower IP address received             0   Lower Priority received           0
Tracking priority overflow:           0
Advertisements received errors:
Interval mismatch                     0   Invalid TTL                       0
Invalid packet type                   0
Invalid VRRP IP address               0   Invalid packet length             0
VRRP Up timestamp:                    N/A, DOWN
Master Up timestamp:                  N/A, not MASTER
Last advertisement sent timestamp:    never
Last advertisement received timestamp:   never
Current time:                         Wed Sep 25 19:40:42 2013
Number times became VRRP Master:      0
```

The output of the following command shows VRRP IPv4 and IPv6 instances.

```
(host) [mynode] #show vrrp summary
Number of exisitng VRRP IPv4 instances :    2
```

```
Number of exisitng VRRP IPv6 instances :    3
```

The output of the following command shows the configuration for all IPv6 VRRP instances.

```
(host) [mynode] #show vrrp ipv6
Virtual Router 1:
   Description
   Admin State DOWN, VR State INIT
   IPv6 Address ::
   MAC Address 00:00:5e:00:02:01, vlan 0
   Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
   tracking is not enabled
Virtual Router 23:
   Description
   Admin State DOWN, VR State INIT
   IPv6 Address ::
   MAC Address 00:00:5e:00:02:17, vlan 0
   Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
   tracking is not enabled
Virtual Router 255:
   Description
   Admin State UP, VR State MASTER
   IPv6 Address 2006::25
   MAC Address 00:00:5e:00:02:ff, vlan 521
   Priority 100, Advertisement 1 sec, Preemption Disable Delay 0
   tracking is not enabled
```

The output of the following command shows the statistics for IPv4 VRRP instances.

```
(host) [mynode] #show vrrp stats all
Virtual Router 1:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                                0   Received:                          0
Zero priority sent:                  0   Zero priority received:            0
Lower IP address received            0   Lower Priority received            0
Tracking priority overflow:          0
Advertisements received errors:
Interval mismatch                    0   Invalid TTL                        0
Invalid packet type                  0   Authentication failure             0
Invalid auth type                    0   Mismatch auth type                 0
Invalid VRRP IP address              0   Invalid packet length              0
VRRP Up timestamp:                       N/A, DOWN
Master Up timestamp:                     N/A, not MASTER
Last advertisement sent timestamp:       never
Last advertisement received timestamp:   never
Current time:                            Wed Sep 25 19:55:33 2013
Number times became VRRP Master:         0
Virtual Router 23:
Admin State DOWN, VR State INIT
Advertisements:
Sent:                                0   Received:                          0
Zero priority sent:                  0   Zero priority received:            0
Lower IP address received            0   Lower Priority received            0
Tracking priority overflow:          0
Advertisements received errors:
Interval mismatch                    0   Invalid TTL                        0
Invalid packet type                  0   Authentication failure             0
Invalid auth type                    0   Mismatch auth type                 0
Invalid VRRP IP address              0   Invalid packet length              0
VRRP Up timestamp:                       N/A, DOWN
Master Up timestamp:                     N/A, not MASTER
Last advertisement sent timestamp:       never
Last advertisement received timestamp:   never
```

```
Current time:                           Wed Sep 25 19:55:33 2013
Number times became VRRP Master:        0
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config or Enable mode on Mobility Master

show web-cc

```
show web-cc
   categories
   reputation
   md
      stats
   mm
      stats
   stats
   status
   global-bandwidth-contract all|{web-cc-category <category>}|{web-cc-reputation <reputation>}
```

Description

Display information about web content (web-cc) classification settings, category and reputation types, classification statistics and bandwidth contracts.

Syntax

Parameter	Description
`categories`	Display the category index number and the category name for each category type.
`md stats`	Display web content classification table statistics for the managed device. This command must be issued on the managed device.
`mm stats`	Display web content classification table statistics for Mobility Master.
`reputation`	Display the different reputation levels, and the range of reputation scores associated with each level.
`stats`	Display counters for web content traffic and web content classification table statistics
`status`	Display information about the current operational status of the web content classification feature.
`global-bandwidth-contract`	Display settings for global bandwidth contracts assigned to web content classification category types and reputation levels.
`all`	Show all bandwidth contracts
`web-cc-category <category>`	Display information for the specified web-cc category bandwidth contract.
`web-cc-reputation <reputation>`	Display information for the specified web-cc reputation bandwidth contract.

Usage Guidelines

The web content classification feature classifies all (HTTP) web traffic on the network. The output of the **show web-cc** command displays information about Webroot classification categories and risk reputation levels, bandwidth contracts, and the web content classification cache and database.

Examples

To see if the WebCC feature is able to send queries from Mobility Master to the WebRoot server in the cloud, issue the command **show web-cc status**.

```
(host)[mynode](config) #show web-cc status
Web Content Classification Status
---------------------------------
Service Status
------- ------
Web Content Classification enabled :    Yes
DNS/Name Server configured :            Yes
URL Cloud lookup server reachable :     Yes
Mode:                                   MM
Cloud lookup/update available :         Yes
```

A status of **Yes** in the **Cloud lookup/update field** indicates that license pool for that configuration node has a sufficient number of unexpired Web Content Classification licenses. A status of **No** indicates that licenses have expired, or that there are not enough licenses for the managed devices in that pool. The **Mode** field indicates operational mode for the WebCC feature. If the managed device is in the default centralized WebCC mode, Mobility Master (MM) contacts the WebRoot server for URL queries. If the managed device (MD)is in distributed mode, the managed device contacts the WebRoot server directly.

The following command shows the global bandwidth contracts applied to upstream and downstream traffic matching the **music** content category.

```
(host)#how web-cc global-bandwidth-contract web-cc-category music
Web-cc Global Bandwidth Contract
--------------------------------
Web-cc Category/Reputation  Direction   Rate (bits/second)  Contract    Id
--------------------------  ---------   ------------------  --------    --
web-cc-category music       Upstream    55000000            music-2126  2
web-cc-category music       Downstream  20000000            music-745c  1
```

The output of the **show web-cc** command varies, depending upon the parameters specified. The following table describes the information displayed in the output of this command when that parameter is included.

Parameter	Description
`categories`	Include this parameter to display the following information categories in the command output: ■ **Name**: names of the available web content classification catetories ■ **Web Category ID**: ID number associated with a category name.
`reputation`	Include this parameter to display the following information categories in the command output: ■ **RiskLevel**: names of the available web content classification risk levels ■ **Score**: Range of risk scores associated with a risk level

Parameter	Description
`Stats`	Include this parameter to display the following information categories in the command output: ■ **URL miss from sos**: number of times a URL was not found in the internal web content classification cache. ■ **Database hit:** number of times a URL was not found in the interal web content classification cache, but was found by the local web content classification database. ■ **Cloud lookup**: number of times a URL was not found by the local web content classification database, and was sent to the cloud for identification. ■ **Cloud response**: number of times the cloud responded to a cloud lookup request. ■ **RTU updates**: Number of times that the internal web content classification cache was udpated ■ **DB Entries**: Maximum number of entries allowed in the local web content classification database. This value varies by controller type.
`Status`	Include this parameter to display the following information categories in the command output: ■ **Web Content Classification enabled**: Shows if the web content classification feature is enabled or disabled. ■ **DNS/Name Server configured**: Shows if DNS is configured on the controller. The web content classification feature uses DNS to identify the URL cloud server, so DNS must be configured on the controller for this feature to work. ■ **URL Cloud lookup server reachabl**e: Indicates if the controller is able to contact the URL cloud server. ■ **Mode**: Indicates operational mode for the WebCC feature. If the managed device is in centralized mode, the Mobility Master (MM) will contact the WebRoot server for URL queries. If the managed device is in distributed mode, the managed device will contact the WebRoot server directly. ■ **Cloud lookup/update available**: A status of **Yes** indicates if the license pool has a sufficient number of unexpired Web Content Classification licenses. A status of **No** indicates that licenses have expired, or that there are not enough licenses for the managed devices in that pool.
`global-bandwidth-contract`	Include this parameter to display the following information categories in the command output: ■ **Web-cc Category/Reputation**: Name of the web content classification category or reputation level. ■ **Direction:** indicates whether the contract applies to upstream or downstream traffic. ■ **Rate (bits/second) :** bandwidth contract rate, in bits/second. ■ **Contract:** unique name assigned to the web-cc global bandwidth contract. ■ **Id:** identification number assigned to the web-cc global bandwidth contract.

Related Commands

Command	Description	Mode
web-cc	This command defines global bandwidth contracts for HTTP traffic matching a predefined web content category or reputation type.	Config mode

Command History

Release	Modification
ArubaOS 8.2.0.0	The **Mode** and **Cloud lookup/update available** fields were added to the output of the **show webcc-status** command.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show web-proxy

```
show web-proxy
```

Description

Displays information about the port and server configured for the web-proxy.

Example

The following command shows the port configured for the web-proxy server.

```
(host) [mynode] #show web-proxy
  Server: exampleproxy.com
  port: 8080
```

Related Commands

Command	Description	Mode
web-proxy server	This command configures the web-proxy server related information.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show web-server

```
show web-server
   profile
   statistics
```

Description

Displays the configuration and statistics of the controller's web server.

Syntax

Parameter	Description	Range	Default
`profile`	Displays the web server configuration profile.	—	—
`statistics`	Displays the web server statistics. This command helps to troubleshoot Captive Portal scale issues.	—	—

Example

The output of this command shows the web-server configuration.

```
(host) [mynode]# show web-server profile

Web Server Configuration
------------------------
Parameter                                       Value                  Set
---------                                       -----                  ---
Cipher Suite Strength                           high
SSL/TLS Protocol Config                         tlsv1 tlsv1.1 tlsv1.2
Switch Certificate                              default-self-signed
Captive Portal Certificate                      default
IDP Certificate                                 default-self-signed
Management user's WebUI access method           username/password
User absolute session timeout <30-3600> (seconds)  0
User session timeout <30-3600> (seconds)        900
Maximum supported concurrent clients <25-320>   25
Enable WebUI access on HTTPS port (443)         false
Enable bypass captive portal landing page       false
Exclude Security Headers from HTTP Response     false
```

The output of this command displays the web-server statistics.

```
(host) #show web-server statistics

Web Server Statistics:
----------------------
Current Request Rate:            1 Req/Sec
Current Traffic Rate:            0 KB/Sec
Busy Connection Slots:           1
Available Connection Slots:      24
Total Requests Since Up Time:    16854
Total Traffic Since Up Time:     199580 KB
Avg. Request Rate Since Up Time: 0 Req/Sec
Avg. Traffic Rate Since Up Time: 321 Bytes/Sec
Server Scoreboard ____________W____________

Scoreboard Key: _ - Waiting for Connection, s - Starting up
                R - Reading Request, W - Sending Reply
```

```
K - Keepalive, D - DNS Lookup
C - Closing connection, L - Logging
G - Gracefully finishing, I - Idle cleanup of worker
. - Open slot with no current process
```

The output of the **show web-server statistics** command includes the following parameters.

Parameter	Description
`Current Request Rate`	HTTP/HTTPS request rate measured immediately within the last one second.
`Current Traffic Rate`	HTTP/HTTPS data transfer rate measured immediately within the last one second.
`Busy Connection Slots`	Number of simultaneous HTTP/HTTPS sessions currently being served. Each session occupy one slot from the total available slot configured under the **web-max-clients <web-max-client>** parameter.
`Available Connection Slots`	Number of simultaneous HTTP/HTTPS sessions which can be served more than what is being served currently.
`Total Requests Since Up Time`	Total number of HTTP/HTTPS requests received by the web server since the server was up.
`Total Traffic Since Up Time`	Total number of HTTP/HTTPS traffic handled by the web server since the server was up.
`Avg. Request Rate Since Up Time`	Lifetime average of HTTP/HTTPS request rate. This is calculated by dividing the total number of requests received with the web server up-time.
`Avg. Traffic Rate Since Up Time`	Lifetime average of HTTP/HTTPS traffic rate. This is calculated by dividing the total of HTTP/HTTPS traffic with the web server up-time.
`Server Scoreboard`	Displays information of each worker thread of web server.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show websocket

```
show websocket
   clearpass                Show the ClearPass WebSocket Profile
   debug                    Show Web-Socket Interface debug information
   state                    Show Web-Socket connection state
   statistics               Show Web-Socket Interface Statistics
```

Description

Displays the ClearPass WebSocket configuration.

Syntax

Parameter	Description
`clearpass`	Shows the ClearPass WebSocket profile.
`debug`	Shows the WebSocket interface debug information.
`state`	Shows the WebSocket connection state.
`statistics`	Shows the WebSocket Interface statistics.

Example

The output of the following command displays the ClearPass WebSocket profile.

```
(host) [mynode] #show websocket clearpass
ClearPass WebSocket Profile
---------------------------
Parameter                          Value
---------                          -----
ClearPass WebSocket Interface      Enabled
Primary ClearPass Insight Server   10.4.174.104:443 apiadmin/********
Secondary ClearPass Insight Server 10.4.174.105:443 apiadmin/********
```

The output of the following command displays the WebSocket interface debug information.

```
(host) [mynode] #show websocket debug clearpass
ClearPass WebSocket Interface Debug Information
-----------------------------------------------
#Active-DevId-Table  #Working-Queue
------------------  --------------
2                   1
```

The output of the following command displays the current connection state of the ClearPass WebSocket interface that is configured.

```
(host) [mynode] #show websocket state clearpass

ClearPass Web-Socket Connection State [Interface: Enabled]
----------------------------------------------------------
Server                          State
------                          -----
Primary:    SECIRTY67.ACMECOMPANY.COM:443  DOWN
Secondary:  10.17.5.210:443               UP[08/22/16 13:38:50]Established
```

The output of this command includes the following parameters.

Parameter	Description
Server	Displays the primary and secondary ClearPass Insight server.
State	Displays the state of the primary and secondary ClearPass Insight server, which is either UP or DOWN.

The output of the following command displays the current statistics of ClearPass WebSocket interface.

```
(host) [mynode] #show websocket statistics clearpass

ClearPass WebSocket Interface Statistics Summary
------------------------------------------------
DevId Replayed  DevId Created  DevId Deleted  SUB Item Sent  SUB Msg Sent  UNSUB Item Sent
UNSUB Msg Sent  PUB Item Received  PUB Item Posted
--------------  -------------  -------------  -------------  ------------  ---------------  --
------------  -----------------  ---------------
0               10             0              10             1             0                0
              0                  0
```

The output of this command includes the following parameters.

Parameter	Description
DevId Replayed	Counter to track the number of device Ids replayed.
DevId Created	Counter to track the number of device Ids created.
DevId Deleted	Counter to track the number of device Ids deleted.
SUB Item Sent	When an interface is established, the existing device Ids are re-played and sent as sub items to ClearPass.
SUB Msg Sent	Counter to track the sub items that are consolidated and sent to ClearPass as sub messages.
UNSUB Item Sent	Counter to track the sub items sent to ClearPass, when ever a device Id is deleted.
UNSUB Msg Sent	Counter to track the deleted sub items consolidated as a sub message and sent to ClearPass.
PUB Item Received	When a subscribed profile for a specific station is updated in the ClearPass Insight server, a PUB message with the station's device profile information is sent back to the controller through the WebSocket connection. This event is mapped to the ArubaOS device type data.
PUB Item Posted	Counter to track the items successfully posted.

Command History

Release	Modification
ArubaOS 8.0.1.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on managed devices.

show whitelist-db cpsec

```
show whitelist-db cpsec
   cert-type {factory-cert|switch-cert}
   mac-address <name>
   page <num>
   start <offset>
   state {approved-ready-for-cert|certified-factory-cert|unapproved-factory-cert|unapproved-
   no-cert}
```

Description

Display the campus AP whitelist for campus APs using the control plane security feature.

Syntax

Parameter	Description
`cert-type factory-cert|switch-cert`	■ **factory-cert**: Use this parameter if AP is using a factory certificate. ■ **switch-cert**: Use this parameter if AP is using a certificate signed by the switch
`mac-address <name>`	MAC address of the campus AP you want to enter into the CPsec whitelist database.
`page <num>`	ArubaOS CLI displays 50 whitelist database entries per page. Filter the output of this command by displaying information starting at the specified page number.
`start <offset>`	Start displaying the table at the specified record in the database
`state approved-ready-for-cert certified-factory-cert unapproved-factory-cert unapproved-no-cert`	■ **approved-ready-for-cert**: AP in Approved state and is ready to receive a certificate. ■ **certified-factory-cert**: AP in Certified state and has a factory certificate. ■ **unapproved-factory-cert**: AP in Unapproved state and has a factory certificate. ■ **unapproved-no-cert**: AP in Unapproved state and has no or unknown certificate.

Usage Guidelines

Use this command to display the contents of the control plane security whitelist. To view information for a single AP, use the command **show whitelist-db cpsec mac-address <mac-address>**. To view a list of all secure APs on your controller, use the command **show whitelist-db cpsec**. If your deployment includes both Mobility Master and managed devices, then the campus AP whitelist on every managed device contains an entry for every secure AP on the network, regardless of the managed device to which it is connected.

Example

The output of the following command shows the campus AP whitelist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host) #show whitelist-db cpsec mac-address 00:16:CF:AF:3E:E1

Control-Plane Security Whitelist-entry Details
----------------------------------------------
MAC-Address        AP-Group     AP-Name         Enable    State
-----------        --------     -------         ------    -----
```

```
00:16:CF:AF:3E:E1  employee     ap-office1      Enabled   cert-cont-cert

Cert-Type    Description  Revoke Text  Last Updated
---------    -----------  -----------  ------------
switch-cert                            Fri Oct 16 01:21:09 2009

Whitelist Entries: 1
```

The output of this command includes the following parameters:

Parameter	Description
`MAC-Address`	MAC address of the campus AP.
`Enable`	Shows whether the campus AP has been enabled or disabled.
`State`	Shows the current state of the campus AP. ■ **unapproved-no-cert**: AP has no certificate and is not approved. ■ **unapproved-factory-cert:** AP has a preinstalled certificate that was not approved. ■ **approved-ready-for-cert**: AP is valid, but is waiting to receive a certificate. ■ **certified-factory-cert**: AP has an approved factory-installed certificate ■ **certified-controller-cert**: AP has an approved certificate from the managed device. ■ **certified-hold-factory-cert**: An AP is put in this state when the managed device thinks the AP has been certified with a factory certificate yet the AP requests to be certified again. Since this is not a normal condition, the AP will not be reapproved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised. ■ **certified-hold-controller-cert**: An AP is put in this state when the managed device thinks the AP has been certified with a managed device certificate yet the AP requests to be certified again. Since this is not a normal condition, the AP will not be reapproved as a secure AP until a network administrator manually changes the status of the AP to verify that it is not compromised.
`Cert-Type`	Type of certificate used by the AP. ■ **switch-cert**: AP received a certificate from the managed device ■ **factory-cert**: AP has a factory-installed certificate
`Description`	If you included an optional description when you added the AP to the campus AP whitelist, that description will appear here.
`Revoke Text`	If you included an optional revoke description when you manually revoked the AP, that description will appear here.
`Last Updated`	Date and time that the AP record was last updated in the database.

Related Commands

Command	Description	Mode
whitelist-db cpsec add mac-address <name>	Configure the campus AP whitelist for the control plane security feature.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db cpsec-local-switch-list

```
show whitelist-db cpsec-local-switch-list [mac-address <mac-address>]
```

Description

Display the list of managed devices with APs using the control plane security feature.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the managed device whose data you want to view.

Usage Guidelines

When you use the control plane feature on a network with Mobility Master and managed devices, Mobility Master maintains a whitelist of managed devices with APs using control plane security. When you change a campus AP whitelist on any managed device, that managed device contacts Mobility Master to check the local switch whitelist, then contacts every other managed device on the local managed device whitelist to notify it of the change. This allows an AP to move between managed devices and still stay connected to the secure network.

To view information for a single managed device, use the command **show whitelist-db cpsec-local-switch-list mac-address <mac-address>**. To view a list of all managed devices, use the command **show whitelist-db cpsec-local-switch-list**.

Example

The following command shows information for all managed devices in the managed device whitelist:

```
(host) #show whitelist-db cpsec-local-switch-list
Registered Local Switch Details
-----------------------------------
MAC-Address        IP-Address  Sequence Number  Remote Sequence Number  NULL Update Count
-----------        ----------  ---------------  ----------------------  -----------------
00:0b:86:51:a5:4c 10.3.53.2               3    1
0
00:A0:C9:14:C8:29 10.3.53.4               3    0
0
Local Purge  Remote Purge  Remote Last-Seq  Last Update Sent           Last Update Received
-----------  ------------  ---------------  ----------------           --------------------
0            0              2                Mon May 4 13:33:29 2013   Mon May 4 13:33:18 2013
0            0              2                Mon May 4 13:32:55 2013   Mon May 4 13:32:19 2013

Whitelist Entries: 2
```

The output of this command includes the following information:

Parameter	Description
`MAC-Address`	MAC address of the managed device.
`IP-Address`	IP address of the managed device.

Parameter	Description
`Sequence Number`	The number of times the managed device in the whitelist received and acknowledged a campus AP whitelist change from Mobility Master. In the example above, both managed devices received and acknowledged three campus AP whitelist changes sent from Mobility Master.
`Remote Sequence Number`	The number of times that Mobility Master has received and acknowledged a campus AP whitelist change from the managed device in the whitelist. In the example above, Mobility Master received and acknowledged a single campus AP whitelist change from the managed device with the MAC address 00:0b:86:51:a5:4c.
`Null Update Count`	The number of times the managed device has checked its control plane security whitelist and found nothing to synchronize with the remote managed device. By default, the managed device compares its control plane security whitelist against whitelists on other managed devices every minute. If the null update count reaches 5, the managed device will send an “empty sync” heartbeat to the remote managed device to ensure the sequence numbers on both managed devices are the same, then reset the null update count to zero.

Related Commands

Command	Description	Mode
whitelist-db cpsec-local-switch-list	Configure the managed device whitelist for the control plane security feature.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db cpsec-master-switch-list

```
show whitelist-db cpsec-master-switch-list [mac-address <mac-address>]
```

Description

Display the master switch list whitelist on managed devices with APs using the control plane security feature.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of Mobility Master.

Usage Guidelines

When you use the control plane feature on a network with both Mobility Master and managed devices, each managed device has a master switch whitelist which contains the IP and MAC addresses of Mobility Master. If your network has a redundant Mobility Master, then this whitelist will contain more than one entry.

To view information for a single Mobility Master, use the command **show whitelist-db cpsec-master-switch-list mac-address <mac-address>**. To view a list of all Mobility Masters, use the command **show whitelist-db cpsec-master-switch-list**.

Example

The following command shows that the managed devices have a single Mobility Master with the IP address 10.3.53.3:

```
(host) #show whitelist-db cpsec-master-list
Registered Master Switch Details
--------------------------------
Active  MAC-Address        IP-Address  Sequence Number  Remote Sequence Number  NULL Update
Count
------  -----------        ----------  ---------------  ----------------------  --------------
---
1       00:0b:86:61:ed:6c  10.3.53.11  1                3                       1
Local Purge  Remote Purge  Remote Last-Seq  Last Update Sent          Last Update Received
-----------  ------------  ---------------  ----------------          --------------------
0            0             1                Tue Aug  2 13:33:29 2012  Tue Aug  2 13:33:18 2012
```

The output of this command includes

Syntax

Parameter	Description
`MAC-Address`	MAC address of Mobility Master.
`IP-Address`	IP address of Mobility Master.

Parameter	Description
`Sequence Number`	The number of times Mobility Master in the whitelist received and acknowledged a campus AP whitelist change from the managed device. In the example above, Mobility Master received and acknowledged one campus AP whitelist change from the managed device.
`Remote Sequence Number`	The number of times that the managed device has received and acknowledged a campus AP whitelist change from the Mobility Master in the whitelist. In the example above, the managed device received and acknowledged three campus AP whitelist updates from Mobility Master.
`Null Update Count`	The number of times the managed device has checked its control plane security whitelist and found nothing to synchronize with Mobility Master. By default, the managed device compares its control plane security whitelist against whitelists on other managed devices every minute. If the null update count reaches 5, the managed device will send an “empty sync” heartbeat to the remote managed device to ensure the sequence numbers on both managed devices are the same, then reset the null update count to zero.

Related Commands

Command	Description	Mode
whitelist-db cpsec-master-switch-list	Configure the Mobility Master whitelist for the control plane security feature.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db cpsec-seq

```
show whitelist-db cpsec-seq
```

Description

Display the current sequence number for the Mobility Master or managed device whitelists.

Syntax

No Parameters

Usage Guidelines

The current sequence number in the **Sequence Number Details** table shows the number of changes to the campus AP whitelist made on this managed device.

Each managed device compares its campus AP whitelist against whitelists on other managed devices every two minutes. If a managed device detects a difference, it will send its changes to the other managed devices on the network. If all other managed devices on the network have successfully received and acknowledged all whitelist changes made on this managed device, every entry in the **sequence number** column in the managed device whitelist will have the same value as the number displayed in the **Sequence Number Details** table. If a managed device in the Mobility Master or managed device whitelist has a lower sequence number, that managed device may still be waiting to complete its update, or its update acknowledgement may not have yet been received.

Example

The output of the first command below shows that the campus AP whitelist has been updated 3 times on Mobility Master. The second command shows the managed device list on Mobility Master, and verifies that both managed devices have received and acknowledged all three of these changes.

```
(host) #show whitelist-db cpsec-seq
Sequence Number Details
-----------------------
Table Name       Current Seq Number
----------       ------------------
cpsec_whitelist  3

Whitelist Entries: 97

(host) # show whitelist-db cpsec-local-list
Registered Local Controller Details
-----------------------------------
MAC-Address        IP-Address  Sequence Number  Remote Sequence Number  NULL Update Count
-----------        ----------  ---------------  ----------------------  -----------------
00:0b:86:51:a5:4c 10.3.53.2               3    1
0
00:A0:C9:14:C8:29 10.3.53.4               3    0
0

Whitelist Entries: 2
```

Related Commands

Command	Description	Mode
whitelist-db cpsec add mac-address <name>	Configure the campus AP whitelist for the control plane security feature.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db cpsec-status

```
show whitelist-db cpsec-status
   [lms-list]
```

Description

Display aggregate status information APs in the campus AP whitelist.

Syntax

Parameter	Description
`lms-list`	Displays a list of LMS IP addresses.

Example

The output of the following command shows current status information for all APs in the campus AP whitelist:

```
(host) #show whitelist-db cpsec-status

My Mac-Address                00:1a:1e:00:89:b8
My IP-Address                 192.0.2.1
Master IP-Address             192.0.2.1
Switch-Role                   Master
Whitelist-sync is enabled

Entries in Whitelist database

Total entries:                41
Approved entries:              0
Unapproved entries:            0
Certified entries:            40
Certified hold entries:        0
Revoked entries:               1
Marked for deletion entries:   0
Current Sequence Number:       0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db rap

```
show whitelist-db rap
   apgroup <ap-group>
   apname <ap-name>
   export-css <filename>
   fullname <full-name>
   long
   mac-address <address>
   page <num>
   start <offset>
```

Description

View detailed information for the remote AP whitelist database.

Syntax

Parameter	Description
`apgroup <ap-group>`	Display specific AP-entries for this AP-group.
`apname <ap-name>`	Display specific AP-entry for this AP-name.
`export-css`	Export the remote AP white list to a file in the managed device's /flash/config/ folder. This file can be given to a content security provider to manage the remote AP database.
`fullname <full-name>`	Display specific AP-entry for this full-name in the RAP whitelist database.
`long`	Display additional debugging information about an entry in the RAP whitelist, including when it was last updated, the sequence number for the update, and any flags for the entry.
`mac-address <mac-addr>`	Display a whitelist entry for the specified RAP MAC address.
`page`	ArubaOS CLI displays 50 whitelist database entries per page. Filter the output of this command by displaying information starting at the specified page number.
`start <offset>`	Start displaying the table at the specified record in the database

Example

In the example below, the command output has been divided into two tables to fit on a single page of this document. In the CLI, this output would appear in a single, wide table.

```
(host) #show whitelist-db rap

AP-entry Details
----------------

Name               AP-Group  AP-Name       Full-Name    Authen-Username  Revoke-Text
----               --------  -------       ---------    ---------------  -----------
00:0b:86:c3:58:38  local     AP-5B         chucks_AP    Dev\Sarah
00:0b:86:66:01:aa  default   AP-5C         upstairs     Dev              AP invalid
00:1a:1e:c0:1b:e0  default   AP-99                      Dev\Chris
```

```
00:0b:86:66:03:3f  default   LAB-AP        addtl_rap    PM\Kumar
00:0b:86:66:02:09  default   LAB-AP

AP_Authenticated  Description  Date-Added                Enabled  Remote-IP
----------------  -----------  ----------                -------  -------
Authenticated                  Thu Mar  5 21:25:36 2009  Yes      192.0.2.3
Provisioned                    Thu Mar  5 21:25:49 2009  No       192.0.2.78
Authenticated                  Wed Mar  4 20:16:16 2009  Yes      192.0.2.6
Authenticated                  Tue May 19 07:53:29 2009  Yes      192.0.2.12
Provisioned                    Fri May  8 10:37:40 2009  Yes      192.0.2.13

AP Entries: 5
```

The output of this command includes the following information:

Parameter	Description
Name	MAC address of the remote AP.
AP-Group	Name of the AP group to which th remotee AP has been assigned.
AP-name	Name of the remote AP. If no name has been specified, this column will display the remote AP's MAC address
Full-name	Text string used to identify the remote AP. This field often describes the AP's user, and corresponds to the **User Name** field in the RAP whitelist in the WebUI.
Authen-Username	User name of the user who authenticated the remote AP. This parameter holds the user name of the user who authenticated the remote AP. This is related to the zero touch authentication feature, as a user needs authenticate an AP before it gets its complete configuration. Before the AP is authenticated, it is given a restricted configuration to allow users to perform captive portal authorization via the remote AP's ENET ports to authenticate the remote AP. The username used during captive portal authentication will be stored in this field. This cannot be added manually when creating a local-userdb-ap entry.
Revoke-Text	The command **whitelist-db rap revoke** includes an optional **revoke-comment** parameter that allows network administrators to explain why the remote AP was revoked. If a remote AP is revoked, and a revoke comment entered, this text appears in the **revoke-text** column in the **show whitelist-db rap**command. When a local DB entry is reenabled via the command **whitelist-db rap modify mac-addr mode enable**, this field is cleared.
AP_ Authenticated	This column indicates the authorization status of the RAP. A RAP can either be **Authenticated** or **Provisioned**. Remote APs that *do not* support certificated-based provisioning will always display a **Provisioned** status. Remote APs that support certificated-based provisioning can display either a **Authenticated** or **Provisioned** status, depending on their configuration and authentication status. ■ If the remote AP has a defined AP authorization profile, the remote AP will be in a "Provisioned" state with a limited configuration until it is authenticated. After it the remote AP has been authenticated, it will be in an "Authenticated" state. ■ If the remote AP does not have a defined AP authorization profile, the remote AP will be in a "Provisioned" state, but will still receive the full configuration assigned to that AP and its AP group.
Description	A text string used to further identify the remote AP.
Date-Added	Date and time that the AP was added to the local user database

Parameter	Description

`Enabled`	This column shows if the entry in the database is enabled or disabled. Database entries can be enabled or disabled using the CLI commands:
	`whitelist-db rap {add|modify} mac-address <mac-addr> mode {enable|disable}`
	and
	`whitelist-db rap revoke mac-address <mac-addr>`

Related Commands

Command	Description
whitelist-db rap add	Add, delete, modify or revoke remote AP entries in the current emote AP whitelist table.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices

show whitelist-db rap-local-switch-list

```
show whitelist-db rap-local-switch-list [mac-address <mac-address>]
```

Description

Display the remote AP whitelist local switch list on Mobility Master.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the managed device whose data you want to view.

Usage Guidelines

When you have remote APs on a network with both master and managed devices, Mobility Master maintains a whitelist of managed devices with remote APs. When you change a remote AP whitelist on any managed device, that managed device contacts Mobility Master to check the local switch whitelist, then contacts every other managed device on the local managed device whitelist to notify it of the change. This allows a remote AP to move between managed devices and still stay connected to the secure network.

To view information for a single managed device, use the command **show whitelist-db rap-local-switch-list mac-address <mac-address>**. To view a list of all managed devices, use the command **show whitelist-db rap-local-switch-list**.

Example

The following command shows information for all managed devices in the managed device whitelist. The output in the example below has been divided into sections to better fit on the pages of this document. In the ArubaOS CLI, the output appears in a single, long table.

```
(host) #show whitelist-db rap-local-switch-list


Active   MAC-Address        IP-Address          Sequence Number         Remote Sequence Number
-------  -----------        ----------          ---------------         ----------------------
1         00:0b:86:51:a5:4c 10.3.53.2   3                      1
1         00:A0:C9:14:C8:29 10.3.53.4   3                      0

NULL Update Count       Local Purge  Remote Purge  Remote Last-Seq  Last Update Sent
-----------------       -----------  ------------  ---------------  ----------------
0                       0            0              2                Mon May 4 13:33:29 2013
0                       0            0              2                Mon May 4 13:32:55 2013

Last Update Received
--------------------
Mon May 4 13:33:18 2013
Mon May 4 13:32:19 2013W

Whitelist Entries: 2
```

The output of this command includes the following information:

Parameter	Description
`Active`	Shows if the managed device is active on the network. ■ 1: Active ■ 0: Inactive
`MAC-Address`	MAC address of the managed device.
`IP-Address`	IP address of the managed device.
`Sequence Number`	The number of times the managed device in the whitelist received and acknowledged a remote AP whitelist change from Mobility Master. In the example above, both managed devices received and acknowledged three remote AP whitelist changes sent from Mobility Master.
`Remote Sequence Number`	The number of times that Mobility Master has received and acknowledged a remote AP whitelist change from the managed device in the whitelist. In the example above, Mobility Master received and acknowledged a single remote AP whitelist change from the managed device with the MAC address 00:0b:86:51:a5:4c.
`Null Update Count`	The number of times the managed device has checked its remote AP whitelist and found nothing to synchronize with the remote managed device. By default, the managed device compares its remote AP whitelist against whitelists on other managed devices every minute. If the null update count reaches 5, the managed device will send an “empty sync” heartbeat to the remote managed device to ensure the sequence numbers on both managed devices are the same, then reset the null update count to zero.

Related Commands

Command	Description	Mode
show whitelist-db rap-master-switch-list	Delete a Mobility Master from the master Mobility Master table used by the remote AP whitelist	Config mode
whitelist-db rap del	Remove an AP entry from the remote AP whitelist.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db rap-master-switch-list

```
show whitelist-db rap-local-switch-list [mac-address <mac-address>]
```

Description

Display the remote AP whitelist master switch list on managed devices with remote APs

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the managed device whose data you want to view.

Usage Guidelines

When your network has with both master and managed devices, each managed device with associated remote APs has a master switch whitelist which contains the IP and MAC addresses of Mobility Master. If your network has a redundant Mobility Master, then this whitelist will contain more than one entry.

To view information for a single Mobility Master, use the command **show whitelist-db rap-master-switch-list mac-address <mac-address>**. To view a list of all Mobility Masters, use the command **show whitelist-db rap-master-switch-list**.

Example

The following command shows that the managed devices have a single Mobility Master with the IP address 192.0.2.143. The output in the example below has been divided into sections to better fit on the pages of this document. In the ArubaOS CLI, the output appears in a single, long table.

```
Active   MAC-Address           IP-Address       Sequence Number         Remote Sequence
                                                                          Number
-------  -----------           ----------       ---------------         ---------------
1         00:0b:86:51:a5:4c   192.0.2.14        2                       2

NULL Update Count       Local Purge  Remote Purge  Remote Last-Seq  Last Update Sent
-----------------       -----------  ------------  ---------------  ----------------
0                       0            0              1               Mon May 4 12:44:24
0

Last Update Received
--------------------
Mon May 4 12:44:20

Whitelist Entries: 1
```

The output of this command includes the following information:

Parameter	Description
`Active`	Shows if the controller is active on the network. ■ 1: Active ■ 0: Inactive
`MAC-Address`	MAC address of Mobility Master.
`IP-Address`	IP address of Mobility Master.

Parameter	Description
`Sequence Number`	The number of times the Mobility Master in the whitelist received and acknowledged a remote AP whitelist change from the managed device. In the example above, the Mobility Masters received and acknowledged three remote AP whitelist changes sent from a managed device.
`Remote Sequence Number`	The number of times that the managed device has received and acknowledged a remote AP whitelist change from the Mobility Master in the whitelist.
`Null Update Count`	The number of times the managed device has checked its remote AP whitelist and found nothing to synchronize with the remote managed device. By default, the managed device compares its remote AP whitelist against whitelists on other managed devices every minute. If the null update count reaches 5, the managed device will send an “empty sync” heartbeat to the remote managed device to ensure the sequence numbers on both managed devices are the same, then reset the null update count to zero.

Related Commands

Command	Description	Mode
whitelist-db rap-local-switch-list	Delete a managed device from the local switch table used by the remote AP whitelist	Config mode
whitelist-db rap del	Remove an AP entry from the remote AP whitelist.	Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show whitelist-db rap-status

```
show whitelist-db rap-status
```

Description

Display aggregate status information APs in the remote AP whitelist.

Syntax

No parameters.

Example

The output of the following command shows current status information for all APs in the remote AP whitelist:

```
(host) #show whitelist-db rap-status
Entries in Whitelist database

Total entries:                41
Revoked entries:               1
Marked for deletion entries:   0
```

The output of this command includes

Syntax

Parameter	Description
`Total entries`	Total number of entries in the remote AP whitelist
`Revoked entries`	Number of remote APs whose entries have been revoked
`Marked for deletion entries`	Number of remote APs whose entries have been marked for deletion. An entry will not be permanently deleted until all other managed devices on the network acknowledge the deletion.

Related Commands

Command	Description
show whitelist-db rap-master-switch-list	Display the list of Mobility Masters with remote APs managed using the remote AP whitelist
show whitelist-db rap-local-switch-list	Display the list of managed devices with remote APs managed using the remote AP whitelist
show whitelist-db rap	View detailed information for the remote AP whitelist database.
whitelist-db rap add	Add an AP entry to the remote AP whitelist.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wired-blacklist-clients

```
show wired-blacklist-clients
```

Description

This command shows wired clients that are blacklisted.

Usage Guidelines

Issue this command to list the blacklisted wired clients.

Examples

```
(host) [mynode] (config)#show wired-blacklist-clients
```

The output of this command is as follows:

```
Wired user Blacklist table
--------------------------
MAC   AP name   Slot/Port   Reason   Blacklist Time (Sec)
---   -------   ---------   ------   --------------------
b4:b5:2f:8d:cc:96   ac:a3:1e:cd:36:84   0/1         session-blacklist   258
```

Related Commands

Command	Description	Mode
aaa authentication wired	This command configures authentication for a client device that is directly connected to a port on the managed device.	Config mode

Command History

Version	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show wlan anyspot-profile

```
show wlan anyspot-profile [<profile-name>]
```

Description

The output of this command displays configuration settings for a WLAN anyspot profile.

Syntax

Parameter	Description
<profile>	Name of an anyspot profile

Usage Guidelines

The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks. Issue this command without the **<profile>** parameter to display the entire anyspot profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Example

The following command displays configuration information for an active (enabled) anyspot profile with two excluded ESSIDs, and one preset ESSID.

```
Anyspot profile "default"
-------------------------
Parameter                                 Value
---------                                 -----
Enable Anyspot                            true
Exclude ESSID(s) (exact match)            corp_dev_1
Exclude ESSID(s) (exact match)            corp_voip_1
Exclude ESSID(s) (containing string(s))   N/A
Preset ESSID(s)                           corpGuest
```

Parameter	Description
enable-anyspot	Indicates if the anyspot feature is enabled or disabled.
exclude-essid <exclude-essid>	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the **Exclude ESSID** lists. ESSIDs from neighboring APs will automatically appear in this list as long as the anyspot-enabled AP can detect that ESSID.
exclude-wildcard <exclude-wildcard>	An anyspot-enabled radio will not respond to client probe requests using an ESSID that matches a string in the **Exclude ESSID (containing string) list.**
preset-essid <preset-essid>	If a client sends a probe request without an ESSID (that is, the probe request is not looking for a specific network) then the anyspot-enabled AP will respond to the probe request with an ESSID from this list.

Related Commands

Command	Description
wlan anyspot-profile	The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan bcn-rpt-req-profile

```
show wlan bcn-rpt-req-profile <profile-name>
```

Description

Shows configuration and other information about the parameters for the Beacon Report Request frames.

Syntax

Parameter	Description
<profile>	Name of a WLAN beacon report request profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the entire Beacon Report Request profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

For this profile to take effect, the 802.11K feature needs to be enabled.

Examples

```
(host) #show wlan bcn-rpt-req-profile
Beacon Report Request Profile List
----------------------------------
Name     References  Profile Status
----     ----------  --------------
default  1
test     0
Total:2
(host) #
(host) #show wlan bcn-rpt-req-profile default

Beacon Report Request Profile "default"
---------------------------------------
Parameter                          Value
---------                          -----
Interface                          1
Regulatory Class                   12
Channel                            9
Randomization Interval             100
Measurement Duration               100
Measurement Mode for Beacon Reports  active-all-ch
Reporting Condition                2
ESSID Name                         aruba-ap
Reporting Detail                   Disabled
Measurement Duration Mandatory     Disabled
Request Information values         0/21/22
```

The output of this command includes the following parameters:

Parameter	Description
`Interface`	Specifies the Radio interface for transmitting the Beacon Report Request frame. It can have a value of either 0 or 1.
`Regulatory Class`	Specifies the Regulatory Class field in the Beacon Report Request frame.
`Channel`	Specifies the Channel field in the Beacon Report Request frame.
`Randomization Interval`	Specifies the Randomization Interval field in the Beacon Report Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units).
`Measurement Duration`	Specifies the Measurement Duration field in the Beacon Report Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs.
`Measuremement Mode for Beacon Reports`	Specifies the mode used for the measurement. The valid measurement modes are: ■ active-all-ch ■ active-ch-rpt ■ beacon-table ■ passive
`Reporting Condition`	Specifies the value for the "Reporting Condition" field in the Beacon Reporting Information sub-element present in the Beacon Report Request frame.
`ESSID Name`	Specifies the value for the "SSID" field in the Beacon Report Request frame.
`Reporting Detail`	Indicates the value for the "Detail" field in the Reporting Detail sub-element present in the Beacon Report Request frame.
`Measurement Duration Mandatory`	Specifies the "Duration Mandatory" bit of the Measurement Request Mode field of the Beacon Report Request frame.
`Request Information values`	Indicates the contents of the Request Information IE that could be present in the Beacon Report Request frame. The Request Information IE is present for all Measurement Modes except the 'Beacon Table' mode. It consists of a list of Element IDs that should be included by the client in the response frame.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan dot11k-profile

```
show wlan dot11k-profile [<profile>]
```

Description

Show a list of all 802.11k profiles, or display detailed configuration information for a specific 802.11k profile.

Syntax

Parameter	Description
<profile>	Name of an 802.11k profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the 802.11k profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured 802.11k profiles. The **References** column lists the number of other profiles with references to the 802.11k profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan dot11k-profile

802.11K Profile List
--------------------
Name                            References  Profile Status
----                            ----------  --------------
default                         8
11kprofile2             1
Total: 2
```

The following example shows configuration settings defined for the profile **default**.

```
(host) #show wlan dot11k-profile default

802.11K Profile "default"
-------------------------
Parameter                                                       Value
---------                                                       -----
Advertise 802.11K Capability                                    Disabled
Forcefully disassociate on-hook voice clients                   Disabled
Measurement Mode for Beacon Reports                             beacon-table
Configure specific channel for Beacon Requests                  Disabled
Channel requested for Beacon Reports in 'A' band                36
Channel requested for Beacon Reports in 'BG' band               1
Time duration between consecutive Beacon Requests               60 sec
Time duration between consecutive Link Measurement Requests     60 sec
Time duration between consecutive Transmit Stream Measurement Requests  90 sec
```

The output of this command includes the following data columns:

Parameter	Description
Advertise 802.11K Capability	Shows if the profile has enabled or disabled the 802.11K feature.
Forcefully disassociate on-hook voice clients	If enabled, the AP may forcefully disassociate clients that reach the maximum CAC peak capacity or call handoff reservation.
Measurement Mode for Beacon Reports	Shows the profile's beacon measurement mode: ■ **active**: In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ■ **beacon-table**: In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. This is the default beacon measurement mode. ■ **passive**: In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master and managed devices.

show wlan dot11r-profile

```
show wlan dot11r-profile [<profile>]
```

Description

Show a list of all 802.11r profiles, or display detailed configuration information for a specific 802.11r profile.

Syntax

Parameter	Description
<profile>	Name of an 802.11r profile.

Usage Guidelines

Issue this command without the <profile> parameter to display the 802.11r profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured 802.11r profiles. The **References** column lists the number of other profiles with references to the 802.11r profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan dot11r-profile

802.11r Profile List
--------------------
Name              References  Profile Status
----              ----------  --------------
default           8
voice-enterprise  1

Total: 2
```

The following example shows configuration settings defined for the profile **default**.

```
(host) #show wlan dot11r-profile default
802.11r Profile "default"
-------------------------
Parameter                    Value
---------                    -----
Advertise 802.11r Capability  Disabled
802.11r Mobility Domain ID    1
802.11r R1 Key Duration       3600
802.11r R1 Key Assignment     dynamic
```

The output of this command includes the following data columns:

Parameter	Description
Advertise 802.11r Capability	Shows if the profile has enabled or disabled the 802.11r feature.

Parameter	Description
802.11r Mobility Domain ID	Shows the unique ID that identifies the mobility domain.
802.11r R1 Key Duration	Shows the r1 key timeout value in seconds for decrypt-tunnel or bridge mode.
`802.11r R1 Key Assignment`	Shows if the r1 key assignment is static or dynamic.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan edca-parameters-profile

```
show wlan edca-parameters-profile ap|station [<profile>]
```

Description

Display an EDCA profile for APs or for clients (stations). EDCA profiles are specific either to APs or clients.

Syntax

Parameter	Description
<profile>	Name of a EDCA Parameters profile.

Usage Guidelines

Issue this command without the <profile> parameter to display a EDCA Parameters profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has three EDCA Parameters profiles configured for stations. The **References** column lists the number of other profiles with references to the EDCA Parameters profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the Profile Status column.)

```
(host) #show wlan edca-parameters-profile station
EDCA Parameters profile (Station) List
----------------------------------
Name            References  Profile Status
----            ----------  --------------
station-corp1   3
station-corp2   1
testprofile     0

Total:3
```

The following example shows configuration settings defined for the profile **station-corp1**.

```
(host) #show wlan edca-parameters-profile ap station-corp1
EDCA Parameters
---------------
AC            ECWmin   ECWmax   AIFSN   TXOP   ACM
--            ------   ------   -----   ----   ---
Best-effort   4        6        3       0      0
Background    4        10       7       0      0
Video         3        4        1       94     0
Voice         2        3        1       47     0
```

The output of this command includes the following data columns:

Parameter	Description
AC	Name of an Access channel queue (**Best-effort**, **Background**, **Video** or **Voice**).

Parameter	Description
ECWmin	The exponential (n) value of the minimum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.
ECWmax	The exponential (n) value of the maximum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.
AIFSN	Arbitrary inter-frame space number.
TXOP	Transmission opportunity, in units of 32 microseconds.
ACM	If this column displays a 1, the profile has enabled mandatory admission control. If this column displays a 0, the profile has disabled this feature.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	This show command is available in the base operating system, but the controller must have the PEFNG license in order to configure EDCA Parameter Profiles.	Config or Enable mode on Mobility Master.

show wlan hotspot advertisement-profile

```
show wlan hotspot advertisement-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP advertisement profile.

Syntax

Parameter	Description
<profile>	Name of a wlan hotspot advertisement profile.

Usage Guidelines

ANQP profiles and H2QP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to view the ANQP and H2QP profiles to be associated with the advertisement profile.

Issue this command without the **<profile>** parameter to display the entire ANQP advertisement profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured advertisement profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) # show wlan hotspot advertisement-profile
Advertisement Profile List
--------------------------
Name           References  Profile Status
----           ----------  --------------
default        1
Westgate_Mall  2
Total:2.
```

This example displays the configuration settings for the profile **Wireless_rf_profile.**

```
(host) (config) #show wlan hotspot advertisement-profile Wireless_rf_profile
Advertisement Profile "default"
------------------------------
Parameter                              Value
---------                              -----
ANQP Venue Name Profile                venue_mall
ANQP Network Authentication Profile    auth1
ANQP Roaming Consortium Profile        default
ANQP NAI Realm Profile                 Realm2
ANQP 3GPP Cellular Network Profile     default
ANQP IP Address Availability Profile   ipv4_Profile
H2QP WAN Metrics Profile        default
H2QP Operator Friendly Name Profile    default
H2QP Connection Capability Profile     default
H2QP Operating Class Indication Profile default
ANQP Domain Name Profile               corp_domain
```

The output of this command includes the following parameters:

Parameter	Description
ANQP Venue Name Profile	Name of the ANQP Venue Name profile associated with this WLAN advertisement profile.
ANQP Network Authentication Profile	Name of the ANQP Network Authentication profile associated with this WLAN advertisement profile.
ANQP Roaming Consortium Profile	Name of the ANQP Roaming Consortium profile associated with this WLAN advertisement profile.
ANQP NAI Realm Profile	Name of the ANQP NAI Realm profile associated with this WLAN advertisement profile.
ANQP 3GPP Profile	Name of the ANQP 3GPP Cellular Network profile associated with this WLAN advertisement profile.
ANQP IP Address Availability Profile	Name of the ANQP IP Address Availability profile associated with this WLAN advertisement profile.
H2QP WAN Metrics Profile	Name of the H2QPWAN Metrics profile associated with this WLAN advertisement profile.
H2QP Operator Friendly Name Profile	Name of the H2QP Operator Friendly Name profile associated with this WLAN advertisement profile.
H2QP Connection Capability Profile	Name of the H2QP Connection Capability profile associated with this WLAN advertisement profile.
H2QP Operating Class Indication Profile	Name of the H2QP Operating Class Indication profile associated with this WLAN advertisement profile.
ANQP Domain Name Profile	Name of the ANQP domain name profile associated with this WLAN advertisement profile.

Related Commands

wlan hotspot advertisement-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-3gpp-nwk-profile

```
show wlan hotspot anqp-3gpp-nwk-profile [<profile-name>]
```

Description

This profile shows the configuration settings for for a 3GPP Cellular Network profile.

Syntax

Parameter	Description
<profile>	Name of a 3GPP Cellular Network profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Issue this command without the **<profile>**parameter to display the entire list of 3GPP profiles, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured 3GPP profiles. The **References** column lists the number of other profiles with references to the advertisement profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) (config)# show wlan hotspot anqp-3gpp-nwk-profile
ANQP 3GPP Cellular Network Profile List
---------------------------
Name           References  Profile Status
----           ----------  --------------
default        1
Updated_PLMN   2
Total:2.
```

This example displays the configuration settings for the profile **Updated_PLMN.**

```
(host) (config)# show wlan hotspot anqp-3gpp-nwk-profile Updated_PLMN
ANQP 3GPP Cellular Network Profile "Updated_PLMN"
-----------------------------------------
Parameter                       Value
---------                       -----
ANQP 3GPP network profile enable  Enabled
3GPP PLMN1                      310026
3GPP PLMN2                      208000
3GPP PLMN3                      208001
3GPP PLMN4                      N/A
3GPP PLMN5                      N/A
3GPP PLMN6                      N/A
```

The output of this command includes the following parameters:

Parameter	Description
`ANQP 3GPP network profile enable`	Shows if this profile has been enabled ANQP 3GPP Cellular Network profiles are disabled by default.
`3gpp PLMN1`	The Public Land Mobile Networks (PLMN) value of the highest-priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp PLMN2`	The Public Land Mobile Networks (PLMN) value of the second-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp PLMN3`	The Public Land Mobile Networks (PLMN) value of the third-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp PLMN4`	The Public Land Mobile Networks (PLMN) value of the fourth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp PLMN5`	The Public Land Mobile Networks (PLMN) value of the fifth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp PLMN6`	The Public Land Mobile Networks (PLMN) value of the sixth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).

Usage Guidelines

The 3GPP Cellular Network Profile defines an ANQP IE to be sent in a GAS query response from an AP in a hotspot with a roaming relationship with a cellular operator. The 3GPP mobile country code and the 12-bit Mobile Network Code data in the IE can help the client select a 3GPP network.

Values configured in this profile will not be sent to clients unless you:

1. Associate the 3GPP Cellular Network profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-3gpp-nwk-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Related Commands

wlan hotspot anqp-3gpp-nwk-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-domain-name-profile

```
show wlan hotspot anqp-domain-name-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP Domain Name profile.

Syntax

Parameter	Description
<profile>	Name of a Domain Name profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Issue this command without the **<profile>** parameter to display the entire ANQP Domain Name profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Domain Name profile an ANQP advertisement profile. (wlan hotspot advertisement-profile <profile-name> anqp-domain-name-profile)
2. Associate the ANQP advertisement profile with a Hotspot profile. (wlan hotspot h2-profile advertisement-profile <profile-name>)
3. Enable the hotspot feature within that Hotspot profile. (wlan hotspot h2-profile <profile-name>hotspot-enable)

Examples

The example below shows that the controller has two configuredDomain Name profiles. The **References** column lists the number of other profiles with references to the Domain Name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) # show wlan hotspot anqp-domain-name
ANQP Domain Name Profile List
-----------------------------
Name          References  Profile Status
----          ----------  --------------
corp_domain   2
default       1
Total:2.
```

This example displays the configuration settings for the profile **corp_domain.**

```
(host) #show wlan hotspot anqp-domain-name-profile corp_domain
ANQP Domain Name Profile "corp_domain"
--------------------------------------
Parameter     Value
---------     -----
Domain Name   example.com
```

The output of this command includes the following parameters:

Parameter	Description
Domain Name	Domain name of the hotspot operator.

Related Commands

wlan hotspot anqp-domain-name-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-ip-addr-avail-profile

```
show wlan hotspot anqp-ip-addr-avail-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP IP Address Availability profile.

Syntax

Parameter	Description
`<profile>`	Name of an IP Address Availability profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Issue this command without the **<profile>** parameter to display the entire ANQP IP Address Availability profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP IP Address Availability profile an ANQP advertisement profile.(`wlan hotspot advertisement profile <profile-name> anqp-ip-addr-avail-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Examples

The example below shows that the controller has three configured IP Address Availability profiles. The **References** column lists the number of other profiles with references to the IP Address Availability profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) # show wlan hotspot anqp-ip-addr-avail-profile
ANQP IP Address Availability Profile List
-----------------------------------------
Name          References  Profile Status
----          ----------  --------------
default       0
ipv4_Profile  2
ipv6_profile  1
Total:3.
```

This example displays the configuration settings for the profile **ipv4_Profile.**

```
(host) #show rf anqp-ip-addr-avail-profile ipv4_Profile
ANQP IP Address Availability Profile "ipv4_Profile"
-----------------------------------------------
Parameter                      Value
---------                      -----
IPv4 Address Availability Type  public
```

```
IPv6 Address Availability Type  not-available
The output of this command includes the following parameters:
```

Parameter	Description
IPv4 Address Availability Type	Indicates the availability of an IPv4 network. This parameter can display any of the following values: ■ availability-unknown: Network availability cannot be determined. ■ not-available : Network is not available. ■ port-restricted : Network has some ports restricted (for example, the network blocks port 110 to retrict POP mail). ■ port-restricted-double-nated : Network has some ports restricted and multiple routers performing network address translation. ■ port-restricted-single-nated : Network has some ports restricted and a single router performing network address translation. ■ private-double-nated : Network is a private network with multiple routers doing network address translation. ■ private-single-nated : Network is a private network a single router doing network address translation. ■ public : Network is a public network
IPv6 Address Availability Type	Indicates the availability of an IPv6 network. This parameter can display any of the following values: ■ available : An IPv6 network is available. ■ availability-unknown: Network availability cannot be determined. ■ not-available : Network is not available.

Related Commands

wlan hotspot anqp-ip-addr-avail-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-nai-realm-profile

```
show wlan hotspot anqp-nai-realm-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP Network Access Identifier (NAI) Realm profile.

Syntax

Parameter	Description
`<profile>`	Name of an NAI Realm profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Issue this command without the **<profile>** parameter to display the entire ANQP NAI Realm profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP NAI Realm profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-nai-realm-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Examples

The example below shows that the controller has three configured NAI Realm profiles. The References column lists the number of other profiles with references to the NAI Realm profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column

```
(host) # show wlan hotspot anqp-nai-realm-profile

ANQP NAI Realm Profile List
---------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
Realm1   2Realm2   2

Total:3.
```

This example displays the configuration settings for the profile **Realm2.**

```
(host) #show wlan hotspot anqp-nai-realm-profile Realm2
ANQP NAI Realm Profile "Realm2"
-------------------------------
Parameter                              Value
---------                              -----
NAI Realm name                         example.com
```

```
NAI Realm EAP Method                       eap-ttls
NAI Realm Authentication Parameter Type    expanded-eap
```

The output of this command includes the following parameters:

Parameter	Description
NAI Realm name	Name of the NAI realm. The realm name is often the domain name of the service provider.
NAI Realm EAP Method	The NAI Realm Authentication types sent as an ANQP IE in an GAS response
NAI Realm Authentication Parameter Type	The EAP authentication method supported by the hotspot realm.

Related Commands

wlan hotspot anqp-nai-realm-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-nwk-auth-profile

```
show wlan hotspot anqp-nwk-auth-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP network authentication profile.

Syntax

Parameter	Description
<profile>	Name of an ANQP Network Authentication profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Issue this command without the **<profile>** parameter to display the entire ANQP network authentication profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured network authentication profiles. The **References** column lists the number of other profiles with references to the network authentication profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show wlan hotspot anqp-nwk-auth-profile

ANQP Network Authentication Profile List
----------------------------------------
Name         References  Profile Status
----         ----------  --------------
auth1        0
default      0

Total:2.
```

The following example displays the configuration settings for the profile **default.**

```
(host) #show wlan hotspot anqp-nwk-auth-profile default

ANQP Network Authentication Profile "default"
-----------------------------------------------
Parameter                      Value
---------                      -----
Type of Network Authentication  acceptance
Redirect URL                   N/A
```

The output of this command includes the following parameters:

Parameter	Description
Type of Network Authentication	Network Authentication Type being used by the hotspot network. This parameter can be any of the following values: ■ acceptance: Network requires the user to accept terms and conditions. ■ dns-redirection: Additional information on the network is provided through DNS redirection. ■ http-https-redirection : Additional information on the network is provided through HTTP/HTTPS redirection. ■ online-enroll : Network supports online enrollment.
Redirect URL	If information on the network is provided through DNS redirection, this parameter displays the redirection URL.

Related Commands

wlan hotspot anqp-nwk-auth-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-roam-cons-profile

```
show wlan hotspot anqp-roam-cons-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP Roaming Consortium profile.

Syntax

Parameter	Description
<profile>	Name of an ANQP Roaming Consortium profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Issue this command without the <profile>parameter to display the entire ANQP Roaming Consortiumprofile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Roaming Consortium profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-roam-cons-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Examples

The example below shows that the controller has two configured Roaming Consortium profiles. The **References** column lists the number of other profiles with references to the Roaming Consortium profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show wlan hotspot anqp-roam-cons-profile
ANQP Roaming Consortium Profile List
------------------------------------
Name      References  Profile Status
----      ----------  --------------
default   1
Roam_OI2  1
Total:2.
```

This example displays the configuration settings for the profile **Roam_OI2.**

```
(host) #show wlan hotspot anqp-roam-cons-profile Roam_OI2
ANQP Roaming Consortium Profile "Roam_OI2"
------------------------------------------
Parameter                 Value
---------                 -----
Roaming consortium OI Len  3
Roaming consortium OI Len b32af0
```

The output of this command includes the following parameters:

Parameter	Description
`Roaming consortium OI Len`	Length of the OI. The roaming consortium OI length parameter is based upon the number of octets of the Roaming consortium OI. This parameter can have the following values: ■ **0**: 0 Octets in the OI (Null) ■ **3**: OI length is 24-bit (3 Octets) ■ **5**: OI length is 36-bit (5 Octets)
`Roaming Consortium OI`	The roaming consortium OI sent in a GAS query response.

Related Commands

wlan hotspot anqp-roam-cons-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot anqp-venue-name-profile

```
show wlan hotspot anqp-venue-name-profile [<profile-name>]
```

Description

The output of this command displays settings for a WLAN ANQP Venue Name profile.

Syntax

Parameter	Description
<profile>	Name of an ANQP Venue Name profile.

Usage Guidelines

ANQP profiles define the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP profile to be associated with the advertisement profile.

Issue this command without the <profile>parameter to display the entire ANQP Venue Name profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Venue Name profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-venue-name-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Examples

The example below shows that the controller has two configured Venue Name profiles. The **References** column lists the number of other profiles with references to the Venue Name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) # show wlan hotspot anqp-venue-name-profile
ANQP Venue Name Profile List
----------------------------
Name         References  Profile Status
----         ----------  --------------
default      0
venue_mall   0
Total:2.
```

This example displays the configuration settings for the profile venue_mall.

```
(host) #show wlan hotspot anqp-venue-name-profile venue_mall
ANQP Venue Name Profile "venue_mall"
------------------------------------
Parameter      Value
---------      -----
Venue Group    mercantile
Type of Venue  mercantile-shopping-mall
Venue Name     Westfield_Mall
```

The output of this command includes the following parameters:

Parameter	Description
Venue Group	The venue group to be advertised in the ANQP IEs from APs associated with this profile. This parameter can have any of the following values: ■ assembly ■ business ■ educational ■ factory-or-industrial ■ institutional ■ mercantile ■ outdoor ■ reserved ■ residential ■ storage ■ unspecified ■ Utility-Misc ■ Vehicular
Type of Venue	The venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 2610.
Venue Name	The venue name to be advertised in the ANQP IEs from APs associated with this profile.

Related Commands

wlan hotspot anqp-venue-name-profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot hs2-profile

```
show wlan hotspot hs2-profile [<profile-name>]
```

Description

The output of this command displays settings for a Hotspot 2.0 profile.

Syntax

Parameter	Description
`<profile-name>`	Name of a Hotspot 2.0 profile.

Usage Guidelines

Organization Identifiers (OIs) are assigned to service providers when they register with the IEEE registration authority The Roaming Consortium IEs contain information identifying the network and service provider, whose security credentials can then be used to authenticate with the AP transmitting this element.

The OI for the service provider is defined in the ANQP Roaming Consortium profile using the wlan hotspot anqp-roam-cons-profile command. This Hotspot profile allows you to define and send up to three additional OIs to a client. The configurable values for each additional OI include the Organization Identifier itself, the OI length, and the venue group and venue type associated with those OIs.

Issue this command without the **<profile-name>** parameter to display the entire ANQP advertisement profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured Hotspot profiles. The **References** column lists the number of other profiles with references to the Hotspot profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] # show wlan hotspot hs2-profile

Hotspot 2.0 Profile List
------------------------
Name           References  Profile Status
----           ----------  --------------
default        1
Hotspot_1      2
Total:2
```

The following example shows configuration settings defined for the profile **Hotspot1**:

```
(host) [mynode] #show wlan hotspot hs2-profile Hotspot1

Hotspot 2.0 Profile "default"
-----------------------------
Parameter                                                    Value
---------                                                    -----
Advertise Hotspot 2.0 Capability                             Enabled
Additional Steps required for Access Enabled                 Enabled
Network Internet Access                                      Enabled
Length of Query Response                                     255 octets
```

```
Access network Type                                                    public-chargeable
Roaming Consortium Len Entry 1                                         3 octets
Roaming Consortium OI Entry 1                                          C499AA
Roaming Consortium Len Entry 2                                         0
Roaming Consortium OI Entry 2                                          N/A
Roaming Consortium Len Entry 3                                         0
Roaming Consortium OI Entry 3                                          N/A
Additional Roaming Consortium OI's(displayed in Advertisement Profile) 1
Venue Group Type                                                       mercantile
Venue Type                                                             mercantile-shopping-
mall
Type of Hotspot 2.0 Indication Element                                 31
Advertisement Profile                                                  Westgate_Mall
```

The output of this command includes the following data columns:

Parameter	Description
`Advertise Hotspot 2.0 Capability`	Shows if this profile has been enabled.
`Additional Steps required for Access Enabled`	If this parameter is enabled, the AP will send the following IEs (IEs) in response to the client's the ANQP query. ■ Venue Name ■ Domain Name List ■ Network Authentication Type ■ Roaming Consortium List ■ NAI Realm List **NOTE:** If **asra** is enabled, the advertisement profile for this hotspot must reference an enabled network authentication type profile. For more information on enabling an network authentication type profile, see wlan hotspot anqp-nwk-auth-profile on page 2605.
`Network Internet Access`	If enabled, the AP sends an Information Element (IE) indicating that the network allows internet access. By default, a hotspot profile does not advertise network internet access.
`Length of Query Response`	The maximum length of the GAS query response, in octets. The supported range is 1-255 octets.
`Access network Type`	The 802.11u network type. The default setting is *public-chargeable*. ■ emergency-services: emergency services only network ■ personal-device: personal device network ■ private: private network ■ private-guest: private network with guest access ■ public-chargeable: public chargeable network ■ public-free: free public network ■ test: test network ■ wildcard: wildcard network

Parameter	Description
`Roaming Consortium Len Entry 1`	Length of the OI. This value is based upon the number of octets in the **Roaming Consortium OI Entry 1** field. ■ **0**: Zero Octets in the OI (Null) ■ **3**: OI length is 24-bit (3 Octets) ■ **5**: OI length is 36-bit (5 Octets)
`Roaming Consortium OI Entry 1`	Roaming consortium OI assigned to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the **Additional Roaming Consortium OI's (displayed in Advertisement Profile)** parameter is set to 1 or higher.
`Roaming Consortium Len Entry 2`	Length of the OI. This value is based upon the number of octets in the **Roaming Consortium OI Entry 2** field. ■ **0**: Zero Octets in the OI (Null) ■ **3**: OI length is 24-bit (3 Octets) ■ **5**: OI length is 36-bit (5 Octets)
`Roaming Consortium OI Entry 2`	Roaming consortium OI assigned to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the **Additional Roaming Consortium OI's (displayed in Advertisement Profile)** parameter is set to 2 or higher.
`Roaming Consortium Len Entry 3`	Length of the OI. This value is based upon the number of octets in the **Roaming Consortium OI Entry 3** field. ■ **0**: Zero Octets in the OI (Null) ■ **3**: OI length is 24-bit (3 Octets) ■ **5**: OI length is 36-bit (5 Octets)
`Roaming Consortium OI Entry 3`	Roaming consortium OI assigned to one of the service provider's top three roaming partners. This additional OI will only be sent to a client if the **Additional Roaming Consortium OI's (displayed in Advertisement Profile)** parameter is set to 3 or higher.
`Additional Roaming Consortium OI's (displayed in Advertisement Profile)`	Number of additional roaming consortium Organization Identifiers (OIs) advertised by the AP.
`Venue Group Type`	The venue groups to be advertised in the IEs from APs associated with this hotspot profile. The default setting is **unspecified**.
`Venue Type`	Venue type to be advertised in the IEs from APs associated with this hotspot profile.

Parameter	Description
`Type of Hotspot 2.0 Indication Element`	Advertisement protocol types to be used by the AP. ■ **anqp**: Access Network Query Protocol ■ **emergency**: Emergency Alert System ■ **mih-cmd-event**: Media Independent Handover (MIH) Command and Event Services Capability Discovery ■ **mih-info**: Media Independent Handover (MIH) Information Service. This option allows handovers between differing kinds of wireless access protocols and technologies, allowing access points on different IP subnets to communicate with each other at the link level while maintaining session continuity.
`Advertisement Profile`	Advertisement profile associated with this hotspot profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot h2qp-conn-capability-profile

```
show wlan hotspot h2qp-conn-capability-profile [<profile>]
```

Description

The output of this command displays settings for a WLAN H2QP connection capability profile.

Syntax

Parameter	Description
`<profile>`	Name of H2QP connection capability profile

Usage Guidelines

The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about the IP protocols and associated port numbers that are available and open for communication.

Values configured in this profile will not be sent to clients unless you:

1. Associate the H2QP profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> h2qp-conn-cap-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Examples

Issue this command without the optional <profile> parameter to display a list of all configured connection capability profiles. Include the <profile> parameter to display details for a specific profile.

The example below shows that the controller has four configured connection capability profiles. The **References** column lists the number of other profiles with references to the connection capability profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
H2QP Connection Capability Profile List
---------------------------------------
Name              References  Profile Status
----              ----------  --------------
branch-hotspot-1  6
branch-hotspot-2  5
default           1
downtown-hotspot  1
Total:4
```

The following example displays the current configuration settings for the default H2QP connection capability profile.

```
(host) (config) #show wlan hotspot h2qp-conn-capability-profile  default
H2QP Connection Capability Profile "default"
--------------------------------------------
Parameter                                                  Value
---------                                                  -----
H2QP Connection Capability ICMP port                       Disabled
H2QP Connection Capability FTP port(TCP Protocol)          Disabled
```

```
H2QP Connection Capability SSH port(TCP Protocol)                    Disabled
H2QP Connection Capability HTTP port(TCP Protocol)                   Disabled
H2QP Connection Capability TLS VPN port(TCP Protocol)                Disabled
H2QP Connection Capability PPTP VPN port(TCP Protocol)               Disabled
H2QP Connection Capability VOIP port(TCP Protocol)                   Disabled
H2QP Connection Capability VOIP port(UDP Protocol)                   Disabled
H2QP Connection Capability IKEv2 port for IPSec VPN                  Disabled
H2QP Connection Capability May be used by IKEv2 port for IPSec VPN   Disabled
H2QP Connection Capability ESP port(Used by IPSec VPN)               Disabled
```

The output of this command includes the following information:

Parameter	Description
`H2QP Connection Capability ICMP port`	Shows if the ICMP port is enabled and available. (port 0)
`H2QP Connection Capability FTP port`	Shows if the FTP port is enabled and available. (port 20)
`H2QP Connection Capability SSH port`	Shows if the SSH port is enabled and available. (port 22)
`H2QP Connection Capability HTTP port`	Shows if the HTTP port is enabled and available. (port 80)
`H2QP Connection Capability TLS VPN port`	Shows if the TCP TLS port used VPNs is enabled and available. (port 80)
`H2QP Connection Capability PPTP VPN port`	Shows if the PPTP port used by IPsec VPNs is enabled and available. (port 1723)
`H2QP Connection Capability VoIP port (UDP)`	Shows if the UDP VoIP port is enabled and available. (port 5060)
`H2QP Connection Capability VoIP port (TCP)`	Shows if the TCP VoIP port is enabled and available. (port 5060)
`H2QP Connection Capability IKEv2 port for IPSec VPN`	Shows if the IKEv2 port 4500 is enabled and available
`H2QP Connection Capability May be used by IKEv2 port for IPSec VPN`	Shows if the IKEv2 port 500 is enabled and available
`H2QP Connection Capability ESP port (Used by IPSec VPN)`	Shows if the ESP port used by IPsec VPNs is enabled and available. (port 0)

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot h2qp-op-cl-profile

```
show wlan hotspot h2qp-op-cl-profile [<profile>]
```

Description

The output of this command displays settings for a WLAN H2QP operating class profile.

Syntax

Parameter	Description
`<profile>`	Name of H2QP operating class profile

Usage Guidelines

The values configured in this H2QP Operating Class profile list the channels on which the hotspot is capable of operating. It may be useful where, for instance, a mobile device discovers a hotspot in the 2.4 GHz band but finds it is dual-band and prefers the 5 GHz band.

Examples

Issue this command without the optional <profile> parameter to display a list of all configured connection capability profiles. Include the <profile> parameter to display details for a specific profile.

The example below shows that the controller has two configured operating class profiles. The **References** column lists the number of other profiles with references to the operating class profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)(H2QP Connection Capability Profile "default") #show wlan hotspot h2qp-op-cl-profile
H2QP Operating Class Indication Profile List
--------------------------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
newopcl  1
Total:2
```

The following example displays the current configuration setting for the default H2QP operating class profile.

```
(host)(H2QP Connection Capability Profile "default") #show wlan hotspot h2qp-op-cl-profile
default
H2QP Operating Class Indication Profile "default"
-------------------------------------------------
Parameter                                 Value
---------                                 -----
H2QP Operating Class(Valid Values 1-255)  1
```

The output of this command includes the following information:

Parameter	Description
`H2QP Operating Class (Valid Values 1-255)`	Displays the current operating class for the devices' BSS. The supported range for this field is 1-255, and the default value is 1.

Related Commands

Command	Description
wlan hotspot h2qp-op-cl-profile	Use this command to configure WLAN H2QP operating class profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot h2qp-operator-friendly-name-profile

```
show wlan hotspot h2qp-operator-friendly-name-profile [<profile>]
```

Description

The output of this command displays settings for a H2QP operator-friendly name profile.

Syntax

Parameter	Description
<profile>	Name of H2QP operator-friendly name profile.

Usage Guidelines

The operator-friendly name defined in this profile is a free-form text field that can identify the operator and also something about the location.Issue this command without the **<profile>** parameter to display the entire operator-friendly name profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the controller has two configured operator-friendly name profiles. The **References** column lists the number of other profiles with references to the operator-friendly name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host)(config)# show wlan hotspot h2qp-operator-friendly-name-profile
H2QP Operator Friendly Name Profile List
----------------------------------------
Name       References  Profile Status
----       ----------  --------------
default    0
operator1  8
Total:2
```

The following example displays the configuration settings for the profile **operator1.**

```
(host) (H2QP Operator Friendly Name Profile "operator1") #show wlan hotspot h2qp-operator-
friendly-name-profile operator1
H2QP Operator Friendly Name Profile "operator1"
-----------------------------------------------
Parameter                              Value
---------                              -----
Operator Friendly Name Language Code   eng
Operator Friendly Name                 CoffeeHouseGuest
```

The output of this command includes the following parameters:

Parameter	Description
Operator Friendly Name Language Code	An ISO 639 language code that identifies the language used in the Operator Friendly Name field.

Parameter	Description
Operator Friendly Name	An operator-friendly name sent by devices using this profile. The name can be up to 64 alphanumeric characters, and can include special characters and spaces. If the name includes quotation marks (“), you must include a backslash character (\) before each quotation mark. (e.g. \"example\")

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot h2qp-osu-prov-list-profile

```
show wlan hotspot h2qp-osu-prov-list-profile <profile-name>
```

Description

This command displays settings for a H2QP OSU providers list profile.

Syntax

Parameter	Description
`<profile-name>`	Name of the H2QP OSU providers list profile.

Usage Guidelines

The name defined in this profile is a free-form text field that can identify the OSU providers list. Issue this command without the **<profile-name>** parameter to display the entire OSU providers profile list. Include a profile name to display detailed configuration information for that profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

show wlan hotspot h2qp-wan-metrics-profile

```
show wlan hotspot h2qp-wan-metrics-profile [<profile-name>]
```

Description

The output of this command displays settings for a H2QP WAN metrics profile.

Syntax

Parameter	Description
<profile-name>	Name of H2QP WAN metrics profile.

Usage Guidelines

The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about access network characteristics such as link status and the capacity and speed of the WAN link to the Internet. Issue this command without the **<profile-name>** parameter to display the entire WAN metrics profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has two configured WAN metrics profiles. The **References** column lists the number of other profiles with references to the WAN metrics profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [mynode] (H2QP Connection Capability Profile "default") #show wlan hotspot h2qp-wan-
metrics-profile

H2QP WAN Metrics Profile List
-----------------------------
Name     References  Profile Status
----     ----------  --------------
default  0
fastwan  6
Total:2
```

The following example shows the current configuration settings for the profile 'fastwan':

```
(host) [mynode] #show wlan hotspot h2qp-wan-metrics-profile fastwan

H2QP WAN Metrics Profile "fastwan"
----------------------------------
Parameter                              Value
---------                              -----
H2QP WAN metrics link status           link_up
H2QP WAN metrics symmetric WAN link    Disabled
H2QP WAN metrics link at capacity      Disabled
WAN Metrics uplink speed               1000
WAN Metrics downlink speed             1000
WAN Metrics uplink load                100
WAN Metrics downlink load              100
WAN Metrics load measurement duration  100
```

The output of this command includes the following information:

Parameter	Description
`H2QP WAN metrics link status`	Indicates the status of the WAN Link by displaying one of the following values. The default link status is **reserved**, which indicates that the link status is unknown or unspecified. ■ link_down ■ link_test ■ link_up ■ reserved
`H2QP WAN metrics symmetric WAN link`	This parameter indicates if the WAN Link has same speed in both the uplink and downlink directions.
`H2QP WAN metrics link at capacity`	This parameter indicates if the WAN Link has reached its maximum capacity. If this parameter is enabled, no additional mobile devices will be permitted to associate to the hotspot AP.
`WAN Metrics uplink speed`	This parameter indicates the current WAN backhaul uplink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the uplink speed is unknown or unspecified.
`WAN Metrics down link speed`	This parameter indicates the current WAN backhaul downlink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.
`WAN Metrics uplink load`	The percentage of the WAN uplink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.
`WAN Metrics downlink load`	The percentage of the WAN downlink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.
`WAN Metrics load measurement duration`	Duration over which the downlink load is measured, in tenths of a second.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

show wlan ht-ssid-profile

```
show wlan ht-ssid-profile [<profile-name>]
```

Description

This command displays the list of all high-throughput SSID profiles, or detailed configuration information for a specific high-throughput SSID profile.

Syntax

Parameter	Description
`<profile-name>`	Name of a high-throughput SSID profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire high-throughput SSID profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has two configured high-throughput SSID profiles. The **References** column lists the number of other profiles with references to the high-throughput SSID profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

```
(host) [mynode] #show wlan ht-ssid-profile

High-throughput SSID profile List
---------------------------------
Name                          References  Profile Status
----                          ----------  --------------
default                       2
dot1X_CP-htssid_prof          1
ade-sloan-htssid_prof         1

Total:3
```

The following example shows configuration settings defined for the profile **default**:

```
(host) #show wlan ht-ssid-profile default

High-throughput SSID profile "default"
--------------------------------------
Parameter                                                    Value
---------                                                    -----
High throughput enable (SSID)                                Enabled
40 MHz channel usage                                         Enabled
Very High throughput enable (SSID)                           Enabled
80 MHz channel usage (VHT)                                   Enabled
BA AMSDU Enable                                              Enabled
Temporal Diversity Enable                                    Disabled
Legacy stations                                              Allowed
Low-density Parity Check                                     Enabled
Maximum number of spatial streams usable for STBC reception  1
Maximum number of spatial streams usable for STBC transmission  1
```

```
MPDU Aggregation                                          Enabled
Max received A-MPDU size                                  65535 bytes
Max transmitted A-MPDU size                               65535 bytes
Min MPDU start spacing                                    0 usec
Short guard interval in 20 MHz mode                       Enabled
Short guard interval in 40 MHz mode                       Enabled
Short guard interval in 80 MHz mode                       Enabled
Supported MCS set                                         0-31
VHT - Supported MCS map                                   9,9,9,9
VHT - Explicit Transmit Beamforming                       Enabled
VHT - Transmit Beamforming Sounding Interval              25 msec
VHT - Multi User Transmit Beamforming                     Enabled
Maximum VHT MPDU size                                     11454 bytes
Maximum number of MSDUs in an A-MSDU on best-effort AC    2 MSDUs
Maximum number of MSDUs in an A-MSDU on background AC     2 MSDUs
Maximum number of MSDUs in an A-MSDU on video AC          2 MSDUs
Maximum number of MSDUs in an A-MSDU on voice AC          0 MSDUs
```

The output of this command includes the following data columns:

Parameter	Description
`High throughput enable (SSID)`	Displays if the high-throughput (802.11n) feature is enabled or disabled on the SSID. Default: Enabled.
`40 MHz channel usage`	Shows if the profile enables or disables the use of 40 MHz channels. Default: Enabled.
`Very High throughput enable (SSID)`	Displays if the very high-throughput (802.11ac) feature is enabled or disabled on the SSID. Default: Enabled.
`80 MHz channel usage (VHT)`	Displays the status of the 80 MHz channel for very high-throughput is enabled or disabled. Default: Enabled.
`BA AMSDU Enable`	Displays if the AP has enabled or disabled the ability to receive Aggregated-MAC Service Data Unit (A-MSDU) in Block ACK (BA) negotiation. Default: Enabled.
`Temporal Diversity Enable`	Displays if temporal diversity has been enabled or disabled. When this feature is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries. Default: Disabled.
`Legacy stations`	Allows or disallows associations from legacy (non-HT) stations. By default, this parameter is enabled (legacy stations are allowed).
`Low-density Parity Check`	If enabled, the AP will advertise Low-density Parity Check (LDPC) support. LDPC improves data transmission over radio channels with high levels of background noise. Default: Enabled.

Parameter	Description
Maximum number of spatial streams usable for STBC reception	Displays the maximum number of spatial streams usable for Space-Time Block Code (STBC) reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.) **NOTE:** If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
Maximum number of spatial streams usable for STBC transmission	Displays the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.) **NOTE:** If transmit beamforming is enabled, STBC will be disabled for beamformed frames.
MPDU Aggregation	Displays if the profile enables or disables MAC Protocol Data Unit (MPDU) aggregation. Default: Enabled.
Max received A-MPDU size	Displays the configured maximum size of a received aggregate MPDU, in bytes.
Max transmitted A-MPDU size	Displays the configured maximum size of a transmitted aggregate MPDU, in bytes.
Min MPDU start spacing	Displays the configured minimum time between the start of adjacent MPDUs within an aggregate MPDU, in microseconds.
Short guard interval in 20 MHz mode	Displays if the profile enables or disables use of short (400 ns) guard interval in 20 MHz mode. Default: Enabled.
Short guard interval in 40 MHz mode	Displays if the profile enables or disables use of short (400 ns) guard interval in 40 MHz mode. Default: Enabled.
Short guard interval in 80 MHz mode	Displays if the profile enables or disables use of short (400 ns) guard interval in 80 MHz mode. Default: Enabled.
Supported MCS set	Displays a list of Modulation Coding Scheme (MCS) values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20 MHz vs. 40 MHz vs. 80 MHz) and the number of spatial streams used by the mesh node. Default: 0-31 ■ MCS value of 16-23 are supported on 130 Series, RAP-155, and 11ac APs only. ■ MCS value of 24-31 are supported on 320 Series APs only.

Parameter	Description
VHT - Supported MCS map	Displays a list of supported MCS map for very high throughput SSID. Comma separated list of maximum supported MCS for spatial streams 1 through 4. Valid values for maximum MCS are 7, 8, 9, and '-' (if spatial stream is not supported). Maximum MCS of a spatial stream cannot be higher than the previous streams. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx. Default: 9,9,9,9.
VHT - Explicit Transmit Beamforming	Displays if VHT Explicit Transmit Beamforming status is enabled or disabled for the 802.11ac-capable APs. When this feature is enabled, the AP requests information about the MIMO channel and uses that information to transmit data over multiple transmit streams using a calculated steering matrix. The result is higher throughput due to improved signal at the beamformee (the receiving client). If this parameter is disabled, all other transmit beamforming settings will not take effect. Default: Enabled.
VHT - Transmit Beamforming Sounding Interval	Displays the time interval in milliseconds between updates of VHT Transmit Beamforming channel estimation. (802.11ac-capable APs only) **NOTE:** This is applicable for 802.11ac-capable APs only. Default: 25 milliseconds.
VHT - Multi User Transmit Beamforming	Displays if the VHT Multi-User Transmit Beamforming is enabled or disabled. If this parameter is disabled, all other Multi-User Transmit Beamforming configuration parameters have no effect. **NOTE:** This parameter is applicable for 320 Series APs only. Default: Enabled.
Maximum VHT MPDU size	Displays the maximum size of a VHT MPDU. Default: 11454 bytes.
Maximum number of MSDUs in an A-MSDU on best-effort AC	Displays the maximum number of MSDUs in a TX A-MSDU on best-effort Access Category (AC). Default: 2. **NOTE:** In tunnel and decrypt-tunnel forwarding mode, TX A-MSDU is disabled if the value is set to 0. If the value is set to non-zero, TX A-MSDU is enabled and set to this value.
Maximum number of MSDUs in an A-MSDU on background AC	Displays the maximum number of MSDUs in a TX A-MSDU on background AC. Default: 2. **NOTE:** TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on background AC is disabled and assigning any value has no effect.
Maximum number of MSDUs in an A-MSDU on video AC	Displays the maximum number of MSDUs in a TX A-MSDU on video AC. Default: 2. **NOTE:** TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on video AC is disabled and assigning any value has no effect.

Parameter	Description
`Maximum number of MSDUs in an A-MSDU on voice AC`	Displays the maximum number of MSDUs in a TX A-MSDU on voice AC. Default: 0. **NOTE:** TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on voice AC is disabled and assigning any value has no effect.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wlan rrm-ie-profile

```
show wlan rrm-ie-profile [<profile-name>]
```

Description

This command displays the list of all radio resource management information element (RRM IE) profiles, or the detailed configuration information for a specific RRM IE profile.

Syntax

Parameter	Description
`<profile-name>`	Name of an RRM IE profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire RRM IE profile list. Include a profile name to display detailed configuration information for that profile.

Examples

The following example displays the configuration information for the "default" RRM IE profile:

```
(host) [mynode] #show wlan rrm-ie-profile default

RRM IE Profile "default"
------------------------
Parameter                          Value    Set
---------                          -----    ---
Advertise Enabled Capabilities IE  Enabled
Advertise Country IE               Enabled
Advertise Power Constraint IE      Enabled
Advertise TPC Report IE            Enabled
Advertise QBSS Load IE             Enabled
Advertise BSS AAC IE               Enabled
Advertise Quiet IE                 Enabled
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wlan ssid-profile

```
show wlan ssid-profile [<profile-name>]
```

Description

This command displays the list of all SSID profiles, or detailed configuration information for a specific SSID profile.

Syntax

Parameter	Description
<profile-name>	Name of an SSID profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire **SSID** profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has six configured SSID profiles. The **References** column lists the number of other profiles with references to the SSIDs profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

```
(host) [mynode] #show wlan ssid-profile

SSID Profile List
-----------------
Name                              References  Profile Status
----                              ----------  --------------
coltrane-ssid-profile             1
corp1   -ssid-profile                                  3
Remote                            1
Secure-Profile2                   0
test-ssid-profile                 1
wizardtest-ssid-profile           1

Total:6
```

The following example shows configuration settings defined for the SSID Profile **Remote**:

```
(host) [mynode] #show wlan ssid-profile remote

SSID Profile "Remote"
---------------------
Parameter                                       Value
---------                                       -----
SSID enable                                     Enabled
ESSID                                           aruba-ap
Encryption                                      opensystem
Enable Management Frame Protection              Disabled
Require Management Frame Protection             Disabled
DTIM Interval                                   1 beacon periods
802.11a Basic Rates                             6 12 24
802.11a Transmit Rates                          6 9 12 18 24 36 48 54
802.11g Basic Rates                             1 2
```

```
802.11g Transmit Rates                              1 2 5 6 9 11 12 18 24 36 48 54
Station Ageout Time                                 1000 sec
Max Transmit Attempts                               8
RTS Threshold                                       2333 bytes
Short Preamble                                      Enabled
Max Associations                                    64
Wireless Multimedia (WMM)                           Disabled
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave    Enabled
WMM TSPEC Min Inactivity Interval                   0 msec
DSCP mapping for WMM voice AC                       N/A
DSCP mapping for WMM video AC                       N/A
DSCP mapping for WMM best-effort AC                 N/A
DSCP mapping for WMM background AC                  N/A
Multiple Tx Replay Counters                         Disabled
Hide SSID                                           Disabled
Deny_Broadcast Probes                               Disabled
Local Probe Request Threshold (dB)                  0
Auth Request Threshold (dB)                         0
Disable Probe Retry                                 Enabled
Battery Boost                                       Disabled
WEP Key 1                                           N/A
WEP Key 2                                           N/A
WEP Key 3                                           N/A
WEP Key 4                                           N/A
WEP Transmit Key Index                              1
WPA Hexkey                                          N/A
WPA Passphrase                                      N/A
Maximum Transmit Failures                           0
EDCA Parameters Station profile                     N/A
EDCA Parameters AP profile                          N/A
BC/MC Rate Optimization                             Disabled
Rate Optimization for delivering EAPOL frames       Enabled
Strict Spectralink Voice Protocol (SVP)             Disabled
High-throughput SSID Profile                        default
802.11g Beacon Rate                                 default
802.11a Beacon Rate                                 default
Video Multicast Rate Optimization                   default
Advertise QBSS Load IE                              Disabled
Advertise Location Info                             Enabled
Advertise AP Name                                   Disabled
802.11r Profile                                     N/A
Enforce user vlan for open stations                 Enabled
Enable OKC                                          Enabled
```

The output of this command includes the following data columns:

Parameter	Description
SSID	Shows if the profile has enabled or disabled this SSID.
ESSID	Name that uniquely identifies a wireless network. If the ESSID includes spaces, you must enclose it in quotation marks.
Encryption	The layer-2 authentication and encryption type used on this ESSID.
Enable Management Frame Protection	Enables management frame protection.

Parameter	Description
Require Management Frame Protection	If enabled, requires management frame protection.
DTIM Interval	The interval, in milliseconds, between the sending of Delivery Traffic Indication Messages (DTIMs) in the beacon.
802.11a Basic Rates	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses.
802.11a Transmit Rates	Set of 802.11a rates at which the AP is allowed to send data.
802.11g Basic Rates	List of supported 802.11b/g rates, in Mbps, that are advertised in beacon frames and probe responses.
802.11g Transmit Rates	Set of 802.11b/g rates at which the AP is allowed to send data.
Station Ageout Time	Time, in seconds, that a client is allowed to remain idle before being aged out.
Max Transmit Attempts	Maximum transmission failures allowed before the client gives up.
RTS Threshold	Wireless clients transmitting frames larger than this defined threshold must issue Request to Send (RTS) and wait for the AP to respond with Clear to Send (CTS).
Short Preamble	Shows if the profile enables or disables short preamble for 802.11b/g radios
Max Associations	Maximum number of wireless clients for the AP
Wireless Multimedia (WMM)	Shows if the profile enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function (EDCF)
Wireless Multimedia U-APSD (WMM-UAPSD) Powersave	Shows if the profile enables or disables Wireless Multimedia (WMM) UAPSD powersave.
WMM TSPEC Min Inactivity Interval	Specifies the minimum inactivity time-out threshold of WMM traffic.
DSCP mapping for WMM voice AC	DSCP value used to map WMM voice traffic.
DSCP mapping for WMM video AC	DSCP value used to map WMM video traffic.
DSCP mapping for WMM best-effort AC	DSCP value used to map WMM best-effort traffic.
DSCP mapping for WMM background AC	DSCP value used to map WMM background traffic.

Parameter	Description
902il Compatibility Mode	(For clients using NTT DoCoMo 902iL phones only) When enabled, the managed device does not drop packets from the client if a small or old initialization vector value is received.
Hide SSID	Shows if the profile enables or disables hiding of the SSID name in beacon frames.
Deny_Broadcast Probes	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.
Local Probe Response	Shows if the profile enables or disables local probe response on the AP. If this option is enabled, the AP is responsible for sending 802.11 probe responses to wireless clients' probe requests. If this option is disabled, then the managed device sends the 802.11 probe responses.
Auth Request Threshold (dB)	Displays the SNR threshold below which incoming authentication requests are ignored.
Disable Probe Retry	Shows if the profile enables or disables battery MAC level retries for probe response frames.
Battery Boost	If enabled, this feature converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval.
WEP Key 1	Displays the Static WEP key associated with this key index.
WEP Key 2	Displays the Static WEP key associated with this key index.
WEP Key 3	Displays the Static WEP key associated with this key index.
WEP Key 4	Displays the Static WEP key associated with this key index.
WEP Transmit Key Index	Shows the key index that specifies which static WEP key is to be used.
WPA Hexkey	WPA pre-shared key (PSK).
WPA Passphrase	WPA passphrase used to generate a pre-shared key (PSK).
Maximum Transmit Failures	Maximum transmission failures allowed before the client gives up.

Parameter	Description
EDCA Parameters Station profile	Name of the enhanced distributed channel access (EDCA) Station profile that applies to this SSID.
EDCA Parameters AP profile	Name of the enhanced distributed channel access (EDCA) AP profile that applies to this SSID.
BC/MC Rate Optimization	Shows if the profile enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate.
Rate Optimization for delivering EAPOL frames	If this option is enabled, APs using this profile will use a more conservative rate for more reliable delivery of EAPOL frames.
Strict Spectralink Voice Protocol (SVP)	Shows if the profile enables or disables strict Spectralink Voice Protocol (SVP).
High-throughput SSID Profile	Name of the high-throughput SSID profile associated with this SSID profile.
802.11g Beacon Rate	The beacon rate for 802.11g (use for Distributed Antenna System (DAS) only). Using this parameter in normal operation may cause connectivity problems.
802.11a Beacon Rate	The beacon rate for 802.11a (use for Distributed Antenna System (DAS) only). Using this parameter in normal operation may cause connectivity problems.
Video Multicast Rate Optimization	The rate for video multicast frames.
Advertise QBSS Load IE	Enables the AP to advertise the QBSS load element. The element includes the following parameters that provide information on the traffic situation: ■ **Station count**: The total number of stations associated to the QBSS. ■ **Channel utilization**: The percentage of time (normalized to 255) the channel is sensed to be busy. The access point uses either the physical or the virtual carrier sense mechanism to sense a busy channel. ■ **Available admission capacity**: The remaining amount of medium time (measured as number of 32us/s) available for a station via explicit admission control. The QAP uses these parameters to decide whether to accept an admission control request. A wireless station uses these parameters to choose the appropriate access points.

Parameter	Description
`Advertise Location Info`	APs that are part of this VAP will broadcast their GPS coordinates in the beacons and probe response frames as part of a vendor-specific Information Element.
`Advertise AP Name`	If this parameter enabled, APs will broadcast the AP name configured by the **ap-name** command. This option is disabled by default.
`802.11r Profile`	The associated **dot11r-profile** with the SSID profile.
`Enforce user vlan for open stations`	Shows the strict enforcement of data traffic only in user's assigned vlan (Open stations only).
`Enable OKC`	The status of the Opportunistic Key Caching. Opportunistic Key Caching (OKC) is a similar technique, not defined by 802.11i, available for authentication between multiple APs in a network where those APs are under common administrative control. An Aruba deployment with multiple APs under the control of a single controller is one such example. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wlan traffic-management-profile

```
show wlan traffic-management-profile [<profile-name>]
```

Description

This command displays the list of all traffic management profiles, or detailed configuration information for a specific traffic management profile.

Syntax

Parameter	Description
`<profile-name>`	Name of a traffic management profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire traffic management profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has three configured traffic management profiles. The **References** column lists the number of other profiles with references to the traffic management profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

```
(host) [mynode] #show wlan traffic-management-profile

Traffic management profile List
-------------------------------
Name     References  Profile Status
----     ----------  --------------
mgmt1    3
mgmt2    2
Total:2
```

The following example shows configuration settings defined for the profile **mgmt1**:

```
(host) [mynode] #show wlan traffic-management-profile mgmt1

Traffic management profile "default"
------------------------------------
Parameter                   Value
---------                   -----
Proportional BW Allocation  N/A
Report interval             5 min
Station Shaping Policy      default-access
```

The output of this command includes the following data columns:

Parameter	Description
`Proportional BW Allocation`	Minimum bandwidth, as a percentage of available bandwidth, allocated to an SSID when there is congestion on the wireless network. An SSID can use all available bandwidth if no other SSIDs are active.
`Report interval`	Number of minutes between bandwidth usage reports.
`Station Shaping Policy`	Shows which of three possible Station Shaping policies is configured on the profile. ■ **default-access**: Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting. ■ **fair-access**: Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities. The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network.You must set traffic shaping to f**air-access** to use this bandwidth allocation value for an individual virtual AP. ■ **preferred-access**: High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show wlan tsm-req-profile

```
show wlan tsm-req-profile [<profile-name>]
```

Description

This command displays configuration and other information about the parameters for the Transmit Stream and Category Measurement (TSM) Request frames.

Syntax

Parameter	Description
`<profile-name>`	Name of this profile. Name must be 1-63 characters.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire TSM Request profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

For this profile to take effect, the 802.11K feature needs to be enabled.

Examples

```
(host) [mynode] #show wlan tsm-req-profile default

TSM Report Request Profile "default"
------------------------------------
Parameter                           Value
---------                           -----
Request Mode for TSM Report Request  normal
Number of repetitions                65535
Duration Mandatory                   Enabled
Randomization Interval               0
Measurement Duration                 25
Traffic ID                           96
Bin 0 Range                          200
```

The output of this command includes the following information:

Parameter	Description
`Request mode for TSM Report Request`	Shows the request mode for the Transmit Stream and Category Measurement Request frame.
`Number of repetitions`	Shows the "Number of Repetitions" field in the Transmit Stream and Category Measurement Request frame.
`Duration Mandatory`	Shows the "Duration Mandatory" part of the **Measurement Request Mode** field of the Transmit Stream and Category Measurement Request frame.
`Randomization Interval`	Shows the **Randomization Interval** field in the Transmit Stream and Category Measurement Request frame.

Parameter	Description
`Measurement Duration`	Shows the **Measurement Duration** field in the Transmit Stream and Category Measurement Request frame.
`Traffic ID`	Shows the **Traffic Identifier** field in the Transmit Stream and Category Measurement Request frame.
`Bin 0 Range`	Shows the **'Bin 0 Range'** field in the Transmit Stream and Category Measurement Request frame.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wlan virtual-ap

```
show wlan virtual-ap [<profile-name>]
```

Description

Displays the list of all Virtual AP profiles, or detailed configuration information for a specific Virtual AP profile.

Syntax

Parameter	Description
`<profile-name>`	Name of a Virtual AP profile

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire Virtual AP profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has six configured Virtual AP profiles. The **References** column lists the number of other profiles with references to the Virtual AP profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

```
(host) [mynode] #show wlan virtual-ap

Virtual AP profile List
-----------------------
Name                              References  Profile Status
----                              ----------  --------------
coltrane-vap-profile              1
default
MegTest
Remote                            1
test-vap-profile                  1
wizardtest-vap-profile            1
Total: 6
```

The following example shows configuration settings defined for the profile **wizardtest-vap-profile**:

```
(host) [mynode] #show wlan virtual-ap test-vap-profile

Virtual AP profile "wizardtest-vap-profile"
---------------------------
Parameter                                   Value
---------                                   -----
AAA Profile                                 default
802.11K Profile                             default
SSID Profile                                default
Virtual AP enable                           Enabled
VLAN                                        N/A
Forward mode                                tunnel
Allowed band                                all
Band Steering                               Disabled
Steering Mode                               prefer-5ghz
Dynamic Multicast Optimization (DMO)        Enabled
```

```
Dynamic Multicast Optimization (DMO)            Threshold  6
Drop Broadcast and Multicast                     Disabled
Convert Broadcast ARP requests to unicast        Enabled
Authentication Failure Blacklist Time            3600 sec
Blacklist Time                                   3600 sec
Deny inter user traffic                          Disabled
Deny time range                                  N/A
DoS Prevention                                   Disabled
HA Discovery on-association                      Disabled
Mobile IP                                        Enabled
Preserve Client VLAN                             Disabled
Remote-AP Operation                              standard
Station Blacklisting                             Enabled
Strict Compliance                                Disabled
VLAN Mobility                                    Disabled
FDB Update on Assoc                              Disabled
WMM Traffic Management Profile                   N/A
Anyspot Profile                                  N/A
```

The output of this command includes the following data columns:

Parameter	Description
AAA Profile	Name of the AAA profile associated with this virtual AP.
802.11K Profile	Name of an 802.11k profile associated with this virtual AP.
SSID Profile	Name of an SSID profile associated with this virtual AP.
Virtual AP enable	Shows if the profile enables or disables the virtual AP.
VLAN	The VLAN(s) into which users are placed in order to obtain an IP address.
Forward mode	Forwarding mode defined on the profile: ■ tunnel mode ■ bridge mode ■ split-tunnel mode ■ decrypt-tunnel mode The forwarding mode controls whether data is tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). When an AP is configured to use the decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the managed device, which then applies firewall policies to the user traffic. When the managed device sends traffic to a client, the managed device sends 802.3 traffic through the GRE tunnel to the AP, which then converts it to encrypted 802.11 and forwards to the client.

Parameter	Description
Allowed band	The band(s) on which to use the virtual AP: ■ **a**—802.11a band only (5 GHz) ■ **g**—802.11b/g band only (2.4 GHz) ■ **all**—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)
Band Steering	If enabled, ARM's band steering feature encourages dual-band capable clients to stay on the 5GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones.
Steering Mode	Band steering supports three different band steering modes: ■ **Force-5GHz**: When the AP is configured in **force-5GHz** band steering mode, the AP will try to force 5 Ghz-capable APs to use that radio band. ■ **Prefer-5GHz** (Default): If you configure the AP to use **prefer-5GHz** band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. ■ **Balance-bands**: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5Ghz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz while the 2.5 GHz band operates in 20 MHz. **NOTE:** Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in ArubaOS versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default **prefer-5GHz** steering mode available in ArubaOS 6.0 and later.
Dynamic Multicast Optimization (DMO)	If enabled DMO techniques will be used to reliably transmit video data.
Dynamic Multicast Optimization (DMO) Threshold	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.
Drop Broadcast and Multicast	If enabled, the virtual AP will filter out broadcast and multicast traffic in the air.
Convert Broadcast ARP requests to unicast	If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client.
Authentication Failure Blacklist Time	Time, in seconds, a client is blocked if it fails repeated authentication. An authentication failure blacklist time of 0 blocks failed users indefinitely.
Blacklist Time	Number of seconds that a client is quarantined from the network after being blacklisted.

Parameter	Description
Deny Inter User Traffic	This option, when enabled, denies traffic between the clients using this virtual AP profile. The **firewall** comand includes an option to deny all inter-user traffic, regardless of the Virtual AP profile used by those clients. If the global setting to deny inter-user traffic is enabled, all inter-user traffic between clients will be denied, regardless of the settings configured in the virtual AP profiles. If the setting to deny inter-user traffic is disabled globally but enabled on an individual virtual ap, only the traffic between un-trusted users and the clients on that particular virtual AP will be blocked.
Deny time range	Time range for which the AP will deny access.
DoS Prevention	If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.
HA Discovery on-association	If enabled, home agent discovery is triggered on client association instead of home agent discovery based on traffic from client. Mobility on association can speed up roaming and improve connectivity for clients that do not send many uplink packets to trigger mobility (VoIP clients). Best practices is to leave this parameter disabled as it increases IP mobility control traffic between controllers in the same mobility domain. Enable this parameter only when voice issues are observed in VoIP clients. **NOTE: ha-disc-onassoc** parameter works only when IP mobility is enabled and configured on the controller.
Mobile IP	Shows if the profile has enabled or disabled IP mobility.
Preserve Client VLAN	This parameter allows clients to retain their previous VLAN assignment if the client disassociates from an AP and then immediately re-associates either with same AP or another AP on same controller.
Remote-AP Operation	Shows when the virtual AP operates on a remote AP: ■ **always**—Permanently enables the virtual AP (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ **backup**—Enables the virtual AP if the remote AP cannot connect to the controller (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ **persistent**—Permanently enables the virtual AP after the remote AP initially **connects** to the controller (Bridge Mode only). This option can be used for any (Open/PSK/802.1X) bridge VAPs. ■ **standard**—Enables the virtual AP when the remote AP connects to the controller. This option can be used for any (bridge/split-tunnel/tunnel/d-tunnel) VAPs.

Parameter	Description
Station Blacklisting	Shows if the profile has enabled or disabled detection of denial of service (DoS) attacks, such as ping or SYN floods, that are not spoofed deauth attacks.
Strict Compliance	If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.
Multi Association	If enabled, this feature allows a station to be associated to multiple APs. If this feature is disabled, when a station moves to new AP it will be de authorized by the AP to which it was previously connected, deleting station context and flushing key caching information
Fast Roaming	Shows if the AP has enabled or disabled fast roaming.
VLAN Mobility	Shows if the AP has enabled or disabled VLAN (Layer-2) mobility.
WMM Traffic Management Profile	WMM Traffic Management Profile associated with this Virtual AP Profile
Anyspot profile	Anyspot Profile associated with this Virtual AP Profile

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wlan wmm-traffic-management-profile

```
show wlan wmm-traffic-management-profile [<profile-name>]
```

Description

This command displays the list of all WMM traffic management profiles, or detailed configuration information for a specific WMM traffic management profile.

Syntax

Parameter	Description
`<profile-name>`	Name of the WMM traffic management profile.

Usage Guidelines

Issue this command without the **<profile-name>** parameter to display the entire WMM traffic management profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that the managed device has two configured WMM traffic management profiles. The **References** column lists the number of other profiles with references to the WMM traffic management profile, and the **Profile Status** column indicates whether the profile is predefined. (User-defined profiles will not have an entry in the **Profile Status** column.)

```
(host) [mynode] #show wlan wmm-traffic-management-profile

WMM Traffic management profile List
-------------------------------
Name     References  Profile Status
----     ----------  --------------
default  3
test     2

Total:2
```

The following example shows configuration settings defined for the profile **test**:

```
(host) [mynode] #show wlan traffic-management-profile test

WMM Traffic management profile "test"
-----------------------------------
Parameter              Value
---------              -----
Enable Shaping Policy  true
Voice Share            40 %
Video Share            43 %
Best-effort Share      10 %
Background Share       7 %
```

The output of this command includes the following data columns:

Parameter	Description
`Enable Shaping Policy`	Displays if WMM based traffic shaping is enabled on the managed device.
`Voice Share`	Displays the bandwidth allocation in percentage (%) for voice access traffic category.
`Viceo Share`	Displays the bandwidth allocation in percentage (%) for video access traffic category.
`Best-effort Share`	Displays the bandwidth allocation in percentage (%) for best effort access traffic category.
`Background Share`	Displays the bandwidth allocation in percentage (%) for background access traffic category.

Related Commands

Command	Description
wlan wmm-traffic-management-profile	Configures WMM traffic management profile on the managed device.

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wmm tspec-statistics

```
show wmm tspec-statistics
```

Description

A WMM client can send a Traffic Specification (TSPEC) signaling request to the AP before sending traffic of a specific AC type, such as voice. This command displays TSPEC statistics information.

Syntax

No parameters.

Example

The following command displays TSPEC statistics information:

```
(host) [mynode] #show wmm tspec-statistics

TSPEC Enforcement statistics
----------------------------
Name                                        Value
----                                        -----
TSPEC ADDTS Request                         0
TSPEC accepted                              0
TSPEC denied due to CAC                     0
TSPEC enforcement timer events              0
Calls established within enforcement period 0
TSPEC deleted after enforcement period      0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms ap

```
show wms ap {<bssid>|list|stats [mon-mac <mon-mac> bssid <bssid>]|tree}
```

Description

This command displays information for APs currently monitored by the Wireless Management System (WMS).

Syntax

Parameter	Description
<bssid>	Enter the AP's BSSID number in hexadecimal format (XX:XX:XX:XX:XX:XX).
list	Shows the list of all APs monitored by WMS.
stats	Shows the **AP Statistics** table for all APs.
mon-mac <mon-mac>	Shows the **AP Tree** table for an AP with the specified MAC address.
bssid <bssid>	Shows the **AP Tree** table for an AP with the specified BSSID.
tree	Show the APs seen by each monitoring probe in the WMS.

Usage Guidelines

The WMS feature periodically sends statistics that it has collected for APs and Probes to the WMS process. When WMS receives an event message from an AM, it will save the event information along with the BSSID of the AP that generated the event in the WMS database. When WMS receives statistics from the AM, it updates its state, and the database.

Examples

The **show wms ap <bssid>** command displays a list of AP MAC addresses and the BSSIDs seen by each AP.

```
(host) [mynode] #show wms ap 00:0d:67:20:db:4b

AP Info
-------
BSSID              SSID            Channel  Type        RAP_Type     Status  Ageout  HT-Type
-----              ----            -------  ----        --------     ------  ------  -------
00:0d:67:20:db:4b  Ericsson5G-1-1  149      generic-ap  interfering  up      0       HT-20mhz

HT-Sec-Chan
-----------
 0
Probe Info
----------
MAC                IP               Name    Type     Status  AP Type
---                --               ----    ----     ------  -------
40:e3:d6:76:19:70  191.191.191.252  ap-205  soft-ap  up      205
40:e3:d6:8d:ca:f0  191.191.191.253  ap-215  soft-ap  up      215
```

The output of this command includes the following information:

Column	Description
BSSID	Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
SSID	The Service Set Identifier (SSID) that identifies a wireless network.
Channel	Channel used by the AP radio.
Type	A WMS AP type can be one of the following: ■ **soft-ap**: An Aruba Access Point (AP). ■ **air-monitor**: An Aruba Air Monitor (AM).
RAP_Type	Indicates one of the following Rogue AP types: ■ Valid (not a rogue AP) ■ Interfering ■ Rogue ■ Suspected Rogue ■ Disabled Rogue ■ Unclassified ■ Known Interfering
Status	If up, the AP is active. If down (or no information is shown) the AP is inactive.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a -1, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
HT-type	The type of high-throughput traffic sent by the AP: ■ **HT-20mhz**: The AP radio uses a single 20 MHz channel ■ **HT-40mhz**: The AP radio uses a 40 MHz channel pair comprised of two adjacent 20 MHz channels.
HT-Sec-Chan	Secondary channel used for 40 MHz high-throughput transmissions.
MAC	MAC address of a probe that can see the specified AP.
IP	IP address of a probe that can see the specified AP.
Name	Name of the probe.
Type	Displays the probe type: A WMS probe can be one of the following: ■ **soft-ap**: An Aruba Access Point (AP). ■ **air-monitor**: An Aruba Air Monitor (AM).
Status	If up, the AP is active. If down (or no information is shown) the AP is inactive.
AP Type	AP model type.

The example below shows received and transmitted data statistics for each BSSID seen by a monitoring AP.

```
(host)# show wms ap stats
AP Stats Table
---------------
Monitor-MAC        BSSID              RSSI  TxPkt    RxPkt   TxByte     RxByte    HTRates-Tx
-----------        -----              ----  -----    -----   ------     ------    ----------
00:0b:86:c1:af:20  00:0b:86:9a:f2:00  12    1575675  65      173239998  9340        0
00:0b:86:c1:af:20  00:0b:86:9a:f2:08  12    1560559  0       162297938  0           0
00:0b:86:c1:be:56  00:0b:86:9b:e5:60  12    1683013  4188    184400159  257583      0
00:0b:86:c1:be:56  00:0b:86:9b:e5:68  12    1580152  105     164216336  1470        0
00:0b:86:c2:0a:98  00:0b:86:a0:a9:80  48    1608023  40596   166962148  568386      0
```

```
00:0b:86:c2:1c:08  00:0b:86:a1:c0:80  42    1587097  26236   164904668  453196      0
00:0b:86:c2:1c:38  00:0b:86:a1:c3:80  42    1573040  20511   174536514  654024      0
00:0b:86:c2:3e:a9  00:0b:86:a3:ea:90  48    1588204  34179   165017293  897431      0
00:0b:86:c4:0f:3c  00:0b:86:c0:f3:d0  48    1571202  14258   174338376  351148      0
00:0b:86:c4:4d:06  00:0b:86:c4:d0:70  48    1598423  56198   182267018  3805826     0
00:1a:1e:c0:88:82  00:1a:1e:88:88:30  18    1717310  247532  394461405  14998234    8
00:1a:1e:c0:88:82  00:1a:1e:88:88:20  18    1092023  114722  242006054  2442917     10
00:1a:1e:c0:88:88  00:1a:1e:88:88:90  36    1783226  485620  460219125  27781583    16

HTRates-Rx
----------
 0
 0
 0
 0
 0
 0
 0
 0
 0
 0
 8
 10
 16
```

The output of this command includes the following information:

Column	Description
`Monitor-MAC`	MAC address of an AP.
`BSSID`	Basic Service Set Identifier (BSSID) of a station.
`RSSI`	Received Signal Strength Indicator (RSSI) for the station, as seen by the AP.
`txPkt`	Number of transmitted packets.
`RxPkt`	Number of received packets.
`TxByte`	Number of transmitted bytes.
`RxByte`	Number of received bytes.
`HTRates-Tx`	Number of bytes transmitted at high-throughput rates.
`HTRates-Rx`	Number of bytes received at high-throughput rates.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms channel

```
show wms channel stats <num>
```

Description

This command displays per-channel statistics for monitored APs.

Syntax

Parameter	Description
`<num>`	Channel number.

Example

The following example shows per-channel statistics for monitored APs:

```
(host) [mynode] #show wms channel stats

 Channel Stats Table
--------------------
Monitor-MAC        Channel  NumAP  NumSta  TotalPkt  TotalByte   Noise
-----------        -------  -----  ------  --------  ---------   -----
00:0b:86:c1:af:20  1        1      0       5228276   613640650   97
00:0b:86:c1:af:20  6        1      0       1355      168764      0
00:0b:86:c1:af:20  11       8      0       5880      1040338     0
00:0b:86:c1:af:20  36       0      0       2         28          0
00:0b:86:c1:af:20  40       0      0       2         112         0
00:0b:86:c1:af:20  44       0      0       50        903         0
00:0b:86:c1:af:20  48       0      0       23        544         0
00:0b:86:c1:af:20  149      1      0       27094     557579      0
00:0b:86:c1:af:20  153      3      0       4648662   544817261   99
00:0b:86:c1:af:20  165      1      0       1655      200349      0
00:0b:86:c1:be:56  1        43     4       14446324  1959058619  0
00:0b:86:c1:be:56  6        8      1       14168505  1955474600  96
00:0b:86:c1:be:56  11       72     1       180553    23987119    0
00:0b:86:c1:be:56  36       53     0       14716     1022825     0
00:0b:86:c1:be:56  40       8      0       3033      501568      0
00:0b:86:c1:be:56  44       3      0       1453      217596      0
00:0b:86:c1:be:56  48       4      0       5330      1067660     0
00:0b:86:c1:be:56  149      0      0       609279    72205247    105
00:0b:86:c1:be:56  153      1      0       7615369   779579648   0
00:0b:86:c1:be:56  165      1      0       4238      486121      0
00:0b:86:c2:0a:98  40       4      0       4247      434512      0
00:0b:86:c2:0a:98  48       5      0       4052      420436      0
00:0b:86:c2:0a:98  149      4      0       6548323   732910481   104
00:0b:86:c2:1c:08  40       3      0       4613      478188      0
00:0b:86:c2:1c:08  48       4      0       6235436   658263321   103
00:0b:86:c2:1c:08  149      5      0       18904     803078      0
```

Column	Description
`Monitor-MAC`	MAC address of an AP.

Column	Description
`Channel`	802.11 radio channel.
`NumAP`	Number of other APs seen on the specified channel.
`NumSta`	Number stations seen on the specified channel.
`TotalPkt`	Number of received packets.
`TotalByte`	Number of received bytes.
`Noise`	Current noise level.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms client

```
show wms client {list|<mac>|probe <mac>|stats [mon-mac <mon-mac> mac <mac>]|valid-exempt}
```

Description

This command displays the list of client information for the clients that can be seen by monitoring APs.

Syntax

Parameter	Description
`list`	Show statistics for all monitored clients.
`<mac>`	Show statistics for a client with the specified MAC address, including the BSSID of the AP to which that client is currently associated, and the MAC addresses of other monitoring APs that can see that client.
`probe <mac>`	Specify a client's MAC address to show the BSSIDs of all probes that can see that client.
`stats`	Show the STA stats table, which displays data for all clients seen by each monitoring AP.
`mon-mac <mon-mac> mac <mac>`	Enter a monitoring AP's MAC address (<mon-mac>) and the MAC address of a client (<mac>) to show data for traffic received from and sent to a specific client as seen by a specific AP.
`valid-exempt`	Shows a list of valid-exempt clients.

Example

The **AP Info** table in the example below shows that the client is associated to an AP with the BSSID **00:0b:86:cd:86:a0**. The **Probe info** table shows the MAC addresses of three other APs that can see the client.

```
(host) #show wms client 00:0e:35:29:9b:28

STA Info
--------
MAC                Type   Status  Ageout  HT-Type
---                ----   ------  ------  -------
00:0e:35:29:9b:28  valid  up      -1      HT-40mhz

AP Info
-------
BSSID              SSID    Channel  Type     RAP_Type  Status  Ageout       HT-Type   HT-Sec-
Chan
-----              ----    -------  ----     --------  ------  ------       -------   --------
---
00:0b:86:cd:86:a0  MySSiD  11       soft-ap  valid     up      -1           HT-40mhz  153
```

Column	Description
`MAC`	MAC address of the client
`Type`	Station type (**valid**, **interfering**, or **disabled rogue client**)

Column	Description
Status	If **up**, the client is active. If **down** (or no information is shown) the client is inactive.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a **-1**, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
HT-Type	Type of high-throughput traffic sent by the client.
BSSID	BSSID of the AP to which the client is associated.
SSID	Extended service set identifier (ESSID) of the BSSID.
RAP_Type	Indicates one of the following Rogue AP types: ■ Valid (not a rogue AP) ■ Interfering ■ Rogue ■ Disabled Rogue ■ Suspected Rogue ■ Unclassified ■ Known Interfering
Status	If **up**, the AP is active. If **down** (or no information is shown) the AP is inactive.
Ageout	An ageout time is the time, in minutes, that the client must remain unseen by any probes before it is eliminated from the database. If this column displays a **-1**, the client has not yet aged out. Any other number indicates the number of minutes since the client has passed its ageout interval.
HT-Type	Type of high-throughput traffic sent by the AP.
HT-Sec-Chan	Secondary channel used for high-throughput transmissions.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms counters

```
show wms counters [debug|events]
```

Description

This command displays WMS events and debug counters. If you omit the optional **debug** and **events** parameters, the **show wms counters** command displays the frequently used (general) counters in a single table.

Syntax

Parameter	Description
`debug`	Displays debug counters only.
`events`	Displays events counters only.

Usage Guidelines

This command displays counters for database entries, messages, and data structures. The counters displayed vary for each managed device; if the managed device does not have an entry for a particular counter type, it does not appear in the output of this command

Example

The following example shows output for the **show wms counters** command:

```
(host) [mynode] #show wms counters

Counters
--------
Name                        Value
----                        -----
DB Reads                    288268
DB Writes                   350870
Probe Table DB Reads        2477
Probe Table DB Writes       952
AP Table DB Reads           143992
AP Table DB Writes          138867
STA Table DB Reads          40404
STA Table DB Writes         99687
Probe STA Table DB Reads    101352
Probe STA Table DB Writes   117566
Probe Register              2476
Probe State Update          37077
Set RAP Type                42552
Set RAP Type Conf Level     152
Valid Exempt Station Macs   10
...
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms forwarding-stats

```
show wms forwarding-stats
```

Description

This command displays message forwarding statistics between the WLAN Management System (WMS) and Aruba Air Monitor.

Syntax

No parameters.

Example

The following command displays forwarding statistics between the WMS and Air Monitor:

```
(host) [mynode] #show wms forwarding-stats

WMS Forwarding Stats
--------------------
Item                                    Value
----                                    -----
Messages Forwarded                      10
Messages Dropped                        1
Messages Diverted to Local Processing   0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms general

```
show wms general [debug]
```

Description

This command displays general configuration information for the Aruba WLAN Management System (WMS).

Syntax

Parameter	Description
debug	Displays general debugging information for WMS.

Example

The following command displays general configuration information for WMS:

```
(host) [mynode] #show wms general

General Attributes
------------------
Key                            Value
---                            -----
poll-interval                  60000
poll-retries                   2
ap-ageout-interval             30
adhoc-ap-ageout-interval       5
sta-ageout-interval            30
learn-ap                       disable
persistent-neighbor            enable
persistent-valid-sta           disable
propagate-wired-macs           enable
learn-system-wired-macs        disable
stat-update                    disable
collect-stats                  disable
classification-server-ip       0.0.0.0
rtls-port                      8000
wms-on-master                  enable
event-correlation              logs-and-traps
event-correlation-quiet-time   900
use-db                         enable
calc-poll-interval             60000
Switch IP                      192.192.192.1
Services IP                    192.192.192.10
Controller Svcs Role           Svc Master
Is WMS Master                  enable
Minutes Tick                   10516
```

Command History

Release	Modification
ArubaOS 8.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms monitor-summary

```
show wms monitor-summary
```

Description

This command displays the number of different AP and client types monitored over the last 5 minutes, 1 hour, and since the managed device was last reset.

Syntax

No parameters.

Usage Guidelines

The WLAN management system (WMS) monitors wireless traffic to detect any new AP or wireless client stations that attempt to connect to the network. When an AP or wireless client is detected, it is classified and its classification is used to determine the security policies which should be enforced on the AP or client. Use the **show wms monitor-summary** command to view a quick summary of each classified AP and client type currently on the network.

If AP learning is enabled (with the wms general command), non-Aruba APs connected on the same wired network as Aruba APs are classified as valid APs. If AP learning is disabled, a non-Aruba AP is classified as an unsecure or suspect-unsecure AP.

Example

The following example displays a summary of monitored APs and clients on a managed device:

```
(host) [mynode] #show wms monitor-summary

WMS Monitor Summary
-------------------
                          Last 5 Min  Last Hour  All
-                         ----------  ---------  ---
Valid APs                 1           1          1
Interfering APs           57          57         60
Rogue APs                 3           3          3
Manually Contained APs    0           0          0
Unclassified APs          0           0          0
Neighbor APs              0           0          0
Suspected Rogue APs       138         138        139
Valid Clients             0           0          0
Interfering Clients       1           1          1
Manually Contained Clients 0          0          0
```

Command History

Release	Release
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms probe

```
show wms probe
```

Description

This command displays detailed information on WMS probes.

Syntax

No parameters.

Example

This example shows the Probe List table for WMS probes. The output below has been split into two tables to better fit in this document. In the actual CLI, this information appears in a single, long table.

```
(host) [mynode] #show wms probe

Probe List
----------
Monitor Eth MAC    BSSID              PHY Type         IP               LMS IP         Scan
Status  Updates  Reqs/Fails  Stats  Type
---------------    -----              --------         --               ------         ----  -
-----  -------  ----------  -----  ----
40:e3:d6:cf:61:96  40:e3:d6:76:19:60  80211GHT-20mhz   191.191.191.252  192.192.189.1  No
Up      6850     1/0         0      soft-ap
40:e3:d6:cf:61:96  40:e3:d6:76:19:70  80211AVHT-80mhz  191.191.191.252  192.192.189.1  No
Up      6860     0/0         0      soft-ap
40:e3:d6:c0:dc:ae  40:e3:d6:8d:ca:e0  80211GHT-20mhz   191.191.191.253  192.192.189.1  No
Up      6924     1/0         0      soft-ap
40:e3:d6:c0:dc:ae  40:e3:d6:8d:ca:f0  80211AVHT-80mhz  191.191.191.253  192.192.189.1  No
Up      6909     0/0         0      soft-ap
Total:4
```

Column	Description
`Monitor Eth MAC`	Ethernet MAC address of a probe.
`BSSID`	Probe Radio BSSID.
`PHY Type`	Radio PHY type: ■ 802.11A ■ 802.11AHT-40Mbps ■ 802.11AHT-20Mbps ■ 802.11G ■ 802,11GHT-20Mbps
`IP`	IP address of the AP.
`LMS IP`	IP address of the AP's managed device.
`Scan`	Shows if the Air Monitor is performing scanning.
`Status`	If the scan column displays a status of Up, the AP or AM is active
`Updates`	Number of updates the AP or AM sent to the WMS database since the managed device was last reset.

Column	Description
`Reqs/Fails`	Number of database update requests that have not yet been added into the database. and the number of failed database requests.
`Stats`	Total number of statistics updates sent to the database.
`Type`	A WMS AP type can be one of the following: ■ **soft-ap**: An Aruba Access Point (AP). ■ **air-monitor**: An Aruba Air Monitor (AM).

Command History

Release	Release
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms rogue-ap

```
show wms rogue-ap <bssid> [list]
```

Description

This command displays statistics for APs classified as rogues APs.

Syntax

Parameter	Description
`<bssid>`	BSSID of a rogue AP.
`list`	Shows Rogue AP list.

Usage Guidelines

The optional output modifiers | begin , | exclude, and | include help you display those lines that begin, include, exclude, respectively, the line expression given in the CLI command. The | redirect-output modifier helps you redirect the command output.

Example

The output of this command shows statistics for a suspected rogue AP:

```
(host) [mynode] #show wms rogue-ap 00:0b:86:d4:ca:12

Suspect Rogue AP Info
---------------------
Key                Value
---                -----
BSSID              00:0b:86:89:c6:20
SSID               aruba-ap
Channel            1
Type               generic-ap
RAP Type           suspected-rogue
Status             up
Match Type         AP-Rule
Match MAC          00:0b:86:61:8a:d0
Match IP           0.0.0.0
Match AM           ssahoo-155
Match Method       Exact-Match
Match Time         Sun Sep 19 19:11:40 2010
```

The output of this command includes the following information:

Column	Description
`BSSID`	BSSID of the suspected rogue AP.
`SSID`	The rogue AP's Extended service set identifier.
`Channel`	Channel used by a radio on the rogue AP.

Column	Description
Type	Indicates if the AP is an Aruba AP, a Cisco AP, or an AP from any other manufacturer (generic AP).
RAP Type	Type of rogue AP, ■ **Suspect-unsecure**: AP has not been confirmed as a rogue AP. ■ **unsecure**: AP has been confirmed as a rogue AP
Status	Shows if the AP is active (**up**) or inactive (**down**).
Match Type	Describes how the AP was classified as a rogue. ■ **Eth-Wired-MAC**: An Aruba AP or AM detected that a single MAC address was in both the Ethernet Wired-Mac table and a non-valid AP wired-Mac table. ■ **AP-Wired-MAC**: An interfering AP is marked as rogue when the Aruba AP finds a MAC address in one of its valid AP wired-mac table and in an interfering AP wired-mac table. You can enable or disable the AP-Wired-MAC matching method using the CLI command **ids unauthorized-device-profile overlay-classification**. ■ **Config-Wired-MAC**: This type of classification occurs when an Aruba AP or AM detects a match between a wired MAC table and a pre-defined MAC address that has manually defined via the command ids unauthorized-device-profile . ■ **External-Wired-MAC**: This type of classification occurs when an Aruba AP or AM detects a match between a wired MAC table entry and a pre-defined MAC address manually defined in the ids rap-wml-server-profile table. ■ **Base-BSSID-Override**: If an Aruba AP is detected as rogue, then all virtual APs on the particular rogue are marked as rogue using Base-BSSID-Override match type. ■ **Manual**: An AP is manually defined as a rogue by via the command wms ap <bssid> mode rogue. ■ **EMS**: An AP is manually defined as a rogue by via the Element Management System.
Match MAC	MAC address of a wired device that helped identify the AP as a rogue. If the AP has not been identified as a rogue, this column will display the MAC address 00:00:00:00:00:00.
Match IP	IP address of a wired device that helped identify the AP as a rogue.
Match AM	Aruba Air Monitor that reported seeing the rogue AP.
Match Method	This variable indicates the type of match.
Match Time	Time the AP was identified as a rogue AP.

Command History

Release	Modification
ArubaOS 8.2.0.0	The **list** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms rogue-ap list

```
show wms rogue-ap list
```

Description

This command displays the information on the rogue APs in the network.

Syntax

No parameter.

Usage Guidelines

When an AM classifies an interfering AP as a Rogue AP it sends that classification to the WMS process.

Use this command to list all known Rogue APs that may be potential security threats.

Examples

The **show wms rogue-ap list** command displays a list of rogue APs detected in the network.

```
(host)[mynode] #show wms rogue-ap list
AP List
-------
BSSID             ESSID        Class   PHY Type AP-name Encryp        IBSS   Last Mon Eth MAC
-----             -----         -----  -------- ------- ------        ----  ----------------
ac:a3:1e:53:72:94 arturo04      rogue  80211A           wpa2-psk-aes   no    ac:a3:1e:cd:35:5a
84:d4:7e:64:1c:72 hpeguest      rogue  80211A           open           no    ac:a3:1e:cd:35:5a
00:62:ec:26:2e:2f smtcwireless  rogue  80211A           wpa-8021x-tkip no    c8:b5:ad:c3:ac:fc
Total: 3
```

The output of this command includes the following information:

Column	Description
BSSID	Basic Service Set Identifier (BSSID) for the AP. This is usually the AP's MAC address.
ESSID	The Extended Service Set Identifier (SSID) that identifies a wireless network.
Class	AP classification: will always be set to 'rogue'. A rogue AP that is unauthorized and is plugged into the wired side of the network. You can configure automatic shutdown of rogue APs in the IDS unauthorized device detection profile.
PHY Type	Shows one of the following 802.11 types: ■ 802.11a ■ 802.11b ■ 802..11g ■ 802.11 ag
AP-name	Name of the rogue AP.
Encryp	Encryption type used on each listed rogue AP.

Column	Description
IBSS	Shows if ad hoc BSS is enabled or disabled on each listed rogue AP.
Last Mon Eth MAC	Shows the last monitored MAC address seen on the wired network for this rogue AP.

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on the controller or managed device.

show wms routers

```
show wms routers [<mac>]
```

Description

This command displays learned router MAC information for WMS APs.

Syntax

Parameter	Description
<mac>	MAC address of a probe that can see the router.

Usage Guidelines

This command displays the MAC addresses of devices that have been determined to be routers by the listed APs. This output of this command will be blank if there is not any broadcast or multicast activity in an AP's subnet.

Example

In the example below, a single WMS AP has learned MAC information for four different routers.

```
(host) [mynode] #show wms routers

Router Mac 00:08:00:00:11:12 is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
Router Mac 00:08:00:00:11:29 is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
Router Mac 00:08:00:00:11:57 is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
Router Mac 00:08:00:00:11:6e is Seen by APs
-------------------------------------------
AP-Name
-------
AP32
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms rules

```
show wms rules
   config
   state
   summary
```

Description

This command displays the internal state and matching information of rules created using the ids ap-classification-rule command.

Syntax

Parameter	Description
`config`	Displays the following information for each AP classification rule: ■ name ■ ids ■ match-ssid ■ min-snr ■ max-snr ■ min-prcnt ■ max-prcnt ■ ssids ■ enabled ■ classify ■ conf-incr ■ flags ■ match-cnt
`state`	Displays the following information for each AP classification rule: ■ SSID Match Table ■ SSID Exclude Table ■ SNR Table ■ Probe Count Table
`summary`	Displays a summary of AP classification rules.

Usage Guidelines

Issue this command to view existing AP classification rules. AP classification rule configuration can only be performed on a Mobility Master. If AMP is enabled via the mobility-manager command, then processing of the AP classification rules is disabled on Mobility Master. A rule is identified by its ASCII character string name (32 characters maximum). The AP classification rules have one of the following specifications:

- SSID of the AP
- SNR of the AP
- Discovered-AP-Count or the number of APs that can see the AP

Example

The output in the example below shows that although two rules have been defined, neither have been enabled using the **ids ap-rule-matching rule-name <name>** command.

```
(host) [mynode] #show wms rules summary
```

```
AP Classification Rules Summary
-------------------------------
Parameter                Value
---------                -----
Num Rules                2
Num Active-Rules         0
Num SSID-to-match        0
Num SSID-to-exclude      0
Num SNR-bounds           0
Num Probe-Count-bounds   0
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wms system

```
show wms system
```

Description

This command displays the WMS system configuration and system state.

Syntax

No parameters.

Example

The following example shows the WMS System Configuration and System State tables:

```
(host) [mynode] #show wms system

System Configuration
--------------------
Key                              Value
---                              -----
max-ap-threshold                 0
max-sta-threshold                0
max-rbtree-entries               0
max-system-wm                    1000
system-wm-update-interval        8
periodic-ap-snapshot-interval    180
periodic-rap-snapshot-interval   30
periodic-sta-snapshot-interval   180
override-svc-termination         disable
System State
-------------
Key                     Value
---                     -----
Max AP Threshold        250000
Max STA Threshold       750000
Total AP Count          371
Total STA Count         14
Max RB-tree Threshold   2000000
Current RB-Tree Count   530
Poll Count(Max)         1(4)
WMS Offload State
-----------------
Metric          Threshold  Current
------          ---------  -------
AP Count        200000     371
STA Count       600000     14
RB-Tree Count   1600000    530
Probe Count     20000      4
WMS Offload: Disabled
Learned OUIs for Deployed APs
-----------------------------
OUI
---
40:e3:d6:00:00:00
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

show wms wired-mac

```
show wms wired-mac {gw-mac [<mac>]|monitored-ap-wm [<mac>]|prop-eth-mac [<mac>]|reg-ap-oui
[<mac>]|summary|system-gw-mac [<mac>]|system-wired-mac [<mac>]|wireless-device [<mac>]}
```

Description

This command displays a summary table of WLAN Management System (WMS) wired MAC information. This command can display a list of APs aware of a specific gateway MAC address, or list the wired MAC addresses known to a single AP.

Syntax

Column	Description
gw-mac	Shows gateway wired MAC information collected from the APs.
<mac>	Displays information for a single MAC address.
monitored-ap-wm	Shows monitored AP wired MAC information collected from the APs.
<mac>	Displays information for a single MAC address.
prop-eth-mac	Shows wired mac information collected from the APs.
<mac>	Displays information for a single MAC address.
reg-ap-oui	Shows registered AP OUI information collected from the APs, including each registered OUI, and the time that OUI was last seen.
<mac>	Displays information for a single MAC address.
summary	Display a wired MAC summary that includes the number of each of the following MAC types: ■ Registered AP OUIs ■ Propagated Ethernet MACs. ■ Potential Wireless Device MACs ■ Monitored AP Wired MACs ■ System Wired MACs ■ System Gateway MACs
system-gw-mac	Shows system gateway MAC information learned at the managed device, including the age of each MAC address.
<mac>	Displays information for a single MAC address.
system-wired-mac	Shows system wired MAC information learned at the managed device.
<mac>	Displays information for a single MAC address.
wireless-device	Show routers or potential wireless devices information, including the MAC address of the device, and the MAC address of the AP or managed device that saw the device.
<mac>	Displays information for a single MAC address.

Example

The following example shows the wired MAC summary:

```
(host) [mynode] #show wms wired-mac summary

Wired MAC Summary
-----------------
Type                            Count
----                            -----
Gateway MACs                    1
Registered AP OUIs              16
Propagated Ethernet MACs        0
Potential Wireless Device MACs  0
Monitored AP Wired MACs         0
System Wired MACs               0
System Gateway MACs             0
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show wnm-dot11v bss-tm-response

```
show wnm-dot11v bss-tm-response station-mac <mac>
```

Description

This command displays the BSS transition management response for a given client.

Syntax

Column	Description
<mac>	MAC address of the client.

Example

The following example shows the BSS transition management response for a client:

```
(host) [mynode] #show wnm-dot11v bss-tm-response station-mac 58:94:6b:31:d0:f0
VLAN Assignment
---------------
VLAN   #CLIENTS
----   --------
1      0
192    1
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command Introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

show ip interface brief

```
show ip interface brief
```

Description

This command displays the IP-related information on all interfaces in summary format.

Syntax

No parameters.

Example

```
(host) #show  ip interface brief

Interface                   IP Address / IP Netmask        Admin    Protocol     VRRP-IP
vlan 1                   172.16.0.254 / 255.255.255.0      up       up
vlan 2                      10.4.62.9 / 255.255.255.0      up       up
loopback                  unassigned / unassigned          up       up
mgmt                      unassigned / unassigned          down     down
```

The following table details the columns and content in the show command.

Column	Description
Interface	List the interface and interface identification, where applicable.
IP Address /IP Netmask	List the IP address and netmask for the interface, if configured.
Admin	States the administrative status of the interface. Enabled—up Disabled—down
Protocol	Status of the IP on the interface. Enabled—up Disabled—down
VRRP-IP	VRRP IP address associated to the interface.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

snmp-server

```
snmp-server
   community <string>
   enable
   engine-id
                  host IPv4/IPv6 Address|version {1 <name> udp-port <port>}|2c|{3 <name>}
      [inform] [interval <seconds>] [retrycount <number>] [udp-port <port>]}
   inform queue-length <size>
   source controller-ip
   stats
   trap {source [IPv4|IPv6 Address]|<name>}
   user
        <word>
        [auth-prot [md5|sha] <string>]
        [priv-prot {AES|DES} <string>]
```

Description

This command configures SNMP parameters.

Syntax

Parameter	Description	Range	Default
`community`	Sets the read-only community string.	—	—
`enable`	Enables sending of SNMP traps to the configured host.	—	disabled
`engine-id`	Sets the SNMP server engine ID as a hexadecimal number.	24 characters maximum	—
`host`	Configures the IPv4/IPv6 Address address of the host to which SNMP traps are sent. This host needs to be running a trap receiver to receive and interpret the traps sent by the controller.	—	—
`version`	Configures the SNMP version and security string for notification messages.	—	—
`inform`	Sends SNMP inform messages to the configured host.	—	disabled
`inform`	Specifies the length for the SNMP inform queue.	100-350	250

Parameter	Description	Range	Default
`stats`	Allows file-based statistics collection. The Mobility Master generates a file that contains statistics data to display information in chart and graph formats. File-based statistics collection is transparent to the user and increases the efficiency of transferring information.		enabled
`trap {source [IPv4|IPv6 Address]|<name>}`	Configures source IPv4 or IPv6 address or name of SNMP traps.	—	disabled
`user`	Configures an SNMPv3 user profile.	—	—
`<word>`	USM security model user name		
`[auth-prot [md5|sha] <string>]`	Authentication protocol of the user and the password to use with the protocol.	MD5/SHA	SHA
`[priv-prot {AES|DES} <string>]`	Privacy protocol of the user and the password to use with the protocol.	AES/DES	DES

Usage Guidelines

This command configures SNMP parameters. You configure SNMP-related information for APs in an SNMP profile which you apply to an AP group or to a specific AP.

Example

The following command configures an SNMP user:

```
(host) [mynode] (config) #snmp-server user temp auth-prot md5 temp12 priv-prot aes temp34
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

spanning-tree

```
spanning-tree
   forward-time <value>
   hello-time <value>
   max-age <value>
   mode <rapid> | <rapid-pvst>
   priority <value>
   vlan range {<word>|[remove <word> {forward-time|hello-time|max-age|priority}]}
```

RSTP is backward compatible with STP and is enabled by default. For ease of use, this command uses the spanning tree keyword.

Description

This command configures global settings for the Rapid Spanning Tree Protocol (RSTP) and Per VLAN Spanning Tree (PVST+). Refer to interface gigabitethernet for details on enabling and configuring spanning tree for an individual interface.

Syntax

Parameter	Description	Range	Default
`forward-time`	Specifies the time, in seconds, the port spends in the listening and learning state. During this time, the port waits to forward data packets.	4-30	15 seconds
`hello-time`	Specifies the time, in seconds, between each bridge protocol data unit (BPDU) transmitted by the root bridge.	1-10	2 seconds
`max-age`	Specifies the time, in seconds, the root bridge waits to receive a hello packet before changing the STP topology.	6-40	20 seconds
`mode`	Set the spanning tree mode to either Rapid Spanning Tree (802.1w) or PVST+ (Per VLAN Spanning Tree)	N/A	N/A
`<rapid>`	Set the spanning tree mode to RSTP (Rapid Spanning Tree Protocol).	N/A	N/A
`<rapid-pvst>`	Set the spanning tree mode to PVST+ (Per VLAN Spanning Tree protocol)	N/A	N/A
`priority`	Set the priority of a bridge to make it more or less likely to become the root bridge. The bridge with the lowest value has the highest priority. When configuring the priority, remember the following: The highest priority bridge is the root bridge. The highest priority value is 0 (zero).	0-65535	32768

Parameter	Description	Range	Default
`vlan range <WORD>`	Enter the keywords **vlan range** followed by the range of VLAN ID's. Separate the VLAN IDs with a hyphen, comma or both to indicate the range. For example: 2-3 or 2,4,6 or 2-6,11	—	—
`remove <word>`	Removes range of VLAN IDs.	—	—
`remove <word> forward-time`	Removes the spanning tree forward interval.	—	—
`remove <word> hello-time`	Removed the spanning tree hello interval.	—	—
`remove <word> max-age`	Removes the spanning tree maximum age interval.	—	—
`remove <word> priority`	Removes the spanning tree priority interval.	—	—

Usage Guidelines

This command configures the global RSTP settings and is backward compatible with past versions of ArubaOS using STP.

By default, all interfaces and ports run RSTP as specified in 802.1w and 802.1D. The default RSTP values can be used for most implementations.

Use the `no spanning-tree` command to disable RSTP.

Examples

The following command sets the time a port spends in the listening and learning state to 3 seconds:

```
(host) [mynode] #spanning-tree forward-time 3
```

The following command sets the time the root bridge waits to transmit BPDUs to 4 seconds:

```
(host) [mynode] #spanning-tree hello-time 4
```

The following command sets the time the root bridge waits to receive a hello packet to 30 seconds:

```
(host) [mynode] #spanning-tree max-age 30
```

The following command sets the bridge priority to 10, making it more likely to become the root bridge:

```
(host) [mynode] #spanning-tree priority 10
```

The follow command sets a spanning-tree VLAN range

```
(host) [mynode] #spanning-tree vlan range 2-8,11
```

Command History:

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Configuration mode on Mobility Master

ssh

```
ssh
   disable-ciphers {aes-cbc | aes-ctr}
   disable-mac hmac-sha1-96
   disable_dsa
   mgmt-auth {public-key [username/password]|username/password [public-key]}
   <username> <ip_addr>
```

Description

This command configures SSH access to a Mobility Master.

Syntax

Parameter	Description	Default
`disable-ciphers`	Disables cipher authentication for SSH. Specify the cipher to be disabled.	—
`aes-cbc`	Disables AES-CBC authentication for SSH. This parameter enables the **`aes-ctr`** encryption.	—
`aes-ctr`	Disables AES-CTR authentication for SSH. This parameter enables the **`aes-cbc`** encryption.	—
`disable-mac`	Disables Message Authentication Code algorithm for SSH authentication.	hmac-sha1-96
`hmac-sha1-96`	Disables HMAC-SHA1-96 authentication for SSH.	
`disable_dsa`	Disables DSA authentication for SSH. Only RSA authentication is used.	—
`mgmt-auth`	Configures the authentication method for the management user. You can specify a username and password only, public key only, or both username and password and public key.	username and password
`<username>`	Username for SSH login.	—
`<ip_addr>`	IPv4 or IPv6 address of the remote machine.	—

Usage Guidelines

Public key authentication is supported using a X.509 certificate issued to the management client. If you specify public-key authentication, you need to load the client X.509 certificate into Mobility Master and configure certificate authentication for the management user with the **mgmt-user ssh-pubkey** command.

Example

The following command configures SSH access using public key authentication only:

```
(host) [mynode] (config) #ssh mgmt-auth public-key
   mgmt-user ssh-pubkey client-cert ssh-pubkey cli-admin root
```

The following command enables **AES-CBC** and disables **AES-CTR** on the SSH server:

```
(host) [md] (config) #ssh disable-ciphers aes-ctr
```

The following command enables both the cipher encryptions on the SSH server:

```
(host) [md] (config) #no ssh disable-ciphers
```

The following command disables **HMAC-SHA1-96** on the SSH server:

```
(host) [md] (config) #ssh disable-mac hmac-sha1-96
```

Related Commands

Command	Description
show ssh	Displays the SSH configuration details.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.3.0.0	The following parameters are introduced to configure cipher and MAC authentication: ■ **disable-ciphers** ■ **disable-mac**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

sso idp-profile

```
sso idp-profile <sso_prof_name>
   clone <source>
   idp <string> <url>
   no
```

Description

This command configures an SSO Identity Provider profile for use with application SSO with L2 Authentication.

Syntax

Parameter	Description
`<sso_prof_name>`	Name of the L2SSO profile.
`clone <source>`	Copies data from another SSO IDP profile.
`idp <string> <url>`	Configures the name and URL of Mobility Master's IDP server.
`no`	Deletes the command.

Usage Guidelines

This command is used to configure an SSO IDP profile, which establishes the name and URL of the IDP server that Mobility Master uses for application SSO.

ClearPass Policy Manager is the only device that can act as an IDP server for application SSO with an Aruba managed device.

Example

```
(host) [mynode] (config) #sso idp-profile profile1
   idp url1 cppm128.arubanetworks.com/idp.login
```

Related Commands

Command	Description
show sso idp-profile	Displays all SSO IDP profiles.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

stm

```
stm
   add-blacklist-client <macaddr>
   disable-timing-stats
   enable-timing-stats
   kick-off-sta <macaddr> <bssid>
   purge-blacklist-clients
   remove-blacklist-client <macaddr>
   start-trace <macaddr>
   stop-trace <macaddr>
   mon-update-queue <threshold>
```

Description

This command is used to manually disconnect a client from an AP or control the blacklisting of clients.

Syntax

Parameter	Description
`add-blacklist-client`	MAC address of the client to be added to the denial of service list.
`disable-timing-stats`	Disables performance monitoring in STM.
`enable-timing-stats`	Enables performance monitoring in STM.
`kick-off-sta`	When you use the kick-off-sta feature specify a client's MAC address and BSSID, the AP sends deauthorization frames to the station to disconnect it.
`<macaddr>`	MAC address of client to be disconnected.
`<bssid>`	The associated BSSID of the client to be disconnected.
`purge-blacklist-client`	Clear the entire client blacklist.
`remove-blacklist-client <macaddr>`	Specify the MAC address of a client to remove it from the denial of service list.
`start-trace <macaddr>`	Starts tracing probe requests and probe responses from the specified client.
`stop-trace <macaddr>`	Stops tracing probe requests and probe response from the specified client.
`mon-update-queue <threshold>`	Configures the maximum queue size for the STM monitoring updates. **NOTE:** This parameter is available only in Config mode on Mobility Master.

Usage Guidelines

When you blacklist a client, the client is not allowed to associate with any AP in the network. If the client is connected to the network when you blacklist it, a deauthentication message is sent to force the client to disconnect. The blacklisted client is blacklisted for the duration specified in the virtual AP profile. The client blacklist supports up to 4,000 individual client entries.

The managed device retains the client blacklist in the user database, so the information is not lost if the managed device reboots. When you import or export the managed device's user database, the client blacklist will be exported or imported as well.

Example

The following command blacklists a client:

```
(host) #stm add-blacklist-client 00:01:6C:CC:8A:6D
```

Related Commands

Command	Description
show stm	This command is used to display the deauthentication reasons and the monitoring update queue information from the station management module.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master.

support

```
support
```

Description

This command, which should be used only in conjunction with Aruba customer support, is for controller debugging purposes only.

Syntax

No parameters.

Usage Guidelines

This command is used by Aruba customer support for debugging the controller. Do not use this command without the guidance of Aruba customer support.

Example

The following command allows Aruba customer support to debug the controller:

```
(host) #support
```

Command History

Version	Modification
ArubaOS 2.4	Command introduced as the **secret** command
ArubaOS 3.1	Command renamed to **support**

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

syscontact

```
syscontact <syscontact>
```

Description

This command configures the name of the system contact for the managed device.

Syntax

Parameter	Description
`<syscontact>`	An alphanumeric string that specifies the name of the system contact.

Usage Guidelines

Use this command to enter the name of the person who acts as the system contact or administrator for the managed device. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the alphanumeric string. For example, to create the system contact name Lab Technician 1, enter "Lab Technician 1" at the prompt.

To change the existing name, enter the command with a different string. The new name takes affect immediately. To unconfigure the name, enter "" at the prompt.

Example

The following command defines **LabTechnician** as the system contact name:

```
(host) [mynode] (config) #syscontact LabTechnician
```

Related Commands

Command	Description
show syscontact	Displays the system contact information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on managed devices.

syslocation

```
syslocation <syslocation>
```

Description

This command configures the name of the system location for the managed device.

Syntax

Parameter	Description
`<syslocation>`	An alphanumeric string that specifies the name of the system location.

Usage Guidelines

Use this command to indicate the location of the managed device. You can use a combination of numbers, letters, characters, and spaces to create the name. To include a space in the name, use quotation marks to enclose the text string.

To change the existing name, enter the command with a different string. To unconfigure the location, enter "" at the prompt.

Example

The following command defines **SalesLab** as the system location:

```
(host) [mynode] (config) #syslocation "Building 10, second floor, room 21E"
syscontact LabTechnician
```

Related Commands

Command	Description
show syslocation	Displays the system location information.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on managed devices.

tar

```
tar clean {crash|flash|logs}| crash [kernel] | flash | logs [tech-support {no-controllerip
 | user <mac-address>}]
```

Description

This command archives a directory.

Syntax

Parameter	Description
`clean`	Removes a tar file
`crash`	Removes crash.tar
`flash`	Removes flash.tar.gz
`logs`	Removes logs.tar
`crash`	Archives the crash directory to crash.tar. A crash directory must exist.
`kernel`	Archives the kernel crash directory to kernel_crash.tar.
`flash`	Archives and compresses the /flash directory to flash.tar.gz.
`logs`	Archives the logs directory to log.tar.
`tech-support {no-controllerip | user <mac-address>}`	Optionally, technical support information can be included for a specific user.

Usage Guidelines

This command creates archive files in Unix tar file format.

Example

The following command creates the log.tar file with technical support information:

```
(host) [mynode] (config) #tar logs tech-support
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	This command is available in the base operating system. The **ipaccess-group** parameter requires the PEFNG license. The **xsec** parameter requires the xSec license.	Enable or config mode on Mobility Master.

telnet

```
telnet <host> [port <port_num>]
   cli
   soe
```

Description

This command enables telnet to Mobility Master or to an AP through Mobility Master.

Syntax

Parameter	Description	Default
`host`	IP address of the host Mobility Master	—
`port`	Port number in the host	—
`cli`	Enable telnet using the CLI.	Disabled
`soe`	Enable telnet using Serial over Ethernet (SoE).	Disabled

Usage Guidelines

Use the host and port to specify the host IP address and the port to enable telnet. This command is available only in **Enable** mode.

Use the **cli** option to enable telnet to Mobility Master.

Use the **soe** option to enable telnet using the SoE protocol. This allows you to remotely manage an AP directly connected to Mobility Master.

Example

The following example enables telnet to Mobility Master using the CLI:

```
(host) [mynode] (config) #telnet cli
```

Related Commands

Command	Description
show telnet	Displays the telnet access status.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master.

threshold

```
threshold
   controlpath-cpu <value>
   controlpath-memory <value>
   datapath-cpu <value>
   no-of-APs <value>
   no-of-locals <value>
   total-tunnel-capacity <value>
   user-capacity <value>
   no
```

Description

This command configures managed device capacity thresholds which, when exceeded, trigger alerts.

Syntax

Parameter	Description	Range	Default
`controlpath-cpu <value>`	Sets an alert threshold, in percentage, for the control path CPU capacity that must be exceeded before the alert is sent.	0-100%	80%
`controlpath-memory <value>`	Sets an alert threshold, in percentage, for the control path memory consumption that must be exceeded before the alert is sent.	0-100%	85%
`datapath-cpu <value>`	Sets an alert threshold, in percentage, for the datapath CPU capacity that must be exceeded before the alert is sent.	0-100%	30%
`no-of-APs <value>`	The maximum number of APs that can be connected to a managed device is determined by that managed device's model type and installed licenses. Use this command to trigger an alert when the number of APs currently connected to the managed device exceeds a specific percentage of its total AP capacity.	0-100%	80%
`no-of-locals <value>`	Sets an alert threshold, in percentage, for the Mobility Master's capacity to support managed devices that must be exceeded before the alert is sent.	0-100%	80%
`total-tunnel-capacity <value>`	Sets an alert threshold, in percentage, for the managed device's tunnel capacity that must be exceeded before the alert is sent.	0-100%	80%
`user-capacity <value>`	Sets an alert threshold, in percentage, for the managed device's user capacity that must be exceeded before the alert is sent.	0-100%	80%

Usage Guidelines

The managed device sends a *wlsxThresholdExceeded* SNMP trap and a syslog error message when the managed device has exceeded a set percentage of the total capacity for that resource. A *wlsxThresholdCleared* SNMP trap and error message will be triggered if the resource usage drops below the threshold once again.

Example

The following command configures a new alert threshold for controlpath memory consumption:

```
(host) [mynode] (config) #threshold datapath-cpu 90
```

If this threshold is exceeded then subsequently drops below the 90% threshold, the managed device would send the following two syslog error messages.

```
Mar 10 13:13:58  nanny[1393]: <399816> <ERRS> |nanny|  Resource 'Control-Path Memory' has gone
above  90%  threshold, value : 93
Mar 10 13:16:58  nanny[1393]: <399816> <ERRS> |nanny|  Resource 'Control-Path Memory' has come
below  90%  threshold, value : 87
```

Related Commands

Command	Description
show threshold	Displays the managed device capacity thresholds which, when exceeded, triggers alerts.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

time-range

```
time-range
   absolute <name> [end <mm/dd/yyyy> <hh:mm>][start <mm/dd/yyyy> <hh:mm>]
   no
   periodic <name>
      Daily <hh:mm> to <hh:mm>
      Friday <hh:mm> to <hh:mm>
      Monday <hh:mm> to <hh:mm>
      Saturday <hh:mm> to <hh:mm>
      Sunday <hh:mm> to <hh:mm>
      Thursday <hh:mm> to <hh:mm>
      Tuesday <hh:mm> to <hh:mm>
      Wednesday <hh:mm> to <hh:mm>
      Weekday <hh:mm> to <hh:mm>
      Weekend <hh:mm> to <hh:mm>
```

Description

This command configures time ranges.

Syntax

Parameter	Description
`absolute <name>`	Specifies an absolute time range, with a specific start time, end time, and date.
`end <mm/dd/yyyy> <hh:mm>`	Specifies the end time of the time range.
`start <mm/dd/yyyy> <hh:mm>`	Specifies the start time of the time range.
`no`	Negates any configured parameter.
`periodic <name>`	Specifies a recurring time range. Select the day of the week occurrence, the start time (hh:mm), and the end time (hh:mm).

Usage Guidelines

You can use time ranges when configuring session ACLs. Once you configure a time range, you can use it in multiple session ACLs.

Example

The following command configures a time range for daytime working hours:

```
(host) [mynode] (config) #time-range periodic working-hours
   weekday 7:30 to 18:00
```

Related Commands

Command	Description
show time-range	Displays the configured time ranges.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Next Generation Policy Enforcement Firewall (PEFNG) license.	Enable and Config modes on Mobility Master and managed devices.

time-range-profile

```
time-range-profile <profile-name>
   absolute [start-date <abs_sdate> start-time <abs_stime>][end-date <abs_edate> end-time
   <abs_etime>]
   mode {absolute|periodic}
   no
```

Description

This command configures time range profiles.

Syntax

Parameter	Description
`<profile-name>`	Name of the time range profile.
`absolute`	Specifies an absolute time range profile, with a specific start date, start time, end date, and end time.
`start-date <abs_sdate>`	Start date for the time range profile (mm/dd/yyyy).
`start-time <abs_stime>`	Start time for the time range profile (hh:mm).
`end-date <abs_edate>`	End date for the time range profile (mm/dd/yyyy).
`end-time <abs_etime>`	End time for the time range profile (hh:mm).
`mode`	Time range profile mode: ■ Absolute ■ Periodic
`no`	Negates any configured parameter.

Usage Guidelines

You can use time range profiles when configuring session ACLs. After you configure a time range profile, you can use it in multiple session ACLs.

Example

The following command configures a time range profile for a training class that takes place between 8:30AM and 6:00PM:

```
(host) [node] (config) #time-range-profile training absolute
   start-date <06/19/2016>
   start-time <08:30>
   end-date <06/19/2016>
   end-time <18:00>
```

Related Commands

Command	Description
show time-range	Displays the configured time ranges.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Next Generation Policy Enforcement Firewall (PEFNG) license.	Enable and Config modes on Mobility Master and managed devices.

traceoptions

```
traceoptions
   chassis-manager flags {all|association|debug|environment-
   monitoring|fru|interface|interface-statistics|ipc|poe-configuration|poe-
   statistics|statistics-sync|system-statistics}
   igmp flags {all|debug|leave|query|report}
   igmp-snooping flags {all|config|errors|receive|transmit}
   interface-manager {flags {all|configuration|dhcp-
   client|ethernet|infrastructure|lacp|loopback|mgmt|oam|port-channel|port-mirroring|system-
   information|tunnel|vlan} | level {debug|error|verbose}}
   layer2-forwarding {flags{all|config|fdb|hsl|interface|ipc|learning|nexthop|port-loop-
   protect|sysinfo|task|timer|tunneled-node|vlan|vlan-assignment|vlan-port} | level
   {debugging|errors|informational} |
   {size <tracefile_size>}}
   lldp flags {all|errors|receive|system-state|transmit}
   mstp {flags {all|config|debug|port-information|received-bpdu-all|role-selection|sent-bpdu-
   all|state-machine-changes|system|topology-change|} | port<mstp_trace_port>}
   no
   ospf flags {all|cnf|db|dd|debug|dr-elec|flood|hello|lsa|lsr|lsu|msm|pkt-all|spf|state}
   pim flags {adjacency|all|debug|jp-asserts|register|route|state}
   rmon {flags {alarm|all|cli|event|history|ifstat|log|snmp} | {level
   {alert|critical|debugging|emergency|errors|informational|notice|warning} | size <trace_
   file_ize>}
   routing flags {all|arp|configuration|event|interface|route}
   stack-manager {flags {adjacency|all|asp|configuration|primary-election|route|system}
   | level {alert|critical|debugging|emergency|errors|informational|notice|warning}
```

Description

This command configures the traceoptions to monitor and log traffic flows.

Syntax

Parameter	Description
`chassis-manager flags`	Configures the chassis manager trace options: ■ **all**—Enables all chassis manager debug tracing. ■ **association**—Enables stack membership and association tracing. ■ **debug**—Enables generic chassis manager debug tracing. ■ **environment-monitoring**—Enables environment monitor debug tracing. ■ **fru**— Enables FRU reporting and management tracing. ■ **interface**—Enables interface debug tracing. ■ **interface-statistics**—Enables packet statistics on interface tracing. ■ **ipc**—Enables inter-process message exchange tracing. ■ **poe-configuration**—Enables power-over-ethernet configuration tracing. ■ **poe-statistics**—Enables power-over-ethernet statistics tracing. ■ **statistics-sync**—Enables statistics tracing. ■ **system-statistics**—Enables chassis system statistics tracing.
`igmp flags`	Configures the IGMP trace options: ■ **all**—Enables tracing on all IGMP modules. ■ **debug**—Enables internal state tracing for IGMP modules. ■ **leave**—Enables IGMP leave processing tracing. ■ **query**—Enables IGMP query processing tracing. ■ **report**—Enables IGMP report processing tracing.

Parameter	Description
`igmp-snooping flags`	Configures the IGMP snooping trace options: ■ **all**—Enables tracing on all igmp-snooping modules. ■ **config**—Enables igmp-snooping configuration tracing. ■ **errors**— Enables igmp-snooping error tracing. ■ **receive**—Enables igmp-snooping PDU received (RX) tracing. ■ **transmit**—Enables igmp-snooping PDU transmit (TX) tracing.
`interface-manager {flags|level}`	Configures the interface manager trace flags: ■ **all**—Enables all interface manager debug message tracing. ■ **configuration**—Enables configuration debug tracing. ■ **dhcp-client**—Enables dhcp client debug tracing. ■ **ethernet**—Enables ethernet interface debug tracing. ■ **infrastructure**—Enables infrastructure debug tracing. ■ **lacp**—Enables LACP debug tracing. ■ **loopback**—Enables loopback interface debug tracing. ■ **mgmt**—Enables management interface debug tracing. ■ **oam**—Enables OAM debug tracing. ■ **port-channel**—Enables port-channel debug tracing. ■ **port-mirroring**—Enables port mirroring debug tracing. ■ **system-information**—Enables system debug messages tracing. ■ **tunnel**—Enables tunnel interface debug tracing. ■ **vlan**—Enables vlan interface debug tracing. Configures the level for interface manager tracing: ■ **debug**—Debug messages ■ **error**—Error messages ■ **verbose**—Verbose debug messages
`layer2-forwarding {flags|level|size}`	Configures the layer2 forwarding trace flags: ■ **all**—Enables tracing on all switching modules. ■ **config**—Enables config module tracing. ■ **fdb**—Enables forwarding database module tracing. ■ **hsl**—Enables HSL module tracing. ■ **interface**—Enables interface module tracing. ■ **ipc**—Enables IPC tracing. ■ **learning**—Enables learning module tracing. ■ **nexthop**—Enables nexthop module tracing. ■ **port-loop**—Enables Port loop protect Protocol tracing. ■ **sysinfo**—Enables sysinfo module tracing. ■ **task**—Enables task tracing. ■ **timer**—Enables task timer tracing. ■ **tunneled-node**—Enables tunneled-node module tracing. ■ **vlan**—Enables vlan module tracing. ■ **vlan-assignment**—Enables VLAN assignment module tracing. ■ **vlan-port**—Enables VLAN port module tracing. Configures the layer2 forwarding tracing levels: ■ **debug**—Debug messages ■ **error**—Error messages ■ **informational**—Informational messages Configures the maximum size for layer2 forwarding trace file in MB.
`lldp flags`	Configures the LLDP trace options: ■ **all**—Enables tracing on all lldp modules. ■ **errors**—Enables lldp error tracing. ■ **receive**—Enables lldp PDU receive (RX) tracing. ■ **system-state**—Enables lldp system-state tracing. ■ **transmit**—Enables lldp PDU transmit (TX) tracing.

Parameter	Description
`mstp {flags|port}`	Configures the MSTP trace flags and trace port: ■ **all**—Enables tracing on all mstp modules ■ **config**—Enables mstp config tracing. ■ **debug**—Enables mstp debug tracing. ■ **port-information**—Enables mstp port information tracing. ■ **received-bpdu-al**—Enables mstp received bpdu tracing. ■ **role-selection**—Enables mstp role selection tracing. ■ **sent-bpdu-all**—Enables mstp sent bpdu tracing. ■ **state-machine-changes**—Enables mstp state machine change tracing. ■ **system**—Enables mstp system tracing. ■ **topology-change**—Enables mstp topology change tracing.
`ospf flags`	Configures the OSPF trace options: ■ **all**—Enables tracing for all ospf events. ■ **cnf**—Enables configuration events tracing. ■ **db**—Enables database operations tracing. ■ **dd**—Enables database description packets tracing. ■ **debug**—Enables internal debug tracing. ■ **dr-elect**—Enables designated router election tracing. ■ **flood**—Enables linkstate flooding tracing. ■ **hello**—Enables tracing for hello packets. ■ **lsa**—Enables link state advertisement packets tracing. ■ **lsr**—Enables link state request packets tracing. ■ **lsu**—Enables link state update packets tracing. ■ **msm**—Enables msm events tracing. ■ **pkt-all**—Enables tracing for all packets. ■ **spf**—Enables SPF operations tracing. ■ **state**—Enables interface, neighbor, area changes tracing.
`pim flags`	Configures PIM sparse mode trace options: ■ **adjacency**—Enables pim sparse mode adjacency tracing. ■ **all**—Enables tracing on all pim sparse mode modules. ■ **debug**—Enables internal state tracing for pim sparse mode modules. ■ **jp-asserts**—Enables pim sparse mode join-prune/assert tracing. ■ **register**—Enables pim sparse mode register tracing. ■ **route**—Enables pim sparse mode route tracing. ■ **state**—Enables pim sparse mode state tracing.

Parameter	Description
`rmon {flag-s|level|size}`	Configures the RMON trace flags: ■ **alarm**—Enables rmon alarm module debug tracing. ■ **all**—Enables rmon all module debug tracing. ■ **cli**—Enables rmon CLI module debug tracing. ■ **event**—Enables rmon event debug tracing. ■ **history**—Enables rmon history module debug tracing. ■ **ifstat**—Enables rmon interface statistics debug tracing. ■ **log**—Enables rmon log debug tracing. ■ **snmp**—Enables rmon SNMP module debug tracing. Configures the RMON tracing levels: ■ **alert**—Alert messages ■ **critical**—Critical messages ■ **debugging**—Debug messages ■ **emergency**—Emergency messages ■ **errors**—Error messages ■ **informational**—Informational messages ■ **notice**—Notification messages ■ **warning**—Warning messages Configures the maximum size for RMON trace file in MB.
`routing flags`	Configures the layer3 manager trace options: ■ **all**—Enables tracing on all layer3 manager events. ■ **arp**—Enables arp module tracing. ■ **configuration**—Enables layer3 configuration processing tracing. ■ **event**—Enables layer3 manager system events tracing. ■ **interface**—Enables layer3 manager interface events tracing. ■ **route**—Enables route table updates tracing.
`stack-manager {flag-s|level}`	Configures the stack manager trace flags: ■ **adjacency**—Enables stack-manager adjacency tracing. ■ **all**—Enables tracing for all stack-manager modules. ■ **asp**—Enables aruba stacking protocol tracing. ■ **configuration**—Enables tracing for configuration of stack-manager. ■ **primary-election**—Enables tracing for primary election. ■ **route**—Enables stack-manager route calculations tracing. ■ **system**—Enables tracing for stack-manager interaction with other components. ■ **webui**—Enables tracing for stack-manager interaction with WebUI. Configures the stack manager tracing level: ■ **alert**—Alert messages ■ **critical**—Critical messages ■ **debugging**—Debug messages ■ **emergency**—Emergency messages ■ **errors**—Error messages ■ **informational**—Informational messages ■ **notice**—Notification messages ■ **warning**—Warning messages

Example

The following command enables tracing on all IGMP modules:

```
(host) [mynode] (config) #traceoptions igmp flags all
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

tracepath

```
tracepath <global-address>
```

Description

Traces the path of an IPv6 host.

Syntax

Parameter	Description
`<global-address>`	The IPv6 global address of the host.

Usage Guidelines

Use this command to identify points of failure in your IPv6 network.

Example

The following command traces the path of the specified IPv6 host.

```
(host) [mynode] (config) #tracepath 2005:d81f:f9f0:1001::14
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

traceroute

```
traceroute <ipaddr>
   source
```

Description

Trace the route to the specified IP address.

Syntax

Parameter	Description
`<ipaddr>`	The destination IP address.
`source <ipaddr>`	Sets the source IP address through which packets are sent for tracing route.

Usage Guidelines

Use this command to identify points of failure in your network.

Example

The following command traces the route to the device identified by the IP address 10.1.2.3.

```
(host) [mynode] (config) #traceroute 10.1.2.3
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

tunnel-group

```
tunnel-group <tungrpname>
   mode {l2|l3)
   no
   preemptive-failover
   tunnel <tunnel-id>
```

Description

This command creates a tunnel-group to group a set of tunnels.

Syntax

Parameter	Description	Default
`mode {l2|l3}`	Set the type of tunnel-group.	l3
`no`	Negates any parameter configured.	—
`preemptive-failover`	When enabled, this option automatically redirects the traffic upon detecting an active tunnel with a higher precedence in the tunnel-group. When disabled, the traffic gets redirected to a higher precedence tunnel only when the tunnel carrying the traffic fails.	enabled
`tunnel <tunnel-id>`	Adds the specified tunnel ID to the tunnel group. The range is 1-16777215.	—

Usage Guidelines

Use this command to provide redundancy for L3 GRE tunnels. This feature enables automatic redirection of the user traffic to a standby tunnel when the primary tunnel goes down.

To enable L3 GRE tunnel group, you must:

- configure a tunnel-group to group a set of tunnels.
- enable tunnel keepalives on all the tunnel interfaces assigned to the tunnel-group, and
- configure the session ACL with the tunnel-group as the redirect destination.

To enable L2 GRE tunnel group, you must:

- configure the member tunnel and add them to the appropriate VLAN.
- enable tunnel keepalives on the tunnel interface.
- configure the tunnel-group and set the group type to L2, and
- add the member tunnel to the group

You can configure up to 32 tunnel-groups on a managed device with a maximum of 5 tunnels in each tunnel-group.

Example

The following set of commands create a tunnel-group with tunnel IDs 10 and 20 as the members:

```
(host) [mynode] (config) #tunnel-group tgroup1
(host) [mynode] (config-tunnel-group)# mode l3
```

```
(host) [mynode] (config-tunnel-group)# tunnel 10
(host) [mynode] (config-tunnel-group)# tunnel 20
(host) [mynode] (config-tunnel-group)#preemptive-failover
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

tunnel-loop-prevention

`tunnel-loop-prevention`

Description

This command prevents prevent forwarding loops between tunneled nodes on the managed device.

The tunneled node loop prevention function appears on the WebUI as the "Enable Wired Access Concentrator Loop Prevention" option. It is located on the **Configuration > Advanced Services > Wired Access > Wired Access Concentration Configuration** pane.

Syntax

No parameters.

Usage Guidelines

This command prevents forwarding loops between tunnels from the tunneled nodes on the managed device.

To allow a tunneled node-connected machine to communicate with another managed device that is a connected client on the same subnet, you must enable **broadcast-filter-arp**.

Example

The following command prevents tunneled node forwarding:

```
(host) [mynode] (config) #tunnel-loop-prevention
```

Related Commands

```
(host) [mynode] (config) #show tunneled-node config
(host) [mynode] (config) #show tunneled-node state
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master

tunnel-node-mtu

```
tunnel-node-mtu <mtu>
```

Description

This command configures the MTU of a tunneled node.

Syntax

Parameter	Description
`tnode-mtu`	Value of the MTU for the tunneled nodes Range: 1024 to 9216

Usage Guidelines

An Aruba managed device can operate as a Wi-Fi managed device, terminating GRE tunnels from tunneled node switches. As a Wi-Fi managed device, the managed device does not perform full Wi-Fi switching functions. Instead, it accepts traffic from ports designated as tunneled node ports, packages this traffic inside a GRE tunnel, and forwards the traffic back to a central managed device for processing.

Example

The following command configures the MTU of a managed device for tunneled nodes:

```
(host) [mynode] (config) #tunnel-node-mtu 1030
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

tunneled-node-address

```
tunneled-node-address <ipaddr>
```

Description

This command configures the IP address of a tunneled node server.

Syntax

Parameter	Description
`tunneled-node-address`	IP address of the managed device. This is the loopback or IP address of the managed device acting as a tunneled node managed device.

Usage Guidelines

A Aruba managed device can operate as a Wi-Fi managed device, terminating GRE tunnels from tunneled node switches. As a Wi-Fi managed device, the managed device does not perform full Wi-Fi switching functions. Instead, it accepts traffic from ports designated as tunneled node ports, packages this traffic inside a GRE tunnel, and forwards the traffic back to a central managed device for processing.

Example

The following command configures the address of a managed device for tunneled nodes:

```
(host)[mynode] (config) #tunneled-node-address 192.168.1.245
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

uap-blacklist

```
uap-blacklist
   add mac-address <address> description <description>
   del mac-address <address>
   modify mac-address <address> description <description>
   purge
```

Description

This command configures a Unified AP (UAP) blacklist database entry. You can add, delete, or modify AP MAC addresses and description to the blacklist database. If you enable the blacklist policy in the AP deploy profile, the policy is applied to the APs included in this list. You can also purge the UAP blacklist database from the device.

Syntax

Parameter	Description
`add mac-address <address> description <description>`	Adds the specified AP MAC address to the blacklist database.
`del mac-address <address>`	Deletes the specified AP MAC address from the blacklist database.
`modify mac-address <address> description <description>`	Modifies the details of an existing MAC address entry in the blacklist database.
`purge`	Purges the blacklist database.

Example

The following command adds the 11:11:11:11:11:11 MAC address entry to the UAP blacklist database:

```
(host) [mynode] #uap-blacklist add mac-address 11:11:11:11:11:11 description AP-203H
```

The following command modifies the description of the 11:11:11:11:11:11 MAC address entry from **AP-203H** to **AP-203R** in the UAP blacklist database:

```
(host) [mynode] #uap-blacklist add mac-address 11:11:11:11:11:11 description AP-203R
```

The following command deletes the 11:11:11:11:11:11 MAC address entry from the UAP blacklist database:

```
(host) [mynode] #uap-blacklist del mac-address 11:11:11:11:11:11
```

The following command purges the UAP blacklist database from the device:

```
(host) [mynode] #uap-blacklist purge
```

Related Commands

Command	Description
ap deploy-profile	The blacklist policy when enabled in the AP deploy profile, applies the policy to the UAP blacklist database entries.
show uap-blacklist	This command displays the UAP blacklist database entries.

Command History

Release	Modification
ArubaOS8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on master Mobility Master

ucc

```
ucc
   facetime {enable|no|priority video <0-63>}
   h323 {enable|no|priority voice <0-63>}
   ich {channel-utilization-threshold <50-95>|enable|no}
   jabber
      enable
      no
      priority {app-sharing <0-63>|video <0-63>|voice <0-63>}
      server-ip <server-ip>
   noe {enable|no|priority voice <0-63>}
   rtpa-config {enable|no|upstream}
   sccp {enable|no|priority voice <0-63>}
   session-idle-timeout {no|value <35-250>}
   sip
      enable
      midcall-req-timeout
      no
      priority {video <0-63>|voice <0-63>}
      rtcp-inactivity
   skype4b
      enable
      no
      priority {app-sharing <0-63>|video <0-63>|voice <0-63>}
      sdn {http|https}
   tables
   vocera {enable|no|priority voice <0-63>}
   wificalling
      dns-pattern <dns-pattern> service-provider <service-provider>
      enable
      no
      priority voice <0-62>
```

Description

This command configures the various UCC Application Layer Gateways (ALGs).

Syntax

Parameter	Description	Range	Default
`facetime`	Configures the Apple® FaceTime ALG. The ALG is enabled by default. The DSCP value for the video session is 34 by default. This parameter has the following sub-parameters: ■ **enable**– Enable the Apple Facetime ALG on the Mobility Master. ■ **no–** Remove or negate a parameter. ■ **priority**– The DSCP value for the video session.	priority video: 0-63	priority video: 34
`h323`	Configures the H.323 ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters: ■ **enable**– Enable the H.323 ALG on the Mobility Master. ■ **no–** Remove or negate a parameter. ■ **priority**– The DSCP value for the voice session.	priority voice: 0-63	priority voice: 46
`ich`	Configures the intelligent call handling. The setting is enabled by default. The Channel Utilization Threshold is 90 by default. This parameter has the following sub-parameters: ■ **channel-utilization-threshold**–The maximum limit for the channel utilization. ■ **enable**–Enable intelligent call handling on the Mobility Master. ■ **no**–Remove or negate a parameter.	channel-utilization-threshold: 50-95	channel-utilization-threshold: 90
`jabber`	Configures the Cisco® Jabber ALG. The ALG is enabled by default. Enter the Cisco Unified Communication Manager IM & Presence server IP. The DSCP values for the voice, video, and app-sharing sessions are 46, 34, and 34, respectively, by default. This parameter has the following sub-parameters: ■ **enable**–Enable Jabber ALG on the Mobility Master. ■ **no**–Remove or negate a parameter. ■ **priority**–The DSCP value for voice, video, and app-sharing sessions. ■ **server-ip**–Jabber server IP.	app-sharing, video, and voice: 0-63	app-sharing: 34 video: 34 voice: 46
`noe`	Configures the Alcatel-Lucent® New Office Environment (NOE) ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters: ■ **enable**– Enable the NOE ALG on the Mobility Master. ■ **no–** Remove or negate a parameter. ■ **priority**– The DSCP value for the voice session.	priority voice: 0-63	priority voice: 46

Parameter	Description	Range	Default
`rtpa-config`	Configures the real-time analysis of VoIP calls including upstream real-time analysis. The setting is enabled by default. This parameter has the following sub-parameters: ■ **enable**– Enable Real-Time Analysis of VoIP calls. ■ **no–** Remove or negate a parameter. ■ **upstream**–Enable upstream Real-Time Analysis of VoIP calls.	—	—
`sccp`	Configures the Cisco Skinny Client Control Protocol (SCCP) ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters: ■ **enable**– Enable the SCCP ALG on the Mobility Master. ■ **no–** Remove or negate a parameter. ■ **priority**– The DSCP value for the voice session.	priority voice: 0-63	priority voice: 46
`session-idle-timeout`	Configures the UCC session idle timeout. On configuring this parameter, if the voice session is idle for the configured period, UCM aborts the session on the managed device due to inactivity. The default value is 35. This parameter has the following sub-parameters: ■ **no–** Remove or negate a parameter. ■ **value**– Configure UCC session idle timeout in seconds.	value: 35-250	value: 35
`sip`	Configures the Session Initiation Protocol (SIP) ALG. The ALG is enabled by default. You can enable the **SIP Midcall request timeout** and **RTCP inactivity** settings. The DSCP values for the voice and video sessions are 46 and 34, respectively, by default. This parameter has the following sub-parameters: ■ **enable**–Enable SIP ALG on the Mobility Master. ■ **midcall-req-timeout**–Enable SIP Midcall request timeout. ■ **no**–Remove or negate a parameter. ■ **priority**–The DSCP value for voice and video sessions. ■ **rtcp-inactivity**–Enable Real-Time Control Protocol inactivity.	video and voice: 0-63	video: 34 voice: 46

Parameter	Description	Range	Default
`skype4b`	Configures the Microsoft® Lync/Skype for Business ALG. The ALG is enabled by default. You can set the Skype for Business SDN listen protocol over HTTP or HTTPS. Based on the SDN listen protocol configuration, Mobility Master accepts either HTTP or HTTPS messages from the Skype for Business SDN manager. The DSCP values for the voice, video, and app-sharing sessions are 46, 34, and 34, respectively, by default. This parameter has the following sub-parameters: ■ **enable**–Enable Skype for Business ALG on the Mobility Master. ■ **no**–Remove or negate a parameter. ■ **priority**–The DSCP value for voice, video, and app-sharing sessions. ■ **sdn**–Skype for Business SDN listen protocol. The default Skype for Business SDN API listen port is 32000.	app-sharing, video, and voice: 0-63	app-sharing: 34 video: 34 voice: 46
`tables`	Displays the UCC client MAC and IP address table. **NOTE:** This parameter is executable from the **enable** mode.	—	—
`vocera`	Configure the Vocera ALG. The ALG is enabled by default. The DSCP value for the voice session is 46 by default. This parameter has the following sub-parameters: ■ **enable**– Enable the Vocera ALG on the Mobility Master. ■ **no–** Remove or negate a parameter. ■ **priority**– The DSCP value for the voice session.	priority voice: 0-63	priority voice: 46

Parameter	Description	Range	Default
`wificalling`	Configures the Wi-Fi Calling. Wi-Fi Calling is enabled by default. The DSCP value for the voice session is 46 by default. ■ **dns-pattern**– Configure the DNS pattern for the carrier. A maximum of 10 DNS patterns can be configured. DNS patterns for known carriers are configured by default. Default built-in patterns are: - 3 HK - wlan.three.com.hk - ATT - epdg.epc.att.net - Rogers - epdg.epc.mnc720.mcc302.pub.3gppnetwork.org - SmarTone - epdg.epc.mnc006.mcc454.pub.3gppnetwork.org - Sprint - primgw.vowifi2.spcsdns.net - T-Mobile - ss.epdg.epc.mnc260.mcc310.pub.3gppnetwork.org - Verizon - wo.vzwwo.com If the ePDG FQDN of the carrier does not match with the default patterns, use this option to configure the DNS pattern for the carrier. **NOTE:** The DNS IP address that Mobility Master learns for Wi-Fi Calling age out automatically, if there was no DNS query or response matching that IP for more than seven days. **service-provider**– Add the service provider name for enhanced visibility. ■ **enable**– Enable the Wi-Fi calling ALG on the Mobility Master. ■ **no–** Remove or negate a parameter. ■ **priority**– The DSCP value for the voice session.	priority voice: 0-62	priority voice: 46

Usage Guidelines

The UCC ALGs must be configured from the **/mm** node hierarchy of Mobility Master. All the ALGs are enabled by default.

Examples

The following commands enables Wi-Fi calling on Mobility Master:

```
(host) [mm] (config) #ucc wificalling
(host) ^[mm] (WiFiCalling Configuration) #enable
```

The following command displays the UCC client MAC and IP address table. The **ucc tables** command should be executed from the **enable** mode:

```
(host) [mynode] #ucc tables

-------------------------------------------
UCC Client MAC table
--------------------
Client(MAC)         Client(IP)     Type     ALG
-----------         ----------     ----     ---
68:17:29:9f:b6:77   10.15.88.234   Client   Jabber/xmpp/SIP
-------------------------------------------
UCC Client IP table
-------------------
Client(MAC)         Client(IP)     Type     ALG
-----------         ----------     ----     ---
```

```
00:0b:86:8f:d6:b7  10.15.16.50   Server  SIP
00:0b:86:8f:d6:b7  10.15.16.30   Server  Jabber
68:17:29:9f:b6:77  10.15.88.234  Client  Jabber/xmpp/SIP
-------------------------------------------
```

Related Commands

Command	Description
show ucc call-info cdrs	This command displays the Call Detailed Records (CDR) statistics for UCC.
show ucc client-info	This command displays the UCC client status and CDR statistics.
show ucc dns-ip-learning	This command displays the carrier's evolved Packet Data Gateway (ePDG) IP address learned by the managed device. This command is specific for Wi-Fi calling clients.
show ucc facetime	This command displays the Apple Facetime ALG configuration.
show ucc h323	This command displays the H.323 ALG configuration.
show ucc ich	This command displays the Intelligent Call Handling configuration.
show ucc internal-state	This command displays the number of CDRs, flows, and voice clients created. This is a debug command.
show ucc jabber	This command displays the Cisco Jabber ALG configuration.
show ucc noe	This command displays the Alcatel-Lucent New Office Environment (NOE) ALG configuration.
show ucc rtpa-config	This command displays the real-time analysis configuration.
show ucc rtpa-report	This command displays the real-time analysis report.
show ucc sccp	This command displays the Cisco Skinny Client Control Protocol (SCCP) ALG configuration.
show ucc session-idle-timeout	This command displays the UCC session idle timeout configuration.
show ucc sip	This command displays the SIP ALG configuration.
show ucc skype4b	This command displays the Skype4B ALG configuration.
show ucc statistics	This command displays the UCC call statistics.
show ucc trace-buffer	This command displays the UCC call message trace buffer for Cisco Jabber, Cisco SCCP, SIP, and Microsoft Skype for Business ALGs.
show ucc vocera	This command displays the Vocera ALG configuration.
show ucc wificalling	This command displays the Wi-Fi calling configuration.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Master

upgrade internal

```
upgrade internal managed-devices
   copy configured-fileserver
      file <img-file> list <mac-list> partition {0|1}
      force-file <img-file-forced> list <mac-list> partition {0|1}
      force-version <img-version-forced> list <mac-list> partition {0|1}
      version <img-version> list <mac-list> partition {0|1}
   copy fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost> <username> <image-
   path>|tftp <imagehost> <image-path>}
      file <img-file> list <mac-list> partition {0|1}
      force-file <img-file-forced> list <mac-list> partition {0|1}
      force-version <img-version-forced> list <mac-list> partition {0|1}
      version <img-version> list <mac-list> partition {0|1}
   copy-reboot configured-fileserver
      file <img-file> list <mac-list> partition {0|1}
      force-file <img-file-forced> list <mac-list> partition {0|1}
      force-version <img-version-forced> list <mac-list> partition {0|1}
      version <img-version> list <mac-list> partition {0|1}
   copy-reboot fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost> <username>
   <image-path>|tftp <imagehost> <image-path>}
      file <img-file> list <mac-list> partition {0|1}
      force-file <img-file-forced> list <mac-list> partition {0|1}
      force-version <img-version-forced> list <mac-list> partition {0|1}
      version <img-version> list <mac-list> partition {0|1}
   reboot list <mac-list>
```

Description

This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device. This command is internal or hidden

Syntax

Parameter	Description
`copy configured-fileserver`	Copies the configured file server options like file, force-file, version, and force-version.
`copy fileserver`	Specify the file server details like, scp, ftp, tftp.
`copy-reboot configured-fileserver`	Reboots the managed devices after successful upgrade of the respective image using configured-file server options like file, force-file, version and force-version.
`copy-reboot fileserver`	Selects the type of supported servers like, ftp, scp, tftp and reboots the managed device post upgrade.
`reboot`	Reboots the managed device.
`ftp`	Used for mentioning FTP server.
`scp`	Used for mentioning SCP server.
`tftp`	Used for mentioning TFTP server.
`file`	Used for mentioning TFTP server.

Parameter	Description
`force-file`	Exact name of the image or image file.
`force-version`	Used to force the standard image name and is based on the platform type and version running on the managed device.
`version`	Image version and standard name based on platform type generated to load the image.

Example

The following command installs **ArubaOS_72xx_8.0.0.0-svcs-ctrl_55579** image from the configured file server on the network for a managed device with a MAC address **00:1a:1e:01:b0:b0** in partition 0:

```
(host) [mynode] #upgrade internal managed-devices copy configured-fileserver file ArubaOS_
72xx_8.0.0.0-svcs-ctrl_55579 list 00:1a:1e:01:b0:b0 partition 0
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

upgrade managed-devices

```
upgrade managed-devices
   copy configured-fileserver
      file <img-file> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-file <img-file-forced> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-version <img-version-forced> {all|path <node-path>|single <mac-addr>} partition
      {0|1}
      version <img-version> {all|path <node-path>|single <mac-addr>} partition {0|1}
   copy fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost> <username> <image-
   path>|tftp <imagehost> <image-path>}
      file <img-file> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-file <img-file-forced> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-version <img-version-forced> {all|path <node-path>|single <mac-addr>} partition
      {0|1}
      version <img-version> {all|path <node-path>|single <mac-addr>} partition {0|1}
   copy-reboot configured-fileserver
      file <img-file> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-file <img-file-forced> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-version <img-version-forced> {all|path <node-path>|single <mac-addr>} partition
      {0|1}
      version <img-version> {all|path <node-path>|single <mac-addr>} partition {0|1}
   copy-reboot fileserver {ftp <imagehost> <username> <image-path>|scp <imagehost> <username>
   <image-path>|tftp <imagehost> <image-path>}
      file <img-file> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-file <img-file-forced> {all|path <node-path>|single <mac-addr>} partition {0|1}
      force-version <img-version-forced> {all|path <node-path>|single <mac-addr>} partition
      {0|1}
      version <img-version> {all|path <node-path>|single <mac-addr>} partition {0|1}
   reboot
      all
      path <node-path>
      single <mac-addr>
```

Description

This command upgrades the managed devices with the respective options provided in the input, like using different protocol options as well as loading at different node levels and paths, and also can upgrade the single managed device based on the MAC address of the device.

Syntax

Parameter	Description
`copy configured-fileserver`	Copies the configured file server options like file, force-file, version, and force-version.
`copy fileserver`	Specify the file server details like, scp, ftp, tftp.
`copy-reboot configured-fileserver`	Reboots the managed devices after successful upgrade of the respective image using configured-file server options like file, force-file, version and force-version.
`copy-reboot fileserver`	Selects the type of supported servers like, ftp, scp, tftp and reboots the managed device post upgrade
`reboot`	Reboots the managed device.
`all`	Copies/ upgrades image to all managed devices under the respective node path

Parameter	Description
`path`	Copies/ upgrades image under specific node path and all the managed devices under this node path target node and make them as target list.
`single`	Copies/ upgrades image to the specific managed device based on MAC address under the respective node-path.
`ftp`	Used for mentioning FTP server.
`scp`	Used for mentioning SCP server.
`tftp`	Used for mentioning TFTP server.
`file`	Exact name of the image or image file.
`force-file`	Forcing the exact image name on the file-server by ignoring the existing file or image on the managed device..
`force-version`	Used to force the standard image name and is based on the platform type and version running on the managed device.
`version`	Image version and standard name based on platform type generated to load the image.

Example

The following command installs **ArubaOS_72xx_8.0.0.0-svcs-ctrl_55579** image from the configured file server on the network for all the managed devices under the **/md** node-hierarchy in partition 1:

```
(host) [mynode] #upgrade managed-devices copy configured-fileserver file ArubaOS_72xx_8.0.0.0-svcs-ctrl_55579 path /md partition 1
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.
ArubaOS 8.2.0.0	The IPv6 address of the image server was added to the **imagehost** parameter.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

upgrade-pkg

```
upgrade-pkg
   activate <packagename>
   copy
      ftp: <ftphost> <username> <filename> flash: <destfilename>
      scp: <scphost> <username> <filename> flash: <destfilename>
      tftp: <tftphost> flash: <destfilename>
   remove
```

Description

This command upgrades the service module on Mobility Master.

Syntax

Parameter	Description
`activate <packagename>`	Install and activate the service package.
`copy`	Download a service package through an FTP, SCP, or TFTP server.
`remove`	Delete a service package.

Example

This command upgrades the service module on Mobility Master.

```
(host) [mynode] #upgrade-pkg copy ftp: 192.0.2.22 anonymous ArubaOS_MM_8.0.0.0-svcs-ctrl_
appRF_55579 flash: ArubaOS_MM_8.0.0.0-svcs-ctrl_appRF_55579
(host) [mynode] #upgrade-pkg activate ArubaOS_MM_8.0.0.0-svcs-ctrl_appRF_55579
```

This command removes the service module on Mobility Master.

```
(host) [mynode] #upgrade-pkg remove ArubaOS_MM_8.0.0.0-svcs-ctrl_appRF_55579
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

upgrade-profile

```
upgrade-profile
   filepath
   no
   password
   protocol
   serverip
   username
   serverip
   serveraddr
```

Description

This command is used to configure the upgrade profile.

Syntax

Parameter	Description
`filepath`	File path to the location on the image server where the image file(s) reside.
`no`	Delete command
`password`	If you selected the FTP or SCP protocol for the Protocol type, enter the password that Mobility Master will use to connect to the image server.
`protocol`	Specify the protocol used to send the software upgrade from the image server to the managed device. ■ TFTP ■ FTP ■ SCP
`username <username>`	If you specified FTP or SCP for the **protocol** parameter field, enter the user name that Mobility Master uses to connect to the image server.
`serverip`	Specify the IPv4 address of the image server. This parameter is only used by managed devices running versions prior to ArubaOS 8.2 and accepts only IPv4 address. **NOTE:** For FTP or SCP protocol, specify the username and password.
`serveraddr`	Specify the IPv4 or IPv6 address of the image server. This parameter is only used by managed devices running ArubaOS 8.2. **NOTE:** For FTP or SCP protocol, specify the username and password.

Usage Guidelines

This command can be executed only from the **/md** node-hierarchy.

Example

The following command is used to upgrade managed devices:

```
(host) [md] #upgrade-profile
(host) [md] (Upgrade Profile) #serveraddr 2000:192:168:28::59
(host) [md] (Upgrade Profile) #username root
(host) [md] (Upgrade Profile) #password root123
(host) [md] (Upgrade Profile) #filepath Builds
```

```
(host) [md] (Upgrade Profile) #protocol scp
```

Command History

Release	Modification
ArubaOS 8.2.0.0	The **serveraddr** parameter was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

uplink

```
uplink
   cellular
    apn <APN-Profile-Pid> <APN-name>
    priority <prior>
   enable
   health-check ip {<fqdn>|<ip>}
   load-balance
    media-mode
    mode {hash-based|round-robbin|session-count|uplink utilization}
    threshold-limits
    jitter <avg_jitter>
    latency <avg_latency>
    session-count-percent <sess_percent>
   wired
    priority <prior>
    vlan <id> uplink-id {link1|link2|link3|link4}
     backup-link
     max-bandwidth <max_bw_utiln>
     no {backup-link|max-bandwidth|priority|speed|weight}
     priority <wired_vlan_priority>
     speed <uplink_speed>
     weight <wired_vlan_weight>
```

Description

Manage and configure the uplink network connection.

Syntax

Parameter	Description	Range

`cellular`
`apn <APN-Profile-Pid> <APN-Name>`
`priority <prior>`
	Set the cellular uplink configuration. This parameter has two sub-parameters:
	apn: The AP name of the cellular uplink.
	<APN-Profile-Pid>: Connection ID in modem dial string (e.g. "*99***x#", where "x" is the appropriate APN-profile-id number in dial-string)
	<APN-Name>: AP Name (e.g. internet). Contact your service provider if not known.
	priority: Set the priority of the cellular uplink. By default, the cellular uplink is a lower priority than the wired uplink; making the wired link the primary link and the cellular link the secondary or backup link. Configuring the cellular link with a higher priority than your wired link priority will set your cellular link as the primary link.
		priority: 1-255

`enable`	Enable the uplink manager.	—
`load-balance`	Load-balance configuration.	—
`media-mode`	Enable the **Media Mode** option to reevaluate the selected uplink for the session if it is identified as a media session. By default, all sessions use the load-balance mode specified by the **mode** parameter. When you select this option, any time a session is identified as a media session, the uplink is reassigned to the optimal uplink for media sessions, based upon a separate media load-balancing algorithm.	—

Parameter	Description	Range
`mode hash-based|round-robbin|session-count`	Choose one of the following load balancing modes: **Hash based**: Hash-based load balancing uses information from the packets being sent, (e.g. the source IP address, destination IP address, protocol and port numbers to determine how to load balance that traffic) **Round Robin**: Traffic is equally distributed to all the active uplinks **Session Count**: Traffic is balanced between the uplink ports based on the number of sessions managed by each link. The session-distribution is guided by **uplink load-balance threshold-limits session-count <>** percentage.	—
`threshold-limits`	Define latency and session thresholds	—
`jitter <avg_jitter>`	Define the maximum latency allowed for media sessions in media mode. The supported range is 1 - 400 milliseconds, and the default is 20 ms.	1-400 ms
`latency <avg_latency>`	Optimize media sessions by defining the maximum latency allowed for media sessions in media mode. The supported range is 1 - 400 milliseconds, and the default is 20 ms.	1-400 ms
`session-count <sess_count>`	Specify the maximum percentage of total sessions that can be managed by any active uplink. The default % is equally distributed among the number of wired uplink ports present. That is: ■ For 4 uplink ports– 25% ■ For 3 uplink ports– 33% ■ For 2 uplink ports– 50% ■ For 1 uplink port– 100%	—
`media-mode`	Enable load-balancing of media sessions using jitter, latency, pkt-loss of uplinks (disabled by default)	—
`mode`	Configure load-balancing mode. The valid values are hash-based, round-robin, and session-count.	—

Parameter	Description	Range
`threshold-limits`	Set threshold limits for load balancing. The valid values are jitter, latency, and session count percentage.	—
`health-check {ip {<fqdn>|<ip>}`	The **health-check** parameter is introduced to monitor the availability and quality of the connection to a master managed device with the specified FQDN or IP address.	—
`wired`	Define the wired uplink configuration.	—
`priority <prior>`	Define the default priority for wired uplinks. The default wired priority is 200.	1-255
`vlan <id> uplink-id {link1|link2|link3|link4}`	Define the VLAN ID of the uplink VLAN. A maximum of four wired VLANs can be defined.	1-4094
`priority <wired_vlan_priority>`	Set the priority of the wired VLAN uplink-id. Each uplink type has an associated priority; wired ports have the highest priority by default.	1-255
`weight <wired_vlan_weight>`	Set a weight for the uplink VLAN, which will be used in load balancing. The default value is 10.	1-100

Usage Guidelines

A managed device that supports multiple 3G cellular uplink ports in addition to their standard wired ports provides redundancy in the event of connection failure. However, at a time, only one cellular uplink is supported irrespective of many plugged-in. Also, **uplink enable** configuration is required to failover to cellular uplink (that is, active-standby operation). So, if a managed device's wired link cannot access the internet, the managed device can fail over to a secondary cellular link and continue routing traffic.

The uplink manager is disabled by default. Issue the **uplink enable** command to enable the uplink manager.

If **uplink load-balance** is enabled (active-active operation), and the device fails-over to cellular uplink because all wired uplink ports became unusable (unreachable or interface is down) then uplink load-balancing gets disabled automatically. This is because cellular uplink never participates in load-balancing of WAN traffic. Once any wired uplink port becomes usable again, cellular is disconnected and load-balancing get enabled again.

Both **uplink enable** and **uplink health-check** configuration are required for enabling **uplink load-balance**.

To view the health status of an uplink on a services or managed device, issue the command show uplink in the managed device CLI. For a managed device, the health status of its uplink connections are also displayed in the **Status** section of the **Dashboard > WAN** page of the managed device WebUI.

Related Commands

Command	Description
show uplink	Displays uplink configuration details.

Command History

Release	Modification
ArubaOS 8.1.0.0	The **load-balance** and **wired** parameters were added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

usb

```
usb reclassify <address> [<bus>]
```

Description

This command disconnects and reclassifies a USB device connected to a managed device.

Syntax

Parameter	Description
`reclassify`	Disconnect and reclassify a USB device.

Example

This command disconnects and reclassifies a USB device with an address of 18 connected to a managed device.

```
(host-md) #usb reclassify 18
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Eable mode on Mobility Master

user-role

```
user-role <name>
   access-list {eth|mac|session} <acl> [ap-group <group>] [position <number>]
   bw-contract
      app <appname> <bw-contract_name> {downstream|upstream}
      appcategory <appcategory-name> <bw-contract_name> {downstream|upstream}
      exclude {app|appcategory}
      web-cc-category <web-cc-category-name> <bw-contract_name> {downstream|upstream}
      web-cc-reputation {high-risk|low-risk|moderate-risk|suspicious|trustworthy} <bw-contract_
      name> {downstream|upstream}
      <bw-contract-name> [per-user|per-apgroup]{downstream|upstream}
   captive-portal {<STRING>|check-for-accounting}
   dialer <name>
   dpi
   max-sessions <number>
   no ...
   openflow-enable
   pool {l2tp|pptp} <name>
   qos-profile <profile>
   reauthentication-interval [<minutes>|<seconds>]
   registration-role
   sso <profile>
   stateful-kerberos <profile>
   stateful-ntlm <ntlm_profile_name>
   via <profile>
   vlan {VLAN ID|VLAN name}
   web-cc disable
   wispr <wispr_profile_name>
```

Description

This command configures a user role.

Syntax

Parameter	Description	Range	Default
`<name>`	Role name	—	—
`access-list`	Type of ACL to be applied: **eth:** Ethertype ACL, configured with the **ip access-list eth** command. **mac:** MAC ACL, configured with the **ip access-list mac** command. **session:** Session ACL, configured with the **ip access-list session** command.	—	—
`<acl>`	Name of the configured ACL.	–	–

Parameter	Description	Range	Default
`ap-group`	(Optional) AP group to which this ACL applies.	—	—
`position`	(Optional) Position of this ACL relative to other ACLs that you can configure for the user role. 1 is the top.	—	(last)
`bandwidth-contract`	Name of a bandwidth contract or rate limiting policy configured with the **aaa bandwidth-contract** command. The bandwidth contract must be applied to either downstream or upstream traffic.	—	—
`app`	Name of the application bandwidth contract configured for the user role. The bandwidth contract must be applied to either downstream or upstream traffic. **NOTE:** For a complete list of supported applications, issue the command **show dpi application all**.	–	–
`appcategory`	Name of the application category bandwidth contract configured for the user role. The bandwidth contract must be applied to either downstream or upstream traffic. **NOTE:** For a complete list of supported applications, issue the command **show dpi application category all**.	–	–

Parameter	Description	Range	Default
`web-cc-category|web-cc-reputation <cc-name> <bwc-name>`	Apply a bandwidth conract to the specified web content category or reputation level. Bandwidth contracts can be applied to user-defined web content categories created using the web-cc command. The five web content reputation levels are predefined in ArubaOS. **NOTE:** bandwidth contracts applied to a web content category or reputation will not be enforced unless web content classification is enabled using the **firewall web-content-classification** command.	Available reputation categories are: ■ high-risk ■ low-risk ■ moderate-risk ■ suspicious ■ trustworthy	–
`exclude app|appcategory`	Excludes an application or application category from being configured as a bandwidth contract.	–	–
`downstream`	Applies the bandwidth contract to traffic from the controller to the client.	—	—
`per-user`	Specifies that bandwidth contract is assigned on a per-user basis instead of a per-role basis. For example, if two users are active on the network and both are part of the same role with a 500 Kbps bandwidth contract, then each user is able to use up to 500 Kbps.	—	(per role)
`upstream`	Applies the bandwidth contract to traffic from the client to the controller.	—	—
`captive-portal <STRING>`	Name of the captive portal profile configured with the **aaa authentication captive-portal** command.	—	—

Parameter	Description	Range	Default
check-for-accounting	If disabled, RADIUS accounting is done for an authenticated users irrespective of the captive-portal profile in the role of an authenticated user. If enabled, accounting is not done as long as the user's role has a captive portal profile on it. Accounting will start when Auth/XML-Add/CoA changes the role of an authenticated user to a role which doesn't have captive portal profile.	–	enabled
dialer	If VPN is used as an access method, name of the VPN dialer configured with the **vpn-dialer** command. The user can login using captive portal and download the dialer. The dialer is a Windows application that configures the VPN client.	—	—
dpi	Role specific DPI configuration.	—	—
disable	Disable role specific DPI configuration.	–	–
max-sessions	Maximum number of datapath sessions per user in this role.	0-65535	65535
no	Negates any configured parameter.	—	—
openflow-enable	Enables SDN for the user role.	—	disabled

Parameter	Description	Range	Default
pool	If VPN is used as an access method, specifies the IP address pool from which the user's IP address is assigned: l2tp: When a user negotiates an L2TP or IPsec session, specifies an address pool configured with the **ip local pool** command. pptp: When a user negotiates a PPTP session, specifies an address pool configured with the **pptp ip local pool** command.	—	—
<name>	Name of the L2TP or PPTP pool to be applied.	—	—
qos-profile	Applies a QOS profile to the user role.	—	—
reauthentication-interval	Interval, in minutes or seconds, after which the client is required to reauthenticate.	■ 0-4096 in minutes ■ 0-245760 in seconds	0(disabled)
registration-role	If enabled, a user is forced to do MAC-based authentication every time the user connects to the network.	—	disabled
sso	Applies an SSO profile to the user role.	—	—
statefule-kerberos	Applies a stateful Kerberos profile to the user role.	—	—
stateful-ntlm	Apply stateful NTLM authentication to the specified user role		
via	Applies a VIA connection profile to the user role.	—	—

Parameter	Description	Range	Default
`vlan`	Identifies the VLAN ID or VLAN name to which the user role is mapped. This parameters works only when using Layer-2 authentication such as 802.1X or MAC address, ESSID, or encryption type role mapping because these authentications occur before an IP address is assigned. If a user authenticates using a Layer-3 mechanism such as VPN or captive portal this parameter has no effect. **NOTE:** VLAN IDs and VLAN names cannot be listed together.	—	—
`voip-profile`	Applies a VOIP profile to the user role.	—	—
`web-cc disable`	Disable web content classification for this user role. User role bandwidth contracts associated with web content classification categories and reputation types will not enforced unless web content classification is enabled using the **firewall web-content-classification** command.	—	—
`wispr`	Apply WISPr authentication to the specified user role.	—	—

Usage Guidelines

Every client in a user-centric network is associated with a user role. All wireless clients start in an initial role. From the initial role, clients can be placed into other user roles as they pass authentication.

Example

The following command configures a user role:

```
(host)[md](config) #user-role new-user
   dialer default-dialer
   pool pptp-pool-1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Requires the PEFNG license	Config mode on Mobility Master

valid-network-oui-profile

```
valid-network-oui-profile
   no
   oui <oui>
```

Description

This command allows you to add a new OUI to the managed device.

Syntax

Parameter	Description	Range	Default
`no`	Negates any configured parameter.	—	—
`oui <oui>`	The new OUI to be added. Use the aa:bb:cc format to input the new OUI.	—	—

Usage Guidelines

This command adds a new OUI to the managed device. The new OUI must be entered in a aa:bb:cc format.

Example

The following command adds a new OUI to the managed device.

```
(host) [mynode] (config) #valid-network-oui-profile
(host) [mynode] (Valid Equipment OUI profile) #
(host) [mynode] (Valid Equipment OUI profile) #oui 00:11:22
This should only be used when adding equipment with a new OUI.  Are you sure you
want to proceed? [y/n]: y
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master

vlan-bwcontract-explist

```
vlan-bwcontract-explist mac <mac>
```

Description

Use this command to add entries to or remove entries from the MAC exception list for bandwidth contracts on broadcast or multicast traffic.

Syntax

Parameter	Description
`<mac>`	MAC address of a protocol that should be added to or removed from the exception list for bandwidth contracts.

Usage Guidelines

Bandwidth contracts on a VLAN can limit broadcast and multicast traffic. ArubaOS includes an internal exception list to allow broadcast and multicast traffic using the VRRP, LACP, OSPF, PVST and STP protocols. To remove per-vlan bandwidth contract limits on an additional broadcast or multicast protocol, add the MAC address for that broadcast or multicast protocol to the Vlan Bandwidth Contracts MAC Exception List.

Example

The following command adds the MAC address for CDP and VTP to the list of protocols that are not limited by VLAN bandwidth contracts.

```
(host) [mynode] (config) #vlan-bwcontract-explist mac 01:00:0C:CC:CC:CC
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

vlan-name

```
vlan-name <name> [assignment {even|hash}]
```

Description

This command creates a named VLAN on the managed device and given an assignment type.

Syntax

Parameter	Description	Range
`<name>`	Name of the VLAN.	1–32 characters
`assignment`	Sets the assignment type. This determines how a VLAN assignment is handled by the managed device.	—
`even`	Sets the assignment type as even.The Even assignment type is based on an even distribution of VLAN pool assignments.	—
`hash`	Sets the assignment type as hash. The hash type means that the VLAN assignment is based on the station MAC address.	—

Usage Guidelines

Create a named VLAN so you can set up a VLAN pool. A VLAN pool consists of a set of VLAN IDs which are grouped together to efficiently manage multi-managed device networks from a single location.

VLAN pooling should *not* be used with static IP addresses.

The Even VLAN assignment type maintains a dynamic latest usage level of each VLAN ID. Therefore, as users age out, the number of available addresses increases. This leads to a more even distribution of addresses.

The Even type is only supported in tunnel and decrypt tunnel forwarding modes. It is not supported in split or bridge modes and it is not allowed for VLAN pools that are configured directly under a virtual AP. It can only be used under named VLANs. If a VLAN is given an Even assignment in bridge mode, a message displays indicating that the Hash assignment is automatically used instead to retrieve the VLAN ID.

L2 Mobility is not compatible with the existing implementation of the Even VLAN pool assignment type.

Example

The following command creates a VLAN named **mygroup** with the assignment type “even” on the managed device:

```
(host) [mynode] (config) #vlan-name mygroup assignment even
```

Related Commands

Command	Description
`show vlan`	Shows the VLAN.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

vlan

```
vlan <id> [<description>] |[<name> <vlan-ids>]|[range <range>]|[wired aaa-profile <profile>]
```

Description

This command creates a VLAN ID or a range of VLAN IDs on the managed device.

Syntax

Parameter	Description	Range	Default
`<id>`	Identification number for the VLAN.	2-4094	1
`<description>`	Description of a VLAN ID.	1-32 characters; cannot begin with a numeric character	VLAN000x, where x is the ID number.
`<name>`	(Optional) Identification name of the VLAN. The VLAN name was created using the **vlan-name** command.	1-32 characters; a name cannot begin with a numeric character	VLAN<id>
`<vlan-ids>`	(Optional) List of VLAN IDs that are associated with this VLAN. If two or more IDs are listed, the VLAN needs to specified first as a VLAN pool using the **vlan-name** command.	Existing VLAN IDs	1
`range <range>`	Create a range of multiple VLAN IDs by specifying the beginning and ending VLAN ID separated by a hyphen. For example, 55-58	2-4094	—
`remove <WORD>`	List a range of vlans to be removed and it is a comma and a '-' separated list of vlans.	—	—
`wired aaa-profile <profile>`	Assign an AAA profile to a VLAN to enable role-based access for wired clients connected to an untrusted VLAN or port on the managed device. This parameter applies to wired clients only. Note that this profile will only take effect if the VLAN or the port on the managed device is untrusted. If both the port and the VLAN are trusted, no AAA profile is assigned.	—	—

Usage Guidelines

Use the **`interface vlan`** command to configure the VLAN interface, including an IP address. Use the **`vlan-name`** command to create a named VLAN to set up a VLAN pool. A VLAN pool consists of a set of VLAN IDs which are grouped together to efficiently manage multi-managed device networks from a single location.

To enable role-based access for wired clients connected to an untrusted VLAN or port on the managed device, you must use the **wired aaa-profile** parameter to specify the wired AAA profile you would like to apply to that VLAN. If you do not specify a per-VLAN wired AAA profile, traffic from clients connected to an untrusted wired port or VLAN will use the global wired AAA profile, if configured.

Example

The following command creates VLAN ID 27 with the description **myvlan** on the managed device.

```
(host) [mynode] (config) #vlan 27 myvlan
```

The following command associates the VLAN IDs 5, 12 and 100 with VLAN guestvlan on the managed device.

```
vlan guestvlan 5,12,100
```

The following command creates VLAN IDs 200-300, 302, 303-400.

```
(host) [mynode] (config) #vlan range 200-300,302, 303-400
```

Related Commands

Command	Description
show vlan	This command shows a configured VLAN interface number, description and associated ports
aaa authentication wired	This command configures authentication for a client device that is directly connected to a port on the managed device.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

vpn-dialer

```
vpn-dialer <name>
   enable dnetclear|l2tp|pptp|securid_newpinmode|wirednowifi
   ike {authentication {pre-share <key>|rsa-sig}|encryption {3des|des}|
    group {1|2}|hash {md5|sha}|lifetime [<seconds>]}
   ipsec {encryption {esp-3des|esp-des}|hash {esp-md5-hmac|esp-sha-hmac}|
    lifetime [<seconds>]|pfs {group1|group2}}
   no {enable...|ipsec...|ppp...}
   ppp authentication {cache-securid|chap|mschap|mschapv2|pap}
```

Description

This command configures the VPN dialer.

Syntax

Parameter	Description	Range	Default
`<name>`	Name that identifies this VPN dialer configuration.	—	—
`enable`	Enables dialer operations:	—	—
`dnetclear`	Enables “split tunneling” functionality so that traffic destined for the internal network is tunneled while traffic for the Internet is not. This option is not recommended for security reasons.	—	disabled
`l2tp`	Allows the dialer to negotiate a Layer-2 Tunneling Protocol (L2TP)/IPsec tunnel with the managed device.	—	enabled
`pptp`	Allows the dialer to negotiate a Point-to-Point Tunneling Protocol (PPTP) with the managed device.	—	disabled
`securid_newpinmode`	Supports SecurID new and next pin mode.	—	disabled
`wirednowifi`	Allows the dialer to detect when a wired network connection is in use, and shuts down the wireless interface.	—	disabled
`ike`	Configures internet key exchange (IKE) protocol. This configuration must match the IKE policy configured with the **crypto isakmp policy** command on the managed device.	—	—
`authentication`	Specifies whether preshared keys or RSA signatures are used for IKE authentication.	pre-share | rsa-sig	pre-share
`encryption`	Specifies the IKE encryption protocol, either DES or 3DES.	3des | des	3des
`group`	Specifies the Diffie-Hellman group, either 1 or 2.	1 | 2	2

Parameter	Description	Range	Default
hash	Specifies the HASH algorithm, ether SHA or MD5.	md5 | sha	sha
lifetime	Specifies how long an IKE security association lasts, in seconds.	300-86400	28800 seconds
ipsec	Configures IPsec. This configuration must match the IPsec parameters configured with the **crypto dynamic-map** and **crypto ipsec** commands on the managed device.	—	—
encryption	Specifies the encryption type for IPsec, either DES or 3DES.	esp-3des | esp-des	esp-3des
hash	Specifies the hash algorithm used by IPsec, either MD5 or SHA.	esp-md5-hmac | esp-sha- hmac	esp-sha-hmac
lifetime	Specifies how long an IPsec security association lasts, in seconds.	300-86400	7200 seconds
pfs	Specifies the IPsec Perfect Forward Secrecy (PFS) mode, either group 1 or group 2.	group1 | group2	group2
no	Negates any configured parameter.	—	—
ppp authentication	Enables the protocols for PPP authentication. This list should match the L2TP or PPTP configuration configured with the **vpdn** command on the managed device.	—	—
cache-securid	The managed device caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.	—	disabled
chap	Use CHAP with PPP authentication.	—	enabled
mschap	Use MSCHAP with PPP authentication.	—	enabled
mschapv2	Use MSCHAPv2 with PPP authentication.	—	enabled
pap	Use PAP with PPP authentication.	—	enabled

Usage Guidelines

A VPN dialer is a Windows application that configures a Windows client for use with the VPN services in the managed device. When VPN is used as an access method, a user can login using captive portal and download a VPN dialer. You can customize a VPN dialer for a user role configured with the **user-role** command. After the user authenticates via captive portal, a link appears to allow download of the VPN dialer if a dialer is configured for the user role.

Example

The following command configures a VPN dialer:

```
(host)[node] (config) #vpn-dialer default-dialer
  ike authentication pre-share f00xYz123BcA
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master

vpdn group l2tp

```
vpdn group l2tp
   client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
   disable|enable
   l2tp tunnel hello <seconds>
   no ...
   ppp authentication {CACHE-SECURID|CHAP|EAP|MSCHAP|MSCHAPv2|PAP}
   ppp securid cache <minutes>
```

Description

This command configures an L2TP or IPsec VPN connection.

Syntax

Parameter	Description	Range	Default
`client configuration`	Configures parameters for the remote clients.	—	—
`dns`	Configures a primary and optional secondary DNS server.	—	—
`wins`	Configures a primary and optional secondary WINS server.	—	—
`disable|enable`	Disables or enables termination of L2TP clients.	—	enabled
`l2tp tunnel hello`	Configures L2TP tunneling hello timeout, in seconds.	10-1440	60 seconds
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the L2TP configuration configured with the **vpn-dialer** command on the managed device.	—	—
`CACHE-SECURID`	The managed device caches Secure ID tokens so that the user does not need to reauthenticate each time a network connection is lost.	—	—
`CHAP`	Use CHAP with PPP authentication.	—	—
`EAP`	Use EAP-TLS with PPP authentication. Specify this protocol for Windows IPsec VPN clients that use Common Access Card (CAC) Smart Cards that contain user information and digital certificates.	—	—
`MSCHAP`	Use MSCHAP with PPP authentication.	—	—
`MSCHAPv2`	Use MSCHAPv2 with PPP authentication. This is the default for L2TP	—	—
`PAP`		—	—
`ppp securid`	If CACHE-SECURID is configured for PPP authentication, this specifies the time, in minutes, that the token is cached.	15-10080	1440 minutes

Usage Guidelines

L2TP or IPsec relies on the PPP connection process to perform user authentication and protocol configuration. You specify the protocol used for PPP authentication and whether SecureID tokens are cached on the managed device. Client addresses are assigned from a pool configured with the **ip local pool** command.

Example

The following command configures virtual private dial-in networking:

```
(host) [mynode] (coinfig) #vpdn group l2tp
  ppp authentication PAP
  client configuration dns 10.1.1.2
  client configuration wins 10.1.1.2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

vpdn group pptp

```
vpdn group pptp
   client configuration {dns|wins} <ipaddr1> [<ipaddr2>]
   disable|enable
   no ...
   ppp authentication {MSCHAP|MSCHAPv2}
   pptp echo <seconds>
```

Description

This command configures a PPTP VPN connection.

Syntax

Parameter	Description	Range	Default
`client configuration`	Configures parameters for the remote clients.	—	—
`dns`	Configures a primary and optional secondary DNS server.	—	—
`wins`	Configures a primary and optional secondary WINS server.	—	—
`disable|enable`	Disables or enables termination of PPTP clients.	—	enabled
`no`	Negates any configured parameter.	—	—
`ppp authentication`	Enables the protocols for PPP authentication. This list should match the PPTP configuration configured with the **vpn-dialer** command on the managed device.	—	—
`MSCHAP`	Use MSCHAP with PPP authentication.	—	—
`MSCHAPv2`	Use MSCHAPv2 with PPP authentication. This is the default for L2TP	—	—
`pptp echo`	Time, in seconds, that the managed device waits for a PPTP echo response from the client before considering the client to be down. The client is disconnected if it does not respond within this interval.	10-300	60 seconds

Usage Guidelines

PPTP connections require user-level authentication through a PPP authentication protocol (MSHCAPv2 is the currently-supported method.) Client addresses are assigned from a pool configured with the **pptp** command.

Example

The following command configures virtual private dial-in networking:

```
vpdn group pptp
   ppp authentication MSCHAPv2
   client configuration dns 10.1.1.2
   client configuration wins 10.1.1.2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

vpnip

```
vpnip <vpncip>
   ipsec-custom-cert vpnc-mac-1-c <mac-addr> [vpnc-mac-2-c <mac-addr>][ca-cert <ca>|factory-
   ca-cert] [fqdn <local-fqdn>] [interface vlan <id>] [server-cert <sc>|factory-cert]| [suite-
   b gcm128 |gcm256]
   ipsec-factory-cert vpnc-mac-1 <mac-addr>
   peer-mac <peer-mac-1> ipsec <key> {[fqdn <local-fqdn>] [interface vlan <vpnvlanid>]}
```

Description

This command configures the certificate or PSK used by a managed device to create a site-to-site IPsec VPN tunnel to a controller configured as a VPN concentrator.

Syntax

Parameter	Description
`ipsec-custom-cert`	Custom Cert-based IPsec secure communication between a VPN concentrator and a managed device.
`vpnc-mac-1-c <mac-addr>`	Specify the first VPN concentrator's MAC address.
`vpnc-mac-2-c <mac-addr>`	Specify the second VPN concentrator's MAC address.
`ca-cert <ca> | factory-cert`	The specified CA certificate will be used validate the certificate presented by the VPN concentrator. Enter a name of a CA certificate, or choose **factory-cert** to use factory-installed CA Cert chain.
`fqdn <local-fqdn>`	The managed device's FQDN (max 64 bytes) used in IKE. This is optional for a dynamically addressed device.
`interface vlan <id>`	Specify the VLAN ID of a VLAN interface that initiates the IKE tunnel. If no interface is specified, the managed device uses the switch IP.
`server-cert <sc>|factory-cert]`	The managed device will use the specified server certificate for IPsec communication to a VPN concentrator.
`suite-b gcm128|gcm256`	Specify the GCM-128 or GCM-256 Suite B Algorithm
`ipsec-factory-cert`	Factory Cert-based IPsec secure communication between the VPN concentrator and the managed device.
`vpnc-mac-1-c <mac-addr>`	Specify VPN concentrator's MAC address.
`peer-mac <peer-mac-1>`	Specify Peer MAC address for PSK-based authentication.
`ipsec <key>`	Enable IPsec secure communication between the VPN concentrator and the managed device using the specified key.
`fqdn <local-fqdn>`	The managed device's FQDN (max 64 bytes) used in IKE. This is optional for a dynamically addressed device.
`interface vlan <vpnvlanid>`	Specify the VLAN ID of a VLAN interface that initiates the IKE tunnel. If no interface is specified, the managed device uses the switch IP.

Usage Guidelines

Use the **vpnip** command to configure a managed device to communicate with a VPN concentrator in a deployment where both Mobility Master and the VPN concentrator are located within the same DMZ.

When the managed device communicates with the VPN concentrator to set up an IPsec tunnel, any uplink VLAN tag defined via the **uplink wired** command will be sent with the vendor-id during IKE negotiation. This setting can uniquely bind the tunnel from a particular uplink on a managed device to a corresponding crypto map on VPN concentrator.

Example

```
[host](mynode)(config) # vpnip 192.0.0.2 ipsec-factory-cert vpn-mac-1 01:00:5E:00:00:01
```

Related Commands

Command	Description
uplink	Manage and configure the uplink network connection on a managed device.
vpnip	Defines Internet Key Exchange (IKE) parameters used by a VPN concentrator to create secure tunnels between that VPN concentrator and a managed device.

Command History

Release	Modification
ArubaOS 8.2.0.0	New sub-parameter, **vpnc-mac-2-c**, was added.
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master

vpn-peer

```
vpn-peer peer-mac <mac-addr>
   cert-auth {ca-cert <peer-ca> server-cert <peer-sc> [load-balance]}|{factory-cert [load-
   balance]}
   pre-share-key <peer-key> [load-balance]
```

Description

This command defines IKE parameters used by a VPN concentrator to create secure tunnels between that VPN concentrator and a managed device.

Syntax

Parameter	Description
`peer-mac <mac-addr>`	MAC address of the managed device. **NOTE:** If the peer device is an x86 server, then configure the MAC address of the management interface of the managed device. However, if the peer device is a hardware platform, you must provide the MAC address of the VLAN interface of the managed device.
`cert-auth`	Enable certificate authentication.
`ca-cert <peer-ca>`	<peer-ca> is a user-defined name of a trusted CA certificate installed on the VPN concentrator. This CA certificate will be used validate the certificate presented by the managed device.
`server-cert <peer-sc>`	<peer-SC> is a user-defined name of a server certificate installed on the VPN concentrator. The VPN concentrator will use the specified server certificate for IPsec communication to a managed device.
`load balance`	Enables uplink load-balancing on the primary and backup uplinks between a VPN concentrator and a managed device.
`factory-cert`	The factory-installed CA certificate on the VPN concentrator will be used validate the certificate presented by the managed device.
`pre-share-key <peer-key>`	Enable authentication using a PSK.
`load balance`	Enables uplink load-balancing on the primary and backup uplinks between a managed device and a VPN peer.

Usage Guidelines

Issue the **vpn-peer** command on controller configured as a VPN concentrator to define a VPN between that device and another managed device. When the other managed device communicates with the VPN concentrator to set up an IPsec tunnel, any uplink VLAN tag defined via the **uplink wired** command will be sent with the vendor-id during IKE negotiation. This setting can uniquely bind the tunnel from a particular uplink on a managed device to a corresponding crypto map on VPN concentrator.

Example

The following command configures a VPN from a managed device VPN concentrator to another managed device using the factory default certificate.

```
(host)[node] (config) #vpn-peer peer-mac 01:00:5E:00:00:FF factory-cert load-balance
```

Related Commands

Command	Description
vpnip	Configure the certificate or PSK used by a managed device to create a site-to-site IPsec VPN tunnel to a VPN concentrator.
vpn-peer	Defines IKE parameters used by a VPN concentrator to create secure tunnels between that VPN concentrator and a managed device.
uplink	Manage and configure the uplink network connection on a managed device.

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
Available on all platforms	Base operating system	Config mode on Mobility Master .

vrrp

```
ipv6 <id>
   advertise <interval>
   authentication <password>
   description <text>
   holdtime <secs>
   ipv6
   no...
   preempt
   priority <level>
   shutdown
   tracking {interface|master-up-time|vlan|vrrp-master-state}
   vlan <vlanid>
```

Description

This command configures the VRRP.

Syntax

Parameter	Description	Range	Default
`id`	Number that uniquely identifies the VRRP instance, also known as the VRID. This number should match the VRID on the other member of the redundant pair. For ease in administration, you should configure this with the same value as the VLAN ID. After you configure the VRID, the command platform enters VRRP mode. From here, you can access the remaining VRRP commands.	1-255	—
`ipv6`	Include this optional parameter to define a VRRP using an IPv6 address.	–	–
`advertise`	Specifies the time, in seconds, between successive VRRP advertisements sent by the current *master*. Best practices are to use the default value.	1-60 seconds	1 second (1s=1000ms)

Parameter	Description	Range	Default
`authentication`	Configure an optional password of up to eight characters to be used to authenticate VRRP peers in their advertisements. The password must be the same on both members of the redundant pair. The password is sent in plain-text and therefore should not be treated as a security measure. Rather, the purpose of the password is to guard against misconfigurations in the event that other VRRP devices exist on the same network. Note: This parameter is supported only for IPv4.	8 characters	—
`description`	Configure an optional text string to describe the VRRP instance.	1-80 characters	—
`holdtime <secs>`	The VRRP virtual router does not begin listening to advertisements until the holdtime expires. If your deployment includes a VRRP master with preemption disabled and an uplink switch is running RSTP, a higher value will prevent the VRRP master from regaining the master state after it reboots.	30-120 seconds.	45 seconds.

Parameter	Description	Range	Default
`ipv6 address`	Configure the virtual IPv6 address that will be owned by the elected VRRP *master*. Use the same IPv6 address on each member of the redundant pair. This IPv6 address will be redundant - it will be active on the VRRP master, and will become active on the VRRP backup in the event that the VRRP master fails. The IPv6 address must be unique; the IPv6 address cannot be the loopback address of the Mobility Master. Only IPv6 address formats are supported. Starting from ArubaOS 8.2.1.0, you can configure a unique local address as the VRRP IPv6 address on the Mobility Master and the managed devices.	—	—
`no`	Negates all configured VRRP parameters.	—	—
`preempt`	Preempt mode allows a managed device to take over the role of master if it detects a lower priority managed device currently acting as master. Best practices are to use the default value to avoid excessive interruption to users or “flapping” if a problematic managed device is cycling up and down.	—	disabled

Parameter	Description	Range	Default
`delay`	Delay value in seconds. Specifying a value enables the delay timer. The timer is triggered when the VRRP state moves out of backup or init state to become a master. This is applicable only if router pre-emption is enabled. When the timer is triggered, it delays the router for a specified period of time before taking over the master router. In the mean time, if there is an advertisement from another VRRP master (existing master), the router stops the timer and does not transition to master.	0-60 seconds	0
`priority`	Defines the priority level of the VRRP instance for the Mobility Master. This value is used in the election mechanism for the master. A higher number specifies a higher priority. The default priority setting is adequate for most networks.	100	1-255
`shutdown`	Administratively shutdown VRRP. When down, VRRP is not active, although the Mobility Master maintains the configuration information. To start the VRRP instance, use **no shutdown**.	—	enabled (VRRP is down)
`tracking`	Alter the virtual router priority value.	—	—

Parameter	Description	Range	Default
`interface {gigabitethernet <slot/module/port>} {sub <value>}`	Configures VRRP tracking based on Layer-2 interface state transitions. You can track a combined maximum of 16 VLAN and Layer-2 interfaces. ■ <slot/module/port> - Interface in <slot>/<module>/<port> format. ■ sub - Decreases the priority of the VRRP instance by the specified number. When the interface comes up again, the value is restored to the previous priority level. The combined priority and tracking vales cannot exceed 255. If the priority value exceeds 255, the Mobility Master displays an error message. Valid range is 0-255.	—	—
`master-up-time <duration> add <value>`	The VLAN tracking feature monitors how long the Mobility Master has been master for the VRRP instance. ■ duration - This value configures the number of minutes that must elapse before uptime tracking takes place. Valid range is 0-1440 minutes. ■ add - Instructs the Mobility Master to add the specified value to the existing priority level. The combined priority and tracking values cannot exceed 255. Valid range is 0-255. If the priority value exceeds 255, the Mobility Master displays an error message similar to the following - Error: Vrrp 30 priority + tracking value exceeds 255.		—

Parameter	Description	Range	Default
`vlan <vlanid> {sub <value>}`	Configures VRRP tracking based on VLAN state transitions. You can track a combined maximum of 16 VLAN and Layer-2 interfaces. sub - Decreases the priority of the VRRP instance by the specified amount. When the VLAN comes up again, the value is restored to the previous priority level. Valid range is 0-255. The combined priority and tracking values cannot exceed 255. If the priority value exceeds 255, the Mobility Master displays an error message.	—	—
`vrrp-master-state <vrid> add <value>`	Specifies the VRID to use for tracking the state of the VRRP Mobility Master. ■ add - Instructs the Mobility Master to add the specified value to the existing priority level. The combined priority and tracking values cannot exceed 255. Valid value is 0-255. If the priority value exceeds 255, the Mobility Master displays an error message similar to the following - Error: Vrrp 30 priority + tracking value exceeds 255	1-255	—
`vlan`	Specifies the VLAN ID of the VLAN on which VRRP will run.	1-4094	—

Usage Guidelines

Use this command to set parameters for VRRP on the Mobility Master. The default VRRP parameters can be left for most implementations.

You can use a combination of numbers, letters, and characters to create the authentication password and the VRRP description. To include a space in the password or description, enter quotation marks around the string. For example, to create the password Floor 1, enter “Floor 1” at the prompt.

To change the existing password or description, enter the command with a different string. The new password or description takes affect immediately.

To unconfigure the existing password or description, enter "" at the prompt. If you update the password on one managed device, you must update the password on the redundant member pair.

Interface Tracking

You can track multiple VRRP instances to prevent asymmetric routing and dynamically change the VRRP master to adapt to changes in the network. VRRP interface tracking can alter the priority of the VRRP instance based on the state of a particular VLAN or Layer-2 interface. The priority of the VRRP instance can increase or decrease based on the operational state of the specified interface. For example, interface transitions (up or down events) can trigger a recomputation of the VRRP priority, which can change the VRRP master depending on the resulting priority. You can track a combined maximum of 16 interfaces.

You must enable preempt mode to allow a managed device to take over the role of master if it detects a lower priority managed device currently acting as master

Example

The following command configures a priority of 105 for VRRP ID (VRID) 30:

```
(host) [mynode] (config) #vrrp 30
  priority 105
```

The following commands configure VLAN interface tracking and assumes the following:

- You have two managed device, a primary and a backup.
- The configuration highlights the parameters for interface tracking. You may have other parameters configured for VRRP.

Primary Configuration	Backup Configuration
vrrp 10 vlan 10 ip address 10.200.22.254 priority 105 preempt tracking vlan 20 sub 10 vrrp 20 vlan 20 ip address 10.200.22.254 preempt priority 105 tracking vlan 10 sub 10 vrrp 30 vlan 30 ip address 10.200.22.254 preempt priority 105 tracking vlan 20 sub 10	vrrp 10 vlan 10 ip address 10.200.22.254 priority 100 preempt tracking vlan 20 sub 10 vrrp 20 vlan 20 ip address 10.200.22.254 preempt priority 100 tracking vlan 10 sub 10 vrrp 30 vlan 30 ip address 10.200.22.254 preempt priority 100 tracking vlan 20 sub 10

If VLAN 20 goes down, VRRP 20 automatically fails over, VRRP 10 and VRRP 30 would drop their priority to 95, causing a failover to the backup Mobility Master. Once VLAN 20 comes back up, the Mobility Master restores the VRRP priority to 105 for all VRRP IDs and resumes the master VRRP role.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

webcc distributed

```
webcc distributed|centralized
```

Description

This command changes the WebCC operational mode from the default centralized mode to **distributed** mode for the managed device. The WebCC operational mode determines whether the managed device or Mobility Master contacts the cloud WebRoot server for URL lookup queries. In the default centralized mode, the Mobility Master contacts the cloud WebRoot server for URL lookup queries, whereas in **distributed** mode, the managed device contacts the cloud WebRoot server for URL lookup queries.

Syntax

Parameter	Description
`distributed`	Set the WebCC mode for the managed device to distributed mode.
`centralized`	Set the WebCC mode for the managed device to centralized mode. This is the default mode.

Usage Guidelines

The Web Content Classification (WebCC) license allows all web traffic to be classified and allows the managed device to apply firewall policies based on Web content category and reputation. The category and reputation data for each URL is obtained from an external WebRoot Server. The WebCC feature can operate in two distinct modes which control whether the Managed Device or Mobility Master performs the WebCC content lookup tasks. This command can be executed only from the **/md** subtree of the Mobility Master.

Centralized Mode

In the default **centralized** Mode, only Mobility Master downloads the URL entry database from the WebRoot Server. If a URL for Web traffic sent through the managed device does not appear in its datapath cache, the managed device sends a query request to Mobility Master. Mobility Master queries the WebRoot Server, adds the response to its database, then sends information about the URL back to the managed device.

WebCC license usage is calculated for each license pool, and the total count in each pool is sent to each managed device within that pool. If the WebCC licenses expire, or fewer WebCC licenses are available than AP licenses, then individual managed devices within that pool will no longer be able to send query requests to Mobility Master, and WebCC classification will be blocked.

If WebCC classification is blocked due to expired or insufficient licenses, individual managed devices continue to classify requested URLs currently available in the managed device datapath cache until the cache entries time out (usually over a period of 24 to 96 hours, depending upon the reputation level of the URL).

Distributed Mode

In **distributed** mode, each individual managed device downloads the complete URL entry database (approximately 22 MB) directly from the WebRoot Server. If a URL for Web traffic sent through the managed device does not appear in this database, the managed device sends a query to the WebRoot Server, then adds the response to its datapath cache.

WebCC license usage is calculated for each license pool, and the total count in each pool is sent to each managed device within that pool. If the WebCC licenses expire, or fewer WebCC licenses are available than AP

licenses, then individual managed devices within that pool will no longer be able to send new query requests to the WebRoot server. However, the WebCC feature continue to classify requested URLs that are already in the URL entry database on the managed device.

Example

```
(host) [md] (config) #webcc distributed
```

Command History

Release	Modification
ArubaOS 8.2.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	WebCC license	Config mode on Mobility Master.

web-cc

```
web-cc global-bandwidth-contract
   web-cc-category <category-name> downstream|upstream kbits|mbits <bandwidth>
   web-cc-reputation high-risk|low-risk|moderate-risk|suspicious|trustworthy
   downstream|upstream kbits|mbits <1-2000>
```

Description

This command defines global bandwidth contracts for HTTP traffic matching a predefined web content category or reputation type.

Syntax

Parameter	Description	Range	Default
`web-cc-category <category-name>`	Specify a web content category to apply a bandwidth contract to that category type. To see the full list of available web content categories, issue the command **show web-cc categories**.	—	—
`downstream|upstream`	Specify **downstream** to apply the bandwidth contract to downstream traffic from the Mobility Master. Specify **upstream** to apply the contract to upstream traffic to the Mobility Master.	—	—
`kbits|mbits`	Select kbits to define the contract bandwidth in kilobits/second. Select mbits to define the contract in megabits/second.	–	–
`bandwidth`	Define the contract value, If you are defining the bandwith value in kilobits/second, the supported range is 256-2,000,000 kbits. If you are defining the bandwidth value in megabits/second, the supported range is 1-2000 mbits.	256-2,000,000 kbits 1-2000 mbits	—
`web-cc-reputation high-risk|low-risk|moderate-risk|suspicious|trustworthy`	Define a bandwidth contract for traffic associated with one of five predefined reputation types. Session ACLs can be applied to these risk categories using the ip access-list session command.	–	–

Usage Guidelines

The web content classification feature classifies all (HTTP) web traffic on the network. ArubaOS uses the Webroot® classification categories and risk reputation levels, URL database and URL cloud look-up service to classify the web traffic. You can create firewall policies and bandwidth contracts based upon these web traffic classification and reputation types.

Example

The following example creates a 100 megabit/second bandwidth contract for a category called **music**.

```
(host) [/md] (config) #web-cc global-bandwidth-contract web-cc-category music downstream mbits
100
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	WebCC license	Config mode on Mobility Master.

web-proxy server

```
web-proxy server <name>
   port
```

Description

This command configures the web-proxy server related information.

Syntax

Parameter	Description	Range	Default
`<name>`	Specifies the proxy server name / IP address.	—	—
`port`	Specifies the proxy server port.	—	—

Usage Guidelines

When the Mobility Master needs to access data on the cloud or the internet, and if the internet bound traffic needs to pass through a proxy, execute the **web-proxy server** command. Once the command is executed the Mobility Master routes web (HTTP/HTTPS) traffic through the proxy server.

Example

The following command configures the web-proxy server related information:

```
(host) [mynode] (config) #web-proxy server arubaproxy.com port 8080
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

web-server profile

```
web-server profile
   absolute-session-timeout <30-3600>
   bypass-cp-landing-page
   captive-portal-cert <name>
   ciphers {high|low|medium}
   exclude-http-security-headers
   idp-cert <idp-cert>
   mgmt-auth [certificate] [username/password]
   no ...
   session-timeout <session-timeout>
   ssl-protocol [tlsv1 | tlsv1.1 | tlsv1.2]
   switch-cert <name>
   via-client-cert-port <via-client-cert-port>
   web-https-port-443
   web-max-clients <web-max-clients>
```

Description

This command configures the Mobility Master's web server.

Syntax

Parameter	Description	Range	Default
`absolute-session-timeout <30-3600>`	Specifies the absolute time after which the WebUI session times out post a successful authentication.	30-3600 seconds	0 (disabled)
`bypass-cp-landing-page`	If disabled, the Mobility Master uses the new redirection scheme also known as the landing page by default including the meta tag. This can reduce the CPU load on the Mobility Master. The Mobility Master falls back to the old redirection scheme if this parameter is enabled.	—	disabled
`captive-portal-cert`	Specifies the name of the server certificate associated with captive portal. Use the **show crypto-local pki ServerCert** command to see the server certificates installed in the Mobility Master.	—	default

Parameter	Description	Range	Default
`ciphers`	Configures the strength of the cipher suite: ■ **high**: encryption keys larger than 128 bits ■ **low**: 56 or 64 bit encryption keys ■ **medium**: 128 bit encryption keys **NOTE:** This command is not available in FIPS software images because ciphers are pre-configured only to acceptable values.	high, low, medium	high
`exclude-http-security-headers`	Excludes security headers from HTTP response.	—	—
`idp-cert`	Specifies the IDP certificate name configured in the Mobility Master.	—	—
`mgmt-auth`	Specifies the authentication method for the management user; you can choose to use either username or password or certificates, or both username or password and certificates.	username/ password, certificate	username/ password
`no`	Negates any configured parameter.	—	—
`session-timeout <session-timeout>`	Specifies the time of inactivity after which the WebUI session times out and requires login for continued access.	30-3600 seconds	900 seconds
`ssl-protocol`	Specifies the SSL or TLS protocol version used for securing communication with the web server: ■ TLS v1 ■ TLS v1.1 ■ TLS v1.2	—	tlsv1 tlsv1.1 tlsv1.2

Parameter	Description	Range	Default
`switch-cert`	Specifies the name of the server certificate associated with WebUI access. Use the **show crypto-local pki ServerCert** command to see the server certificates installed in the Mobility Master.	—	default
`via-client-cert-port <via-client-cert-port>`	Configures a port for VIA client certificate-based authentication.	—	—
`web-https-port-443`	Enables WebUI access on the HTTPS port (443). When you connect to the WebUI using https (tcp port 443), the Mobility Master continues using port 443 and no longer redirects to port 4343.	—	—
`web-max-clients <web-max-client>`	Configures the web server's maximum number of supported concurrent clients.	25-320	75

Usage Guidelines

There is a default server certificate installed in the Mobility Master, However this certificate does not guarantee security in production networks. Best practices are to replace the default certificate with a custom certificate issued for your site by a trusted CA. See the *ArubaOS User Guide* for more information about how to generate a CSR to submit to a CA and how to import the signed certificate received from the CA into the Mobility Master. After importing the signed certificate into the Mobility Master, use the **web-server profile** command to specify the certificate for captive portal or WebUI access. If you need to specify a different certificate for captive portal or WebUI access, use the **no** command to revert back to the default certificate before you specify the new certificate (see the Example section).

You can use client certificates to authenticate management users. If you specify certificate authentication, you need to configure certificate authentication for the management user with the **mgmt-user webui-cacert** command.

Example

The following commands configure WebUI access with client certificates only, and specify the server certificate for the Mobility Master:

```
(host) [/md] (config) #web-server profile
(host) [/md] (Web Server Configuration) #mgmt-auth certificate
(host) [/md] (Web Server Configuration) #switch-cert ServerCert1
(host) (Web Server Configuration) #!
(host) [/md] (config) #mgmt-user webui-cacert test_string serial 1111 admin root
```

To specify a different server certificate, use the **no** command to revert back to the default certificate *before* you specify the new certificate:

```
(host) [/md] (config) #web-server profile
(host) [/md] (Web Server Configuration) #mgmt-auth certificate
```

```
(host) [/md] (Web Server Configuration) #switch-cert ServerCert1
(host) [/md] (Web Server Configuration) #no switch-cert
(host) [/md] (Web Server Configuration) #switch-cert ServerCert2
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	The **web-server ciphers** and **web-server ssl-protocol** commands require the PEFNG license	Config mode on Mobility Master

websocket clearpass

```
websocket clearpass
   enable
   no
   primary host <host> port <1-65535> username <username> passwd <passwd>
   secondary host <host> port <1-65535> username <username> passwd <passwd>
```

Description

This command configures the ClearPass WebSocket profile. This command configures the primary and secondary ClearPass Insight server.

Syntax

Parameter	Description	Range	Default
`enable`	Enable ClearPass WebSocket interface.	—	—
`no`	Remove or negate a parameter.	—	—
`primary`	Configure the primary ClearPass Insight server. This parameter has the following sub-parameters: ■ **host**–The primary ClearPass Insight server IP address. ■ **port**–The port number of the ClearPass Insight server. ■ **username**– The name of the user who can perform the action on the server. ■ **passwd**– The password of the user.	port: 1-65535 username: 1-255 bytes password: 6-100 bytes	port: 443
`secondary`	Configure the secondary ClearPass Insight server. This parameter has the following sub-parameters: ■ **host**–The primary ClearPass Insight server IP address. ■ **port**–The port number of the ClearPass Insight server. ■ **username**– The name of the user who can perform the action on the server. ■ **passwd**– The password of the user.	port: 1-65535 username: 1-255 bytes password: 6-100 bytes	port: 443

Example

The following commands configures the ClearPass WebSocket interface and the primary and secondary ClearPass Insight server:

```
(host) [mynode] (config) #websocket clearpass
(host) [mynode] (ClearPass WebSocket Profile) #primary host secuirty67.acmecompany.com port
443 username admin passwd changeme
(host) [mynode] (ClearPass WebSocket Profile) #secondary host 10.17.5.210 port 443 username
aosadmin passwd changeme
(host) [mynode] (ClearPass WebSocket Profile) #enable
(host) [mynode] (ClearPass WebSocket Profile) #write memory

Saving Configuration...
Partial configuration for (root) /:
-----------------------------------
Contents of : /flash/config/partial/143/p=.cfg
websocket clearpass
```

```
enable
primary host "secuirty67.acmecompany.com" port 443 username "admin" passwd "changeme"
secondary host "10.17.5.210" port 443 username "aosadmin" passwd "changeme"
!
Partial configuration for /mynode:
-----------------------------------
Contents of : /flash/config/partial/143/p=mynode.cfg
websocket clearpass
enable
primary host "secuirty67.acmecompany.com" port 443 username "admin" passwd "changeme"
secondary host "10.17.5.210" port 443 username "aosadmin" passwd "changeme"
!
Configuration Saved.
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db cpsec add

```
whitelist-db cpsec add mac-address <name>
    ap-group <ap_group>
    ap-name <ap_name>
    description <description>
```

Description

Add an AP entry to the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <name>`	MAC address of the AP you want to enter into the campus AP whitelist database.
`ap-group <ap_group>`	(Optional) Name of the AP group. **NOTE:** If the AP group is not entered, a campus AP boots with "default" as AP group.
`ap-name <ap_name>`	(Optional) Name of the AP. **NOTE:** If the AP name is not entered, a campus AP boots with its MAC address as AP name.
`description <description>`	(Optional) Brief description of the AP. If the description includes spaces, enclose the description in quotation marks.

Usage Guidelines

You can manually add entries to the campus AP whitelist to grant valid APs secure access to the network.

Example

The following command creates a new campus AP whitelist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host) #whitelist-db cpsec add mac-address 00:16:CF:AF:3E:E1
   ap-group default
   ap-name AP-225
   description "AP-225 in lobby"
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

whitelist-db cpsec delete

```
whitelist-db cpsec delete mac-address <mac-address>
```

Description

Remove an individual AP entry to the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to remove from the campus AP whitelist.

Usage Guidelines

Use this command to remove an individual whitelist entries for an AP that has been either removed from the network, or is no longer a candidate for automatic certificate provisioning. If the AP whose entry you deleted is still connected to the network and the control plane security feature is configured to send certificates to all APs (or a range of addresses that include that AP), then the managed device will send the AP another certificate, and the AP will reappear in the campus whitelist. To permanently revoke a certificate from an invalid or suspected rogue AP, use the command whitelist-db cpsec revoke.

Example

The following command removes an AP with the MAC address 10:14:CA:AF:3E:E1 from the campus AP whitelist.:

```
(host) [mynode] (config) #whitelist-db cpsec delete mac-address 10:14:CA:AF:3E:E1
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db cpsec-local-switch-list

```
whitelist-db cpsec-local-switch-list
   del mac-address <mac-address>
   purge
```

Description

Delete a managed device from the local switch whitelist.

Syntax

Parameter	Description
`del mac-address <mac-address>`	Remove a single managed device from the local switch whitelist.
`purge`	Clear all entries from the local switch whitelist

Usage Guidelines

If your deployment includes both Mobility Master and managed devices, then the campus AP whitelist on each managed device contains an entry for every AP on the network, regardless of the managed device to which it is connected. Mobility Master also maintains a whitelist of managed devices with APs using control plane security. When you change a campus AP whitelist on any managed device, that managed device contacts Mobility Master to check the local switch whitelist, then contacts every other managed device on the local switch whitelist to notify it of the change.

If you ever remove a managed device from the network, you must also remove the managed device from the local switch whitelist. If the local switch whitelist contains entries for managed devices no longer on the network, then a campus AP whitelist entry can be marked for deletion but will not be physically deleted, as the managed device will be waiting for an acknowledgement from another managed device no longer on the network. Any unused managed device entries in the local switch whitelist can significantly increase network traffic and reduce managed device memory resources.

Example

The following command removes a managed device from the local switch whitelist:

```
(host) (config) #whitelist-db cpsec-local-switch-list del mac-address 00:1E:33:CA:D2:51
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec-local-switch-list	Show the local switch whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db cpsec-master-switch-list

```
whitelist-db cpsec-master-switch-list
   del mac-address <mac-address>
   purge
```

Description

Delete a Mobility Master from the master switch whitelist.

Syntax

Parameter	Description
`del mac-address <mac-address>`	Remove a single Mobility Master from the master switch whitelist.
`purge`	Clear all entries from the master switch whitelist

Usage Guidelines

Each managed device using the control plane security feature has a master switch whitelist which contains the IP and MAC addresses of its Mobility Master. If your network has a redundant Mobility Master, then this whitelist will contain more than one entry.

The master switch whitelist rarely needs to be purged. Although you can delete an entry from the master switch whitelist, you should do so only if you have removed a master switch from the network. Deleting a valid Mobility Master from the master switch whitelist can cause errors in your network.

Example

The following command removes a Mobility Master from the master switch whitelist

```
(host) [mynode] (config) #whitelist-db cpsec-master-switch-list del mac-address
00:1E:33:CA:D2:51
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec-master-switch-list	Show the master switch whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db cpsec modify

```
whitelist-db cpsec modify mac-address <name>
   ap-group <ap_group>
   ap-name <ap_name>
   cert-type {factory-cert|switch-cert}
   description <description>
   mode {disable|enable}
   revoke-text <revoke-text>
   state {approved-ready-for-cert|certified-factory-cert}
```

Description

Modify an existing entry in the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <name>`	MAC address of an AP in the campus AP whitelist database.
`ap-group <ap_group>`	(Optional) Name of the AP group to which an AP is assigned. **NOTE:** If AP group is not entered, a campus AP boots with "default" as the AP group.
`ap-name <ap_name>`	(Optional) Name of an AP. **NOTE:** If AP name is not entered, a campus AP boots with its MAC address as the AP name.
`cert-type {factory-cert|switch-cert}`	(Optional) Type of certificate used by an AP. ■ **factory-cert**: AP uses a factory-installed certificate. ■ **switch-cert**: AP uses a controller-signed certificate.
`description <description>`	(Optional) Brief description of an AP. If the description includes spaces, enclose the description in quotation marks.
`mode {disable|enable}`	(Optional) Mode of an AP. ■ **disable**: Disables an AP in the campus AP whitelist. A disabled AP cannot contact a managed device over a secure connection. ■ **enable**: Enables a disabled AP in the campus AP whitelist.
`revoke-text <revoke-text>`	(Optional) Brief description why an AP was revoked.
`state {approved-ready-for-cert|certified-factory-cert}`	(Optional) State of an AP. ■ **approved-ready-for-cert**: AP is approved and is ready to receive a certificate. ■ **certified-factory-cert**: AP is certified and has a factory-installed certificate.

Example

The following command changes the AP group, AP name, certificate type, description, mode, revoke text, and state of an AP with MAC address 00:1E:37:CB:D4:52:

```
(host)[node] #whitelist-db cpsec modify mac-address 00:1E:37:CB:D4:52
          ap-group default
          ap-name ap-225
          cert-type factory-cert
          description "AP-225 in lobby"
```

```
mode disable
revoke-text "Maintenance"
state approved-ready-for-cert
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db cpsec purge

```
whitelist-db cpsec purge
```

Description

Clear the campus AP whitelist.

Syntax

No parameters.

Usage Guidelines

Use this command to clear all entries in the entire campus AP whitelist. If your network includes both Mobility Master and managed devices, then each campus AP whitelist is synchronized across all managed devices. If you purge the entire campus AP whitelist on one managed device, that action will clear the campus AP whitelist on every managed device in the network. To delete an individual entry in the campus AP whitelist, use the command whitelist-db cpsec delete.

Example

The following command remove all APs from the campus AP whitelist:

```
(host)[node] (config) #whitelist-db cpsec purge
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db cpsec revoke

```
whitelist-db cpsec revoke mac-address <mac-address> revoke-text <revoke-text>
```

Description

Revoke a certificate from an AP in the campus AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to remove from the cpsec whitelist database.
`revoke-text <revoke-text>`	A brief description why the AP's certificate was revoked, up to 64 alphanumeric characters. If this comment includes spaces, you must enclose the comment in quotation marks.

Usage Guidelines

Use this command to revoke a certificate from a invalid or suspected rogue AP.

Example

The following command revokes a certificate from an AP. This command does not delete a whitelist entry for a revoked AP, but marks its entry with the revoked state.

```
(host)[node] (config) #whitelist-db cpsec revoke mac-address 00:1E:37:CA:D4:51
   revoke-text "revoking cert from a rogue AP."
```

Related Commands

Command	Description	Mode
show whitelist-db cpsec	Show the campus AP whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap add

```
whitelist-db rap add mac-addr <mac-address>
   ap-group <ap-group>
   ap-name <ap-name>
   description <description>
   full-name <full-name>
   mode enable|disable
   remote-ip <ip-addr>
```

Description

Add an AP entry to the remote AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to enter into the remote AP whitelist database.
`ap-group <ap-group>`	AP group of the remote AP.
`ap-name <ap-name>`	Name of the Remote AP.
`description <description>`	Description of the remote AP. If the description includes spaces, it must be enclosed within quotation marks.
`full-name <full-name>`	Name of the client using the remote AP.
`remote-ip <ip-addr>`	IP address used to assign a static inner IP address for the remote AP.

Usage Guidelines

You can manually add entries to the remote AP whitelist to grant valid remote APs secure access to the network.

Example

The following command creates a new remote AP whitelist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host)[node](config) #whitelist-db rap add mac-address 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description	Mode
show whitelist-db rap-master-switch-list	Display the list of Mobility Masters with remote APs managed using the remote AP whitelist	Enable or Config mode
show whitelist-db rap-local-switch-list	Display the list of managed devices with remote APs managed using the remote AP whitelist	Enable or Config mode
show whitelist-db rap	View detailed information for the remote AP whitelist database.	Enable or Config mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap del

```
whitelist-db rap del mac-addr <mac-address>
```

Description

Remove an AP entry from the remote AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to remove from the remote AP whitelist database.

Usage Guidelines

You can manually remove entries from the remote AP whitelist to revoke a remote AP's secure access to the network. If you want to temporarily revoke an AP's access without removing the entry from the whitelist, use the command whitelist-db rap revoke.

Example

The following command revokes and deletes a remote AP whitelist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host)[node] (config) #whitelist-db rap del mac-address 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description
whitelist-db rap add	Add an entry into the remote AP whitelist.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap modify

```
whitelist-db rap modify mac-addr <mac-address>
   ap-group <ap-group>
   ap-name <ap-name>
   description <description>
   full-name <full-name>
   mode enable|disable
   remote-ip <ip-addr>
```

Description

Remove an AP entry from the remote AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the remote AP whose whitelist database entry you want to modify.
`ap-group <ap-group>`	AP group of the remote AP.
`ap-name <ap-name>`	Name of the Remote AP.
`description <description>`	Description of the remote AP. If the description includes spaces, it must be enclosed within quotation marks.
`full-name <full-name>`	Name of the client using the remote AP.
`mode enable|disable`	Enable or disable the remote AP without deleting it from the database.
`remote-ip <ip-addr>`	IP address used to assign a static inner IP address for the remote AP.

Usage Guidelines

You can manually remove entries from the remote AP whitelist to revoke a remote AP's secure access to the network.

Example

The following command modifies a remote AP whitelist entry for an AP with the MAC address 00:16:CF:AF:3E:E1:

```
(host)[node] (config) #whitelist-db rap modify mac-address 00:16:CF:AF:3E:E1
   description "AP moved to second floor"
```

Related Commands

Command	Description
whitelist-db rap add	Add an entry into the remote AP whitelist.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap purge

```
whitelist-db rap purge
```

Description

Clear the remote AP whitelist.

Syntax

No parameters.

Usage Guidelines

Use this command to clear all entries in the entire remote AP whitelist. If your network includes both Mobility Master and managed devices, then each remote AP whitelist is synchronized across all managed devices. If you purge the entire remote AP whitelist on one managed device, that action will clear the remote AP whitelist on every managed device in the network. To delete an individual entry in the remote AP whitelist, use the command whitelist-db rap del.

Example

The following command removes all APs from the remote AP whitelist:

```
(host)[node] (config) #whitelist-db rap purge
```

Related Commands

Command	Description	Mode
show whitelist-db rap	Show the remote AP whitelist for the control plane feature.	Enable mode

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap revoke

```
whitelist-db rap revoke mac-address <mac-address> revoke-comment <comment>
```

Description

Revoke a certificate from an AP in the remote AP whitelist.

Syntax

Parameter	Description
`mac-address <mac-address>`	MAC address of the AP you want to remove from the remote AP whitelist database.
`revoke-comment <comment>`	A brief description why the AP's certificate was revoked, up to 64 alphanumeric characters. If this comment includes spaces, you must enclose the comment in quotation marks.

Usage Guidelines

Use this command to revoke a certificate from a invalid or suspected rogue AP.

Example

The following command revokes a certificate from an AP. This command does not delete a whitelist entry for a revoked AP, but marks its entry with the revoked state.

```
(host) (config) #whitelist-db rap revoke mac-address 00:1E:37:CA:D4:51
   revoke-comment "revoking cert from a rogue RAP."
```

Related Commands

Command	Description
whitelist-db rap del	Delete an entry from the remote AP whitelist

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap-local-switch-list

```
whitelist-db rap-local-switch-list
   del mac-addr <mac-address>
   purge
```

Description

Delete a managed device from the local switch table used by the remote AP whitelist.

Syntax

Parameter	Description
`del mac-address <mac-address>`	Remove a single managed device from the local switch table.
`purge`	Clear all managed devices from the local switch table

Usage Guidelines

If your deployment includes Mobility Master and managed devices, then the remote AP whitelist on each managed device contains an entry for every remote AP on the network, regardless of the managed device to which it is connected. Mobility Master also maintains a whitelist managed devices with remote AP. When you change a remote AP whitelist on any managed device, that managed device contacts Mobility Master to check the local switch whitelist, then contacts every other managed device on the local switch whitelist to notify it of the change.

If you ever remove a managed device from the network, you must also remove the managed device from the local switch whitelist. If the local switch whitelist contains entries for managed devices no longer on the network, then a remote AP whitelist entry can be marked for deletion but will not be physically deleted, as the managed device will be waiting for an acknowledgment from another managed device no longer on the network. Any unused managed device entries in the local switch whitelist can significantly increase network traffic and reduce memory resources.

Example

The following command removes a managed device from the local switch whitelist table:

```
(host)[node] (config) #whitelist-db rap-local-switch-list del mac-address 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description
whitelist-db rap add	Add an entry into the remote AP whitelist.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whitelist-db rap-master-switch-list

```
whitelist-db rap-master-switch-list
   del mac-addr <mac-address>
   purge
```

Description

Delete a Mobility Master from the master switch table used by the remote AP whitelist.

Syntax

Parameter	Description
`del mac-address <mac-address>`	Remove a singleMobility Master from the master switch whitelist.
`purge`	Clear all Mobility Masters from the Registered Master Switch table.

Usage Guidelines

Each managed device with remote APs managed through a remote AP whitelist has a master switch whitelist which contains the IP and MAC addresses of its Mobility Master. If your network has a redundant Mobility Master, then this whitelist will contain more than one entry.

The Mobility Master whitelist rarely needs to be purged. Although you can delete an entry from the master switch whitelist, you should do so only if you have removed a master switch from the network. Deleting a valid Mobility Master from the master switch whitelist can cause errors in your network.

Example

The following command removes a Mobility Master from the master switch whitelist table:

```
(host)[node](config) #whitelist-db rap-master-switch-list del mac-address 00:16:CF:AF:3E:E1
```

Related Commands

Command	Description
whitelist-db rap add	Add an entry into the remote AP whitelist.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

whoami

```
whoami
```

Description

This command displays information about the current user logged into the Mobility Master or managed device.

Syntax

No parameters.

Usage Guidelines

Use this command to display the name and role of the user who is logged into the device for this session.

Example

The following command displays information about the user logged into Mobility Master:

```
(host)[node](config) #whoami
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable and Config mode on Mobility Master

wipe

```
wipe out flash
```

Description

This command erases all data including configuration, logs, license keys, flash backup files and formats the flash file system in the controller.

Execute this command only when the controller is taken out of service or decommissioned.

Syntax

No syntax.

Example

The following command formats the flash file system:

```
(host) #wipe out flash
Do you really want to wipe out the entire flash (y/n): y
Zeroing out flash:.....................................
Flash zeroed out successfully.
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platform	License	Command Mode
All platforms	Base operating system	Enable mode on Mobility Master

wlan anyspot-profile

```
wlan anyspot-profile <profile-name>
   clone <profile-name>
   enable-anyspot
   exclude-essid <exclude-essid>
   exclude-wildcard <exclude-wildcard>
   no
   preset-essid <preset-essid>
```

Description

The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.

Syntax

Parameter	Description
`clone <profile-name>`	Make a copy of an existing anyspot profile.
`enable-anyspot`	Issue this command to enable the anyspot feature. Note that you must associate the anyspot profile with a virtual AP profile for the settings to take effect.
`exclude-essid <exclude-essid>`	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the **Exclude ESSID** lists. To add an ESSID to the list, enter the full name of the ESSID, then click **Add**. To remove an ESSID from the list, select it and click **Delete**. ESSIDs from neighboring APs will automatically appear in this list as long as the anyspot-enabled AP can detect that ESSID.
`exclude-wildcard <exclude-wildcard>`	An anyspot-enabled radio will not respond to client probe requests using an ESSID in the **Exclude ESSID** list. To exclude ESSIDs that partially match a text string, enter that string then click **Add**. To remove a matching string from the list, select it and click **Delete**.
`no`	Remove or negate any configured parameter.
`preset-essid <preset-essid>`	The anyspot-enabled AP will not send an ESSID in beacons, but if a client sends a probe request without an ESSIDs (that is, the probe request is not looking for a specific network) then the anyspot-enabled AP will respond to the probe request with an ESSID from this list.

Usage Guidelines

When an AP is configured to use this feature, the anyspot AP radio hides its configured ESSID in beacons, and compiles a list of other ESSIDs from detected neighboring APs. If the client sends a probe request without a specified ESSID, the anyspot AP will respond with a preconfigured ESSID.

When a client searches for a preferred network, that client sends the SSID of the preferred network in the probe request. The anyspot AP checks to see if there is a neighboring AP using that ESSID that can respond the client's request. If no matching network is found, the anyspot AP sends a response to the client using the SSID from the client request. If the client is authorized to connect to the anyspot AP, that client associates to AP. Once connected to the anyspot AP, the client recognizes the ESSID to which it is connected as one associated with its preferred network, and does not send out any further probe requests.

Example

The following command defines a ESSID to be returned in probe requests that do not contain an ESSID, as well as two ESSIDs that should be excluded from anyspot responses, in the event that a client is probing for one of these excluded ESSIDs.

```
(host) [/md] (config) #wlan anyspot-profile anyspot1
   (host) [/md] (Anyspot profile "anyspot1") #preset SSID companyguest
   (host) [/md] (Anyspot profile "anyspot1") #exclude-ssid corp_dev_essid
   (host) [/md] (Anyspot profile "anyspot1") #exclude-ssid corp_voip_essid
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

wlan bcn-rpt-req-profile

```
wlan bcn-rpt-req-profile <profile-name>
   channel <channel>
   clone <source>
   interface <interface>
   measure-dur-mandatory
   measure-duration <measure-duration>
   measure-mode
   no
   random-interval <random-interval>
   reg-class {1|12}
   request-info <request-info>
   rpt-condition <rpt-condition>
   rpt-detail
   ssid <ssid>
```

Description

Configures a Beacon Report Request Profile to provide the parameters for the Beacon Report Request frames.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	"default"
`channel <channel>`	This option is used to set the Channel field in the Beacon Report Request frame. The Channel value can be set to one of the following: ■ The channel of the AP (when Measurement Mode is set to either 'Passive' or 'Active-All channels') ■ 0 (when Measurement Mode is set to 'Beacon Table') ■ 255 (when Measurement Mode is set to 'Active-Channel Report')	For 802.11b/g band: 1 to 14 For 802.11a band: 36 to 165	255
`clone <source>`	Creates a copy of the Beacon Report Request Profile specified as the <source>. <source> is the name of an existing Beacon Report Request Profile from which parameter values are copied.	—	—
`interface <interface>`	This field is used to specify the radio interface for transmitting the Beacon Report Request frame.	0-1	1
`measure-dur-mandatory`	This value is used to set the Duration Mandatory bit of the Measurement Request Mode field of the Beacon Report Request frame.	—	Disabled
`measure-duration <measure-duration>`	This value is used to set the Measurement Duration field in the Beacon Report Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs.	0 – 65535	0

Parameter	Description	Range	Default
`measure-mode`	Indicates the mode used for the measurement. The valid measurement modes are: ■ **active-all-ch**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ■ **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. ■ **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ■ **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table	–	beacon-table
`no`	Negates any configured parameter.	—	—
`random-interval <random-interval>`	This value is used to set the Randomization Interval field in the Beacon Report Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units). A Randomization Interval of 0 in a measurement request indicates that no random delay is to be used.	0 – 65535	0
`reg-class {1|12}`	This option is used to specify the Regulatory Class field in the Beacon Report Request frame.	For 802.11b/g bands, 12. For 802.11a, use 1	—

Parameter	Description	Range	Default
`request-info <request-info>`	This option is used to indicate the contents of the Request Information IE that could be present in the Beacon Report Request frame. The Request Information IE is present for all Measurement Modes except the Beacon Table mode. It consists of a list of Element IDs that should be included by the client in the response frame.	Any valid element ID in the x/y/z format. For example, 0/21/22.	—
`rpt-condtion <rpt-condition>`	This option is used to indicate the value for the Reporting Condition field in the Beacon Reporting Information sub-element present in the Beacon Report Request frame.	0 - 255	0
`rpt-detail`	This option is used to indicate the value for the Detail field in the Reporting Detail sub-element present in the Beacon Report Request frame.	—	Disabled
`ssid <ssid>`	A unique character string (sometimes referred to as a network name), consisting of no more than 32 characters. The SSID is case-sensitive (for example, WLAN- 01).	—	—

Usage Guidelines

The Beacon Report Request profile is configured under the 802.11K profile.

Example

The following commands configure the parameters under the bcn-rpt-req-profile.

```
(host) [/md] (config) #wlan bcn-rpt-req-profile default
(host) [/md]  (Beacon Report Request Profile "default") #channel 9
(host) [/md]  (Beacon Report Request Profile "default") #interface 1
(host) [/md]  (Beacon Report Request Profile "default") #no measure-dur-mandatory
(host) [/md]  (Beacon Report Request Profile "default") #measure-duration 100
(host) [/md]  (Beacon Report Request Profile "default") #measure-mode active-all-ch
(host) [/md]  (Beacon Report Request Profile "default") #random-interval 100
(host) [/md]  (Beacon Report Request Profile "default") #reg-class 12
(host) [/md]  (Beacon Report Request Profile "default") #rpt-condition 2
(host) [/md]  (Beacon Report Request Profile "default") #no rpt-detail
(host) [/md]  (Beacon Report Request Profile "default") #request-info 0/21/22
(host) [/md]  (Beacon Report Request Profile "default") #ssid aruba-ap
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

wlan client-wlan-profile

```
wlan client-wlan-profile <profile-name>
   auth-as-computer
   auth-as-guest
   clone
   eap-cert
   eap-cert-connect-only-to
   eap-peap
   eap-peap-connect-only-to
   eap-type
   enable-8021x
   ieap-cert-connect-only
   inner-eap
   inner-eap-type
   no
   non-broadcasting-connection
   range-connect
   ssid-profile
```

Description

You can push WLAN profiles to users computers that use the Microsoft Windows Wireless Zero Config (WZC) service to configure and maintain their wireless networks. After the WLAN profiles are pushed to user computers, they are automatically displayed as an ordered list in the preferred networks.

Syntax

Parameter	Description	Default
auth-as-computer	Authenticate with domain credentials.	
auth-as-guest	Authenticate as a guest user.	
clone	Copy settings from another WLAN client profile.	
eap-cert	If you select EAP type as certificate, you can use one of the following options: ■ use-smartcard ■ simple-certificate-selection ■ use-different-name ■ validate-server-certificate	—
eap-cert-connect-only-to	Comma separated list of servers.	
eap-peap	Configure one of the following EAP-PEAP settings: ■ disconnect-if-no-crypto ■ dont-allow-user-authorize ■ enable-fast-reconnect ■ enable-quarantine-checks ■ validate-server-certificate	
eap-peap-connect-only-to	Comma separated list of servers.	

Parameter	Description	Default
eap-type	Select one of the following EAP types used by the client to connect to wireless network: ■ eap-peap - Select this option to specify EAP-PEAP as the authentication protocol. ■ eap-tls - Select this option to specify EAP-TLS as the authentication protocol.	EAP-PEAP
enable-8021x	Select this option to enable 802.1X authentication for this network.	Enabled
ieap-cert-connect-only-to	Command separated list of servers that the Inner EAP Certificates connects to.	
inner-eap	Enter the inner EAP type.	EAP-MSCHAPv2
inner-eap-type	Specify one of the following: ■ eap-gtc - Select this option to specify EAP-GenericTokenCard as the inner authentication protocol. ■ eap-mschapv2 - Select his option to specify EAP-MSCHAPV2 as the inner authentication protocol.	
no	Negate and reset all configuration settings.	
non-broadcasting-connection	Connect even if WLAN is not broadcasting.	Disabled
range-connect	Automatically connect to this WLAN if in range.	
ssid-profile	Enter the name of the SSID profile.	

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

wlan dot11k-profile

```
wlan dotllk <profile-name>
   ap-chan-rpt-11a <ap-chan-rpt-11a>
   ap-chan-rpt-11bg <ap-chan-rpt-11bg>
   bcn-measurement-mode {active-all-ch|active-ch-rpt|beacon-table|passive}
   bcn-req-chan-11a <bcn-req-chan-11a>
   bcn-req-chan-11bg <bcn-req-chan-11bg>
   bcn-req-time <bcn-req-time>
   bcn-rpt-req-profile <profile-name>
   clone <profile-name>
   dot11k-enable
   force-disassoc
   lm-req-time <lm-req-time>
   no ...
   rrm-ie-profile <profile-name>
   tsm-req-profile <profile-name>
   tsm-req-time <tsm-req-time>
```

Description

Configure a 802.11k radio profile.

Syntax

Parameter	Description	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	“default”
`ap-chan-rpt-11a <ap-chan-rpt-11a>`	This value is sent in the Channel field of the AP channel reports on the 'A' radio. You can specify values in the range 34 to 165.	36
`ap-chan-rpt-11bg <ap-chan-rpt-11bg>`	This value is sent in the Channel field of the AP channel reports on the 'BG' radio. You can specify values in the range 1 to 14.	1

Parameter	Description	Default
`bcn-measurement-mode`	Configures a beacon measurement mode for the profile. ■ **active-all-ch**—Enables active beacon measurement mode. In this mode, the client sends a probe request to the broadcast destination address on all supported channels, sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. ■ **active-ch-rpt**—In this mode, the client and returns a report that contains a list of channels in a regulatory class where a client is likely to find an AP, including the AP transmitting the AP channel report. ■ **beacon-table**—Enables beacon-table beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. ■ **passive**—Enables passive beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support the selected measurement mode, it returns a Beacon Measurement Report with the Incapable bit set in the Measurement Report Mode field. Default Mode: beacon-table	beacon-table
`beacon-table`	Enables **beacon-table** beacon measurement mode. In this mode, the client measures beacons and returns a report with stored beacon information for any supported channel with the requested SSID and BSSID. The client does not perform any additional measurements. This is the default beacon measurement mode. **NOTE:** If a station doesn't support beacon-table able measurement mode, it returns a Beacon Measurement Report with the *Incapable* bit set in the *Measurement Report Mode* field.	—
`passive`	Enables **passive** beacon measurement mode. In this mode, the client sets a measurement duration timer, and, at the end of the measurement duration, compiles all received beacons or probe response with the requested SSID and BSSID into a measurement report. **NOTE:** If a station doesn't support passive measurement mode, it returns a Beacon Measurement Report with the *Incapable* bit set in the *Measurement Report Mode* field.	—
`clone <profile-name>`	Copy settings from another specified 802.11k profile.	—
`bcn-req-chan-11a <bcn-req-chan-11a>`	This value is sent in the Channel field of the beacon requests on the 'A' radio. You can specify values in the range 34 to 165.	36
`bcn-req-chan-11bg <bcn-req-chan-11bg>`	This value is sent in the Channel field of the Beacon Requests on the BG radio. You can specify values in the range 1 to 14 or 0 to 255.	1

Parameter	Description	Default
`bcn-req-time <bcn-req-time>`	This option configures the time duration between two consecutive beacon requests sent to a802.11k client. By default, the beacon requests are sent to a802.11k client every 60 seconds. However, if a different value is required, the `bcn-req-time` option can be used. This permits values in the range from 10 seconds to 200 seconds.	60 seconds
bcn-rpt-req-profile <profile-name>	Beacon Report Request Settings for the selected profile.	—
`dot11k-enable`	Enables the 802.11K feature. This feature is disabled by default.	Disabled
`force-dissasoc`	This feature allows the AP to forcefully disassociate on-hook voice clients (clients that are not on a call) after period of inactivity. Without the forced disassociation feature, if an AP has reached its CAC limits and an on-hook voice client wants to start a new call, that client may be denied. If forced disassociation is enabled, those clients can associate to a neighboring AP that can fulfill their QoS requirements. **NOTE:** This feature is disabled by default.	Disabled
`lm-req-time <lm-req-time>`	This option configures the time duration between two consecutive link measurement requests sent to an 802.11k client. By default, link measurement requests are sent to a 802.11k client every 61 seconds. However, you can use the `lm-req-time` option to specify different time interval. This permits values in the range from 10 to 200 seconds.	60 seconds
`no`	Negates or removes any configured parameter.	
`rrm-ie-profile <profile-name>`	RRM IE Settings Profile.	
`tsm-req-profile <profile-name>`	TSM Report Request Settings Profile.	
`tsm-req-time <tsm-req-time>`	This option configures the time duration between two consecutive transmit stream measurement requests sent to a 802.11k client. By default, the transmit stream measurement requests are sent to a 802.11k client every 90 seconds. However, you can use the `tsm-req time` option to specify a different time interval. This permits values in the range from 10 seconds to 200 seconds.	90 seconds

Usage Guidelines

In a 802.11k network, if the AP with the strongest signal is reaches its maximum capacity, clients may connect to an under utilized AP with a weaker signal. A 802.11k profile can assigned to each virtual AP.

Example

The following command enables the 802.11k feature on the 802.11k profile and configures the beacon measurement mode and specifies the time interval for beacon, link, and transmit stream measurement

requests.

```
(host) [/md] (config) #wlan dot11k-profile default
(host) [/md] (802.11K Profile "default") #dot11k-enable
(host) [/md] (802.11K Profile "default") #bcn-measurement-mode beacon-table
(host) [/md] (802.11K Profile "default") #bcn-req-time 60
(host) [/md] (802.11K Profile "default") #lm-req-time 60
(host) [/md] (802.11K Profile "default") #tsm-req-time 90
```

Related Commands

Command	Description
wlan rrm-ie-profile	Configure an radio resource management RRM IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master

wlan dot11r-profile

```
wlan dotllr-profile <profile-name>
   clone
   dot11r
   key-duration <60-86400>
   key-assignment
   mob-domain-id <1-65535>
   no
```

Description

This command configures an 802.11r radio profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	Default
`clone`	Name of an existing dot11r-profile from which the parameter values are copied.	—	—
`mob-domain-id`	An ID that uniquely identifies the mobility domain.	1-65535	1
`dot11r`	Enables the Fast BSS Transition capability.	—	Disabled
`no`	Negates or removes any configured parameter.		—
`key-duration`	The r1 key timeout value in seconds for decrypt-tunnel or bridge mode.	60-86400	3600
`key-assignment`	The list of neighbor APs for decrypt-tunnel or bridge mode. ■ static: Get neighbor AP list from ARM or VBR. ■ dynamic: Use all APs from ap-group as the neighbor list.	—	—

Usage Guidelines

You can enable and configure Fast BSS Transition on a per Virtual AP basis. You must create an 802.11r profile and associate that with the Virtual AP profile through an SSID profile.

Example

The following set of commands enable the 802.11r capability on the 802.11r profile, configures the Fast BSS mobility domain ID, and specifies the r1 key time-out value.

```
(host) [/md] (config)#wlan dot11r-profile default
(host) [/md] (802.11r Profile "default") #fastbss-transition
(host) [/md] (802.11r Profile "default") #fastbss-mob-domain-id 25
(host) [/md] (802.11r Profile "default") #r1key_validity_duration 2500
```

Configure a mobility domain ID that uniquely identifies a mobility domain using the following command:

```
(host) [mynode] (802.11r Profile "default") #mob-domain-id <1-65535>
```

The default value is 1.

Configure the r1 key timeout value in seconds for decrypt-tunnel or bridge mode using the following command:

```
(host) [mynode] (802.11r Profile "default") #key_duration <60-86400>
```

The default value is 3600 seconds.

Apply the 802.11r profile to an SSID profile using the following command:

```
(host) [mynode] (config) #wlan ssid-profile voice dot11r-profile voice-enterprise
```

You can advertise the 802.11r capability on the Virtual AP profile by applying the SSID profile. Use the following command to apply the SSID profile to the Virtual AP profile:

```
(host) [mynode] (config) #wlan virtual-ap voice-AP ssid-profile voice
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

wlan edca-parameters-profile

```
wlan edca-parameters-profile
   ap|station <profile-name>
      background [acm <0-1>]|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]|[txop <0-2047>]
      best-effort [acm <0-1>]|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]|[txop <0-2047>]
      clone <source>
      no
      video [acm <0-1>]|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]|[txop <0-2047>]
      voice [acm <0-1>]|[aifsn <1-15>]|[ecw-max <1-15>|[ecw-min <0-15>]|[txop <0-2047>]
```

Description

This command configures an EDCA profile for APs or for clients (stations).

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	default
`background`	Configures the background queue.	—	—
`best-effort`	Configures the best-effort queue.	—	—
`clone`	Name of an existing EDCA profile from which parameter values are copied.	—	—
`no`	Remove or negate a parameter.	—	—
`video`	Configures the video queue.	—	—
`voice`	Configures the voice queue.	—	—
`acm`	Specifies mandatory admission control. The client reserves the AC through TSPEC signaling. Enter 1 to enable, 0 to disable.	0, 1	0 (disabled)
`aifsn`	Arbitrary inter-frame space number.	1-15	0
`ecw-max`	The exponential (n) value of the maximum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.	1-15	0
`ecw-min`	The exponential (n) value of the minimum contention window size, as expressed by 2^n-1. A value of 4 computes to 2^4-1 = 15.	0-15	0
`txop`	TXOP in units of 32 microseconds. Divide the desired transmission duration by 32 to determine the value to configure. For example, for a transmission duration of 3008 microseconds, enter 94 (3008/32).	0-2047	0

Usage Guidelines

EDCA profiles are specific either to APs or clients. You apply an EDCA profile to a specific SSID profile. use this command only under the guidance of your Aruba technical support representative.

The following are the default values configured for APs:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	6	3	0	No
background	4	10	7	0	No
video	3	4	1	94	No
voice	2	3	1	47	No

The following are the default values configured for clients:

Access Category	ecw-min	ecw-max	aifsn	txop	acm
best-effort	4	10	3	0	No
background	4	10	7	0	No
video	3	4	2	94	No
voice	2	3	2	47	No

Example

The following command configures an EDCA profile for APs:

```
(host) [/md] (config) #wlan edca-parameters-profile ap edca1
(host) [/md] (EDCA Parameters profile (AP) "edca1") #best-effort ecw-min 15 ecw-max 15 aifsn
15 txop 100 acm 1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Master

wlan hotspot advertisement-profile

```
wlan hotspot advertisement profile <profile-name>
   anqp-3gpp-nwk-profile <profile-name>
   anqp-domain-name-profile <profile-name>
   anqp-ip-addr-avail-profile <profile-name>
   anqp-nai-realm-profile <profile-name>
   anqp-nwk-auth-profile <profile-name>
   anqp-roam-cons-profile <profile-name>
   anqp-venue-name-profile <profile-name>
   clone <profile-name>
   h2qp-conn-cap-profile <profile-name>
   h2qp-op-cl-profile <profile-name>
   h2qp-operator-friendly-profile <profile-name>
   h2qp-wan-metrics-profile <profile-name>
   no
```

Description

This command configures a WLAN advertisement profile for an 802.11u public access service provider.

Syntax

Parameter	Description
`anqp-3gpp-nwk-profile <profile-name>`	Name of the Access Network Query Protocol (ANQP) 3GPP cellular network profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-3gpp-nwk-profile on page 2594.
`anqp-domain-name-profile <profile-name>`	Name of the ANQP domain name profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-domain-name-profile on page 2596.
`anqp-ip-addr-avail-profile <profile-name>`	Name of the ANQP IP Address Availability profile to be associated with this WLAN advertisement profile.For more information on configuring this profile, refer to wlan hotspot anqp-ip-addr-avail-profile on page 2598.
`anqp-nai-realm-profile <profile-name>`	Name of the ANQP NAI Realm profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-nai-realm-profile on page 2600.
`anqp-nwk-auth-profile <profile-name>`	Name of the ANQP Network Authentication profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-nwk-auth-profile on page 2605.

Parameter	Description
`anqp-roam-cons-profile <profile-name>`	Name of the ANQP Roaming Consortium profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-roam-cons-profile on page 2607.
`anqp-venue-name-profile <profile-name>`	Name of the ANQP Venue Name profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot anqp-venue-name-profile on page 2609.
`clone <profile-name>`	Make a copy of an existing WLAN Advertisement profile.
`h2qp-conn-cap-profile <profile-name>`	Name of the Hotspot 2.0 Connection Capability profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-conn-capability-profile on page 2612.
`h2qp-op-cl-profile <profile-name>`	Name of the Hotspot 2.0 Operating Class Indication profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-op-cl-profile on page 2614.
`h2qp-operator-friendly-name-profile <profile-name>`	Name of the Hotspot 2.0 operator-friendly name profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-operator-friendly-name-profile on page 2616.
`h2qp-wan-metrics-profile <profile-name>`	Name of the Hotspot 2.0 WAN Metrics profile to be associated with this WLAN advertisement profile. For more information on configuring this profile, refer to wlan hotspot h2qp-wan-metrics-profile on page 2618.
`no`	Negate or remove any existing parameter, returning it to its default value.

Usage Guidelines

Hotspot 2.0 is a WFA specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

Access Network Query Protocol (ANQP) and Hotspot 2.0 Query Protocol (H2QP) profiles define the information in the 802.11u IEs to be broadcast by an 802.11u-capable AP. Use this command to select one of each type of ANQP and H2QP profile to be associated with the advertisement profile.

Values configured in the ANQP profiles will not be sent to clients unless you:

1. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
2. Enable the hotspot feature within that Hotspot profile (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Example

The following command associates the ANQP domain name profile **anqp-dom-1** to the advertisement profile **network1**:

```
(host) [mynode] (config) #wlan hotspot advertisement-profile network1
(host) [mynode] (Advertisement Profile "network1") #anqp-domain-name-profile anqp-dom-1
```

Related Commands

Use the following commands to configure the Hotspot feature:

Command	Description
wlan hotspot anqp-3gpp-nwk-profile	This profile defines information for a 3rd Generation Partnership Project (3GPP) Cellular Network for hotspots that have roaming relationships with cellular operators
wlan hotspot anqp-domain-name-profile	This command defines the domain name to be sent in an Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
wlan hotspot anqp-ip-addr-avail-profile	This command defines available IP address types to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
wlan hotspot anqp-nai-realm-profile	This command defines a Network Access Identifier (NAI) realm whose information can be sent as an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response
wlan hotspot anqp-nwk-auth-profile	This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.
wlan hotspot anqp-roam-cons-profile	This command configures the Roaming Consortium OI information to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response
wlan hotspot anqp-venue-name-profile	This command defines venue information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.
wlan hotspot h2qp-conn-capability-profile	This command defines a Hotspot 2.0 Query Protocol (H2QP) profile that advertises hotspot protocol and port capabilities.
wlan hotspot h2qp-op-cl-profile	This command defines a Hotspot 2.0 Query Protocol (H2QP) profile that defines the Operating Class to be sent in the ANQP IE.
wlan hotspot h2qp-operator-friendly-name-profile	This command defines a Hotspot 2.0 Query Protocol (H2QP) operator-friendly name profile.
wlan hotspot h2qp-wan-metrics-profile	This command creates a Hotspot 2.0 Query Protocol (H2QP) profile that specifies the hotspot WAN status and link metrics.
wlan hotspot hs2-profile	This command configures a hotspot profile for an 802.11u public access service provider.

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-3gpp-nwk-profile

```
wlan hotspot anqp-3gpp-nwk-profile <profile-name>
   3gpp_plmn1 <3GPP-PLMN1>
   3gpp_plmn2 <3GPP-PLMN2>
   3gpp_plmn3 <3GPP-PLMN3>
   3gpp_plmn4 <3GPP-PLMN4>
   3gpp_plmn5 <3GPP-PLMN5>
   3gpp_plmn6 <3GPP-PLMN6>
   clone <source>
   no
```

Description

This profile defines information for a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators.

Syntax

Parameter	Description
`3gpp_plmn1`	The Public Land Mobile Networks (PLMN) value of the highest-priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp_plmn2`	The Public Land Mobile Networks (PLMN) value of the second-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp_plmn3`	The Public Land Mobile Networks (PLMN) value of the third-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp_plmn4`	The Public Land Mobile Networks (PLMN) value of the fourth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp_plmn5`	The Public Land Mobile Networks (PLMN) value of the fifth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`3gpp_plmn6`	The Public Land Mobile Networks (PLMN) value of the sixth-highest priority network. The PLMN is comprised of a 12-bit Mobile Country Code (MCC) and the 12-bit Mobile Network Code (MNC).
`clone <profile-name>`	Copies an existing 3GPP profile.
`no`	Removes an existing parameter.

Usage Guidelines

The 3GPP Cellular Network Profile defines an ANQP information element (IE) to be sent in a Generic Advertisement Service (GAS) query response from an AP in a hotspot with a roaming relationship with a cellular operator. The 3GPP Mobile Country Code (MCC) and the 12-bit Mobile Network Code data in the IE can help the client select a 3GPP network.

Values configured in this profile will not be sent to clients unless you:

1. Associate the 3GPP Cellular Network profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-3gpp-nwk-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. ("`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Example

The following command defines 3GPP data for the 3GPP profile **cellcorp1**:

```
(host) [md] (config) #wlan hotspot anqp-3gpp-nwk-profile cellcorp1
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #enable
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #3gpp_plmn1 310026
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #3gpp_plmn2 208000
(host) [md] ((ANQP 3GPP Cellular Network Profile "cellcorp1") #3gpp_plmn3 208001
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-domain-name-profile

```
wlan hotspot anqp-domain-name-profile <profile-name>
   clone <source>
   domain-name <domain-name>
   no
```

Description

This command defines the domain name to be sent in an Access Network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Syntax

Parameter	Description
`<profile-name>`	ANQP domain name profile.
`clone <source>`	Copies an existing ANQP domain name profile.
`domain-name <domain-name>`	Domain name of the hotspot operator. This alphanumeric string must be 255 characters or less.
`no`	Removes an existing parameter.

Usage Guidelines

Use this command to configure a domain name in the ANQP Domain Name profile. If a client uses the Generic Advertisement Service (GAS) to post an ANQP query to an Access Point, the AP will return an ANQP Information Element with the domain name configured in this profile.

Values configured in this profile are not sent to clients unless you:

1. Associate the ANQP Domain Name profile with an ANQP advertisement profile (`wlan hotspot advertisement profile <profile-name> anqp-domain-name-profile <profile-name>`).
2. Associate the ANQP advertisement profile with a Hotspot profile (`wlan hotspot h2-profile advertisement-profile <profile-name>`).
3. Enable the hotspot feature within that Hotspot profile (`wlan hotspot h2-profile <profile-name> hotspot-enable`).

Example

The following command defines a domain name for the ANQP domain name profile domain1:

```
(host) [md] (config) #wlan hotspot anqp-domain-name-profile domain1
(host) [md] (ANQP Domain Name Profile "domain1") #domain-name example.com
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-ip-addr-avail-profile

```
wlan hotspot anqp-ip-addr-avail-profile <profile-name>
   clone <profile-name>
   ipv4-addr-avail {availability-unknown|not-available|port-restricted|port-restricted-ouble-
   nated|port-restricted-single-nated|private-double-nated|private-single-nated|public}
   ipv6-addr-avail {available|availability-unknown|not-available}
   no
```

Description

This command defines available IP address types to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Syntax

Parameter	Description
`<profile-name>`	Name of the ANQP IP address availability profile.
`clone <source>`	Copies an existing ANQP IP Address Availability profile.
`ipv4-addr-avail`	Indicates the availability of an IPv4 network.
`availability-unknown`	Network availability cannot be determined.
`not-available`	Network is not available.
`port-restricted`	Network has some ports restricted (for example, the network blocks port 110 to restrict POP mail).
`port-restricted-double-nated`	Network has some ports restricted and multiple routers performing network address translation.
`port-restricted-single-nated`	Network has some ports restricted and a single router performing network address translation.
`private-double-nated`	Network is a private network with multiple routers doing network address translation.
`private-single-nated`	Network is a private network a single router doing network address translation.
`public`	Network is a public network.
`ipv6-addr-avail`	Indicates the availability of an IPv6 network.
`available`	An IPv6 network is available.
`availability-unknown`	Network availability cannot be determined.
`not-available`	Network is not available.
`no`	Removes an existing parameter.

Usage Guidelines

The IP Address Availability information configured using this command provides clients with information about the availability of IP address versions and types which could be allocated to those clients after they associate to the hotspot AP.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP IP Address Availability profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-ip-addr-avail-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Example

The following command configures an AP using this profile to advertise a public IPv4 network:

```
(host) [md] (config) #wlan hotspot anqp-ip-addr-avail-profile default
(host) [md] (ANQP IP Address Availability Profile "default") #ipv4-addr-avail public
(host) [md] (ANQP IP Address Availability Profile "default") #ipv6-addr-avail not-available
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-nai-realm-profile

```
wlan hotspot anqp-nai-realm-profile <profile-name>
   clone <source>
   nai-home-realm
   nai-realm-auth-id-1|nai-realm-auth-id-2 {credential-type|expanded-eap|expanded-inner-
   eap|inner-auth-eap|non-eap-inner-auth|reserved|tunneled-eap-credential-type}
   nai-realm-auth-value-1|nai-realm-auth-value-2 {cred-cert|cred-hw-token|cred-nfc|cred-
   none|cred-rsvd|cred-sim|cred-soft-token|cred-user-pass|cred-usim|cred-vendor-spec|eap-
   crypto-card|eap-generic-token-card|eap-identity|eap-method-aka|eap-method-sim|eap-method-
   tls|eap-method-ttls|eap-notification|eap-one-time-password|eap-peap|eap-peap-mschapv2|non-
   eap-chap|non-eap-mschap|non-eap-mschapv2|non-eap-pap|non-eap-rsvd|reserved|tun-cred-
   anon|tun-cred-cert|tun-cred-hw-token|tun-cred-nfc|tun-cred-rsvd|tun-cred-sim|tun-cred-soft-
   token|tun-cred-user-pass|tun-cred-usim|tun-cred-vendor-spec}
   nai-realm-eap-method crypto-card|eap-aka|eap-sim|eap-tls|eap-ttls|generic-token-
     card|identity|notification|one-time-password|peap|peap-mschapv2
   nai-realm-encoding <nai-realm-encoding>
   nai-realm-name <nai-realm-name>
   no
```

Description

This command defines a Network Access Identifier (NAI) realm whose information can be sent as an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Syntax

Parameter	Description
`<profile-name>`	Name of the ANQP NAI realm profile.
`clone <source>`	Copies an existing NAI Realm profile.
`nai-home-realm`	Marks the realm in this profile as the NAI Home Realm.
`nai-realm-auth-id-1|nai-realm-auth-id-2`	Use the **nai-realm-auth-id-1** command to send the one of the following authentication methods for the primary NAI realm ID. Use the **nai-realm-auth-id-2** command to send the one of the following authentication methods for the secondary NAI realm ID.
`credential-type`	The specified authentication ID uses credential authentication.
`expanded-eap`	The specified authentication ID uses the expanded EAP authentication method.
`expanded-inner-eap`	The specified authentication ID uses the expanded inner EAP authentication method.
`inner-auth-eap`	The specified authentication ID uses inner EAP authentication type.

Parameter	Description
non-eap-inner-auth	The specified authentication ID uses non-EAP inner authentication type.
reserved	The specified authentication ID uses Reserved authentication type.
tunneled-eap-credential-type	The specified authentication ID uses the tunneled EAP credential type.
nai-realm-auth-value-1|nai-realm-auth-value-2	Use the **nai-ream-auth-value-1** command to select an authentication value for the authentication method specified by **nai-realm-auth-id-1**. Use the **nai-ream-auth-value-2** command to select the authentication value for the authentication method specified by **nai-realm-auth-id-2**.
cred-cert	Credential - Certificate.
cred-hw-token	Credential - Hardware Token.
cred-nfc	Credential - NFC.
cred-none	Credential - None.
cred-rsvd	Credential - Reserved.
cred-sim	Credential - SIM.
cred-soft-token	Credential - Soft Token.
cred-user-pass	Credential - Username and password.
cred-usim	Credential - USIM.
cred-vendor-spec	Credential - Vendor-specific.
eap-crypto-card	EAP Method - Crypto-card.
eap-generic-token-card	EAP Method - Generic-Token-Card.
eap-identity	EAP Method - Identity.
eap-method-aka	EAP Method - AKA.
eap-method-sim	EAP Method - SIM - GSM Subscriber Iden.
eap-method-tls	EAP Method - TLS - Transport Layer Sec.
eap-method-ttls	EAP Method - TTLS - Tunneled Transport Security.
eap-notification	EAP Method - Notification.
eap-one-time-password	EAP Method - One-Time-Password.
eap-peap	EAP Method - PEAP.

Parameter	Description
eap-peap-mschapv2	EAP Method - PEAP MSCHAP V2.
non-eap-chap	Non-EAP Method - CHAP.
non-eap-mschap	Non-EAP Method - MSCHAP.
non-eap-mschapv2	Non-EAP Method - MSCHAPv2.
non-eap-pap	Non-EAP Method - PAP.
non-eap-rsvd	Non-EAP Method - Reserved for future use.
reserved	Reserved for future use.
tun-cred-anon	Tunneled Credential - ANONYMOUS.
tun-cred-cert	Tunneled Credential - CERTIFICATE .
tun-cred-hw-token	Tunneled Credential - Hardware Token.
tun-cred-nfc	Tunneled Credential - NFC.
tun-cred-rsvd	Tunneled Credential - RESERVED.
tun-cred-sim	Tunneled Credential - SIM.
tun-cred-soft-token	Tunneled Credential - Soft Token.
tun-cred-user-pass	Tunneled Credential - USERNAME and PASSWORD.
tun-cred-usim	Tunneled Credential - USIM.
tun-cred-vendor-spec	Tunneled Credential - VENDOR SPECIFIC.
nai-realm-eap-method	Select one of the options below to identify the EAP authentication method supported by the hotspot realm.
crypto-card	Crypto card authentication
eap-aka	EAP for UMTS Authentication and Key Agreement
eap-sim	EAP for GSM Subscriber Identity Modules
eap-tls	EAP-Transport Layer Security
eap-ttls	EAP-Tunneled Transport Layer Security
generic-token-card	EAP Generic Token Card (EAP-GTC)
identity	EAP Identity type
notification	The hotspot realm uses EAP Notification messages for authentication.

Parameter	Description
one-time-password	Authentication with a single-use password.
peap	Protected Extensible Authentication Protocol
peap-mschapv2	Protected Extensible Authentication Protocol with Microsoft CHAP version 2
nai-realm-encoding <nai-realm-encoding>	Issue this command if the NAI realm named defined by nai-realm-name <nai-realm-name> is a UTF-8 formatted character string that is not formatted in accordance with IETF RFC 4282.
nai-realm-name <nai-realm-name>	Name of the NAI realm. The realm name is often the domain name of the service provider.
no	Negates or removes any existing parameter

Usage Guidelines

An AP's NAI Realm profile identifies and describes a NAI realm accessible using the AP, and the method that this NAI realm uses for authentication. These settings configured in this profile determine the NAI realm elements that are included as part of a GAS Response frame.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP NAI Realm profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name>anqp-nai-realm-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profileadvertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Example

```
(host) [md] (config) #wlan hotspot anqp-nai-realm-profile home
(host) [md] (ANQP NAI Realm Profile "home") #enable
(host) [md] (ANQP NAI Realm Profile "home") #nai-realm-name corp-hotspot.com
(host) [md] (ANQP NAI Realm Profile "home") #nai-realm-auth-id-1 credential-type
(host) [md] (ANQP NAI Realm Profile "home") #nai-realm-auth-value-1 cred-cert
(host) [md] (ANQP NAI Realm Profile "home") #nai-home-realm
(host) [md] (config) #wlan hotspot anqp-nai-realm-profile non-home
(host) [md] (ANQP NAI Realm Profile "non-home") #nai-realm-name corp-hotspot-roam.com
(host) [md] (ANQP NAI Realm Profile "non-home") #nai-realm-eap-method eap-sim
(host) [md] (ANQP NAI Realm Profile "non-home") #nai-realm-auth credential-type
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-nwk-auth-profile

```
wlan hotspot anqp-nwk-auth-profile <profile-name>
   clone <source>
   no
   nwk-auth-type {acceptance|dns-redirection|http-https-redirection|online-enroll}
   url <url>
```

Description

This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.

Syntax

Parameter	Description
`<profile-name>`	Name of the ANQP network authentication profile.
`clone <source>`	Copies an existing ANQP Network Authentication profile.
`no`	Negates any existing parameter.
`nwk-auth-type`	Network authentication type being used by the hotspot network.
`acceptance`	Network requires the user to accept terms and conditions. **NOTE:** This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
`dns-redirection`	Additional information on the network is provided through DNS redirection. **NOTE:** This option requires you to specify a redirection URL string as an IP address, FQDN or URL.
`http-https-redirection`	Additional information on the network is provided through HTTP or HTTPS redirection.
`online-enroll`	Network supports online enrollment.
`url <url>`	URL, IP address, or FQDN used by the hotspot network for the **acceptance** or **dns-redirection** network authentication types.

Usage Guidelines

When you enable the asra option in the WLAN hotspot profile, the settings you configure in the Network Authentication profile are sent in the GAS response to the client.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Network Authentication profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-nwk-auth-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile1advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Example

The following command configures the default Network Authorization profile to use DNS redirection:

```
(host) [md] (config) #wlan hotspot anqp-nwk-auth-profile defaul
(host) [md] (ANQP Network Authentication Profile "default") #nwk-auth-type dns-redirection
redirect-url http://www.example.com/redirect.html
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-roam-cons-profile

```
wlan hotspot anqp-roam-cons-profile <profile-name>
   clone <source>
   no
   roam-cons oi <oi>
```

Description

This command configures the Roaming Consortium OI information to be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Syntax

Parameter	Description
`<profile-name>`	Name of the ANQP roaming consortium profile.
`clone <source>`	Copies an existing ANQP Roaming Consortium profile.
`no`	Negates any existing parameter.
`roam-cons oi <oi>`	Sends the specified roaming consortium OI in a GAS query response. The OI must be a hexadecimal value.

Usage Guidelines

Organization Identifiers (OIs) are assigned to service providers when they register with the IEEE registration authority. The Roaming Consortium IEs contain information identifying the network and service provider, whose security credentials can then be used to authenticate with the AP transmitting this element.

Use the wlan hotspot anqp-roam-cons-profile command to define the OI for the hotspot service provider in the ANQP Roaming Consortium profile. Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Roaming Consortium profile an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-roam-cons-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

To identify additional Roaming consortium OIs used by the service provider's top three roaming partners, configure the wlan hotspot hs2-profile, wlan hotspot hs2-profile or wlan hotspot hs2-profile parameters in the Hotspot Profile.

Example

The following command defines the roaming consortium OI and OI length in the ANQP roaming consortium profile:

```
(host) [md] (config) #wlan hotspot anqp-roam-cons-profile profile1
(host) [md] (ANQP Roaming Consortium Profile "profile1") #roam-cons oi 506F9A
(host) [md] (ANQP Roaming Consortium Profile "profile1") #roam-cons-oi-len 3
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot anqp-venue-name-profile

```
wlan hotspot anqp-venue-name-profile <profile-name>
   clone
   no
   venue-group {outdoor|reserved|utility-misc|vehicular|assembly|business|educational|factory-
   or-industrial|institutional|mercantile|residential|storage|unspecified|utility-
   misc|vehicular}
   venue-lang-code <venue-lang-code>
   venue-name <venue-name>
   venue-type <venue-type>
```

Description

This command defines venue information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response.

Syntax

Parameter	Description
`<profile-name>`	Name of the ANQP venue profile.
`clone <source>`	Copies an existing ANQP Venue Name profile.
`no`	Negates any existing parameter.
`venue-group`	Specify one of the following venue groups to be advertised in the ANQP IEs from APs associated with this profile. The default setting is unspecified. ■ assembly ■ business ■ educational ■ factory-or-industrial ■ institutional ■ mercantile ■ outdoor ■ reserved ■ residential ■ storage ■ unspecified ■ utility-misc ■ vehicular
`venue-lang-code <venue-lang-code>`	An ISO 639 language code that identifies the language used in the Venue Name field.
`venue-name <venue-name>`	Venue name to be advertised in the ANQP IEs from APs associated with this profile. If the venue name includes spaces, the name must be enclosed in quotation marks, e.g. “Midtown Shopping Center”.
`venue-type <venue-type>`	Specify a venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 2610.

Usage Guidelines

Use this command to configure the venue group and venue type in an ANQP Venue Name profile. If a client uses the Generic Advertisement Service (GAS) to post an ANQP query to an Access Point, the AP will return ANQP Information Elements with the values configured in this profile.

Values configured in this profile will not be sent to clients unless you:

1. Associate the ANQP Venue Name profile with an ANQP Advertisement profile. (`wlan hotspot advertisement profile <profile-name> anqp-venue-name-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Venue Types

The following list describes the different venue types that may be configured in a hotspot profile:

- assembly-amphitheater
- assembly-amusement-park
- assembly-arena
- assembly-bar
- assembly-coffee-shop
- assembly-convention-center
- assembly-emer-coord-center
- assembly-library
- assembly-museum
- assembly-passenger-terminal
- assembly-restaurant
- assembly-stadium
- assembly-theater
- assembly-unspecified
- assembly-worship-place
- assembly-zoo
- business-attorney
- business-bank
- business-doctor
- business-fire-station
- business-police-station
- business-post-office
- business-professional-office
- business-research-and-development
- business-unspecified
- educational-primary-school
- educational-secondary-school
- educational-university
- educational-unspecified
- industrial-factory
- institutional-alcohol-or-drug-rehab
- institutional-group-home
- institutional-hospital
- institutional-prison
- institutional-terminal-care
- institutional-unspecified
- mercantile-automotive-service-station
- mercantile-gas-station
- mercantile-grocery
- mercantile-retail
- mercantile-shopping-mall
- merchantile unspecified
- outdoor-bus-stop
- outdoor-city-park
- outdoor-kiosk
- outdoor-muni-mesh-nwk
- outdoor-rest-area
- outdoor-traffic-control
- outdoor-unspecified
- residential-boarding-house
- residential-dormitory
- residential-hotel
- residential-private-residence
- residential-unspecified
- unspecified
- vehicular-airplane
- vehicular-automobile
- vehicular-bus
- vehicular-ferry
- vehicular-motor-bike
- vehicular-ship
- vehicular-train
- vehicular-unspecified

Example

The following command defines an ANQP Venue Name profile for a shopping mall:

```
(host) [md] (config) #wlan hotspot anqp-venue-name-profile Mallprofile1
(host) [md] (ANQP Venue Name Profile "Mallprofile1") #venue-group mercantile
(host) [md] (ANQP Venue Name Profile "Mallprofile1") #venue-name Westgate Shopping Center

(host) [md] (ANQP Venue Name Profile "Mallprofile1") #venue-type mercantile-shopping-mall
```

Command History

Version	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot h2qp-conn-capability-profile

```
wlan hotspot h2qp-conn-capability-profile <profile-name>
   clone <source>
   esp
   icmp
   no
   tcp-ftp
   tcp-http
   tcp-pptp-vpn
   tcp-ssh
   tcp-tls-vpn
   tcp-voip
   udp-ike2-4500
   udp-ike2-500
   udp-voip
```

Description

This command defines an H2QP profile that advertises hotspot protocol and port capabilities.

Syntax

Parameter	Description
`<profile-name>`	Name of the H2QP connection capability profile.
`clone <source>`	Copies an existing hotspot connection capability profile.
`esp`	Include this parameter to enable the Encapsulating Security Payload (ESP) port used by IPsec VPNs. (port 0)
`icmp`	Indicates that the ICMP port is enabled and available. (port 0)
`no`	Negates any existing parameter, returning it to its default disabled value.
`tcp-ftp`	Include this parameter to enable the FTP port. (port 20)
`tcp-http`	Include this parameter to enable the HTTP port. (port 80)
`tcp-pptp-vpn`	Include this parameter to enable the PPTP port used by IPsec VPNs. (port 1723)
`tcp-ssh`	Include this parameter to enable the SSH port. (port 22)
`tcp-tls-vpn`	Include this parameter to enable the TCP TLS port used by VPNs. (port 80)
`tcp-voip`	Include this parameter to enable the TCP VoIP port. (port 5060)
`udp-ike2-4500`	Include this parameter to enable the IKEv2. (port 4500)
`udp-ike2-500`	Include this parameter to enable the IKEv2. (port 500)
`udp-voip`	Include this parameter to enable the UDP VoIP port. (port 5060)

Usage Guidelines

The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about the IP protocols and associated port numbers that are available and open for communication.

Values configured in this profile will not be sent to clients unless you:

1. Associate the H2QP profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> h2qp-conn-cap-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Example

The following example allows the H2QP connection capability profile to advertise the availability of ICMP, HTTP, and VOIP ports:

```
(host) [md] (config) #wlan hotspot h2qp-conn-capability-profile Wan1
(host) [md] (H2QP Connection Capability Profile "Wan1") #icmp
(host) [md] (H2QP Connection Capability Profile "Wan1") #http
(host) [md] (H2QP Connection Capability Profile "Wan1") # voip
(host) [md] (H2QP Connection Capability Profile "Wan1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot h2qp-op-cl-profile

```
wlan hotspot h2qp-op-cl-profile <profile-name>
   clone <source>
   no
   op-cl <op-cl>
```

Description

This command defines an H2QP profile that defines the Operating Class to be sent in the ANQP IE.

Syntax

Parameter	Description
`<profile-name>`	Name of the H2QP operating class indication profile.
`clone <source>`	Copies an existing hotspot operating class profile.
`no`	Negates any existing parameter, returning it to its default disabled value.
`op-cl <op-cl>`	Configures the operating class for the devices' BSS. The supported range for this field is 1-255, and the default value is 1.

Usage Guidelines

The values configured in this H2QP Operating Class profile define the channels on which the hotspot is capable of operating. It may be useful where, for instance, a mobile device discovers a hotspot in the 2.4 GHz band but finds it is dual-band and prefers the 5 GHz band. For a definition of these global operating classes, refer to Table E-4 of IEEE Std 802.11-2012, Annex E.

Values configured in this profile will not be sent to clients unless you:

1. Associate the H2QP profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name> h2qp-op-cl-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name> hotspot-enable`)

Example

The following example configures and enables a profile with the default operating class value:

```
(host) [md] (config) #wlan hotspot h2qp-op-cl-profile profile1
(host) [md] (H2QP Operating Class Indication Profile "profile1") #op-cl 1
(host) [md] (H2QP Operating Class Indication Profile "profile1") #enable
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot h2qp-operator-friendly-name-profile

```
wlan hotspot h2qp-operator-friendly-name-profile <profile-name>
   clone <source>
   no
   op-fr-name <op-fr-name>
   op-fr-name-hex <op-fr-name-hex>
   op-lang-code <op-lang-code>
```

Description

This command defines an H2QP operator-friendly name profile.

Syntax

Parameter	Description
`<profile-name>`	H2QP operator friendly name profile.
`clone <source>`	Copies an existing operator-friendly name profile.
`no`	Negates any existing parameter.
`op-fr-name <op-fr-name>`	An operator-friendly name sent by devices using this profile. The name can be up to 64 alphanumeric characters, and can include special characters and spaces. If the name includes quotation marks (“), you must include a backslash character (\) before each quotation mark. (e.g. \"example\")
`op-fr-name-hex <op-fr-name-hex>`	Operator Friendly Name in HEX.
`op-lang-code <op-lang-code>`	An ISO 639 language code that identifies the language used in the op-fr-name field.

Usage Guidelines

The operator-friendly name configured in this profile is a free-form text field that can identify the operator and also something about the location.

Values configured in this profile will not be sent to clients unless you:

1. Associate the H2QP operator-friendly name profile with an ANQP advertisement profile. (`wlan hotspot advertisement profile <profile-name>h2qp-operator-friendly-profile <profile-name>`)
2. Associate the ANQP advertisement profile with a Hotspot profile. (`wlan hotspot h2-profile advertisement-profile <profile-name>`)
3. Enable the hotspot feature within that Hotspot profile. (`wlan hotspot h2-profile <profile-name>hotspot-enable`)

Example

The example below shows that the managed device has two configured operator friendly name profiles. The **References** column lists the number of other profiles with references to the operator friendly name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [md] (config) #wlan hotspot h2qp-operator-friendly-name-profile profile1
(host) [md] (H2QP Operator Friendly Name Profile "profile1") #op-fr-name my_hotspot
```

```
(host) [md] (H2QP Operator Friendly Name Profile "profile1") #op-lang-code <op-lang-code>
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot h2qp-wan-metrics-profile

```
wlan hotspot h2qp-wan-metrics-profile <profile-name>
   at-capacity
   clone <source>
   downlink-load
   downlink-speed
   load-dur
   no
   symm-link
   uplink-load
   uplink-speed
   wan-metrics-link-status link_down|link_test|link_up|reserved
```

Description

This command creates an H2QP profile that specifies the hotspot WAN status and link metrics.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of the H2QP WAN metrics profile.	—	—
`at_capacity`	Use the **at_capacity** parameter to indicate that the WAN Link has reached its maximum capacity. If this parameter is enabled, no additional mobile devices will be permitted to associate with the hotspot AP.	enable disable	disabled
`clone <source>`	Copies an existing H2QP profile.	—	—
`downlink-load <load>`	The percentage of the WAN downlink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.	1-100	0 (unspecified)
`downlink-speed <speed>`	Use the `downlink_speed <speed>` parameter to indicate the current WAN backhaul downlink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.	0 - 2,147,483,647 Kbps	0 (unspecified)
`load-dur <load_dur>`	Duration over which the downlink load is measured, in tenths of a second.	0 and 65535	0 (unspecified)
`no`	Negates any existing parameter	—	—
`symm-link`	Use the **symn_link** parameter to indicate that the WAN Link has same speed in both the uplink and downlink directions.	enabled disabled	disabled

Parameter	Description	Range	Default
`uplink-load <speed>`	The percentage of the WAN uplink that is currently utilized. If no value is set, this parameter will show a default value of 0 to indicate that the downlink speed is unknown or unspecified.	1-100	0 (unspecified)
`uplink-speed <speed>`	Use the **uplink <speed>** parameter to indicate the current WAN backhaul uplink speed in Kbps. If no value is set, this parameter will show a default value of 0 to indicate that the uplink speed is unknown or unspecified.	0 - 2,147,483,647 kbps	0 (unspecified)
`wan-metrics-link-status`	Define the status of the WAN Link by configuring one of the following values. The default link status is **reserved**, which indicates that the link status is unknown or unspecified.	■ link_down ■ link_test ■ link_up ■ reserved	reserved
`link_down`	WAN link is down.	—	—
`link_test`	WAN link is currently in a test state.	—	—
`link_up`	WAN link is up.	—	—
`reserved`	This parameter is reserved by the Hotspot 2.0 specification, and cannot be configured. This is the default link status.	—	—

Usage Guidelines

The values configured in this profile can be sent in an ANQP IE to provide hotspot clients information about access network characteristics such as link status and the capacity and speed of the WAN link to the Internet.Issue this command without the **<profile-name>** parameter to display the entire WAN metrics profile list, including profile status and the number of references to each profile. Include a profile name to display detailed configuration information for that profile.

Examples

The example below shows that three WAN metrics profiles are configured. The **References** column lists the number of other profiles with references to the operator-friendly name profile, and the **Profile Status** column indicates whether the profile is predefined. User-defined profiles will not have an entry in the **Profile Status** column.

```
(host) [md] #show wlan hotspot h2qp-wan-metrics-profile
H2QP WAN Metrics Profile List
-----------------------------
Name          References  Profile Status
----          ----------  --------------
default       0
WanFastlink

Total:1
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan hotspot hs2-profile

```
wlan hotspot hs2-profile <profile-name>
   access-network-type {emergency-services|personal-device|private|private-guest|public-
   chargeable|public-free|test|wildcard}
   advertisement-profile <profile-name>
   advertisement-protocol {anqp|eas|mih-cmd-event|mih-info|rsvd}
   asra
   clone <source>
   comeback-mode
   gas-comeback-delay <gas-comeback-delay>
   grp-frame-block
   hessid <hessid>
   hotspot-enable
   hotspot-roam-cons-1
   hotspot-roam-cons-2
   hotspot-roam-cons-3
   internet
   no
   p2p-cross-connect
   p2p-dev-mgmt
   pame-bi
   query-response-length-limit <query-response-length-limit>
   radius-cui
   radius-loc-data
   release-number {release-1|release-2|reserved}
   time-advt-cap {no-std-ext-timesrc|timestamp-offset-utc|reserved}
   time-error <milliseconds>
   time-zone <time-zone>
   venue-group <venue-group>
   venue-type <venue-type>
```

Description

This command configures a hotspot profile for an 802.11u public access service provider.

Syntax

Parameter	Description
`<profile-name>`	Name of the hotspot profile.
`access-network-type`	Specifies the 802.11u network type. The default setting is **public-chargeable.** ■ **emergency-services**: emergency services only network ■ **personal-device**: personal device network ■ **private**: private network ■ **private-guest**: private network with guest access ■ **public-chargeable**: public chargeable network ■ **public-free**: free public network ■ **test**: test network ■ **wildcard**: wildcard network
`advertisement-profile <profile-name>`	Advertisement profile associated with this hotspot profile. If this parameter is not changed, the hotspot profile uses with the **default** advertisement profile.

Parameter	Description
`advertisement-protocol`	Select one of the following advertisement protocol types to be used by the AP. ■ **anqp** ■ **emergency**: Emergency Alert System ■ **mih-cmd-event**: Media Independent Handover Command and Event Services Capability Discovery ■ **mih-info**: Media Independent Handover Information Service. This option allows handovers between differing kinds of wireless access protocols and technologies, allowing access points on different IP subnets to communicate with each other at the link level while maintaining session continuity. ■ **rsvd**: Reserved for future use.
`asra`	Issue the Additional Steps Required for Access (ASRA) sub command if any additional steps are required for network access. If this parameter is enabled, the AP will send the following IEs in response to the client's ANQP query. ■ Venue Name ■ Domain Name List ■ Network Authentication Type ■ Roaming Consortium List ■ NAI Realm List **NOTE:** If ASRA is enabled, the advertisement profile for this hotspot must reference an enabled network authentication type profile. For more information on enabling an network authentication type profile, see wlan hotspot anqp-nwk-auth-profile on page 2605.
`clone <source>`	Makes a copy of an existing hotspot profile.
`comeback-mode`	By default, ANQP information is obtained from a GAS Request and Response. If you enable the comeback-mode option, advertisement information is obtained using a GAS Request and Response. as well as a Comeback-Request and Comeback-Response. This option is disabled by default.
`gas-comeback-delay <gas-comeback-delay>`	At the end of the GAS comeback delay interval, the client may attempt to retrieve the query response using a Comeback Request Action frame. The supported range is 100-2000 milliseconds, and the default value is 500 milliseconds.
`grp-frame-block`	This option configures the Downstream Group Addressed Forwarding Disabled Mode. If this feature is enabled, it ensures that the AP does not forward downstream group-addressed frames. It is disabled by default, allowing the AP to forward downstram group-addressed frames.
`hessid <hessid>`	This optional parameter devices an AP's homogenous ESS identifier, which is that device's MAC address in colon-separated hexadecimal format.
`hotspot-enable`	Enables or disables the hotspot. When this feature is enabled, the Information Elements (IEs) for this hotspot are included in beacons and probe responses from the AP. This setting is disabled by default.
`hotspot-roam-cons-1`	Roaming Consortium entry 1 OI value and length.

Parameter	Description
`hotspot-roam-cons-2`	Roaming Consortium entry 2 OI value and length.
`hotspot-roam-cons-3`	Roaming Consortium entry 3 OI value and length.
`internet`	If you issue the **internet** parameter, the AP sends an IE indicating that the network allows internet access. By default, a hotspot profile does not advertise network internet access.
`no`	Negates or removes any configured parameter.
`p2p-cross-connect`	Issue this command to advertise support for P2P Cross Connections. This setting is disabled by default.
`p2p-dev-mgmt`	Issue this command to advertise support for P2P device management. This setting is disabled by default.
`pame-bi`	This option enables the Pre-Association Message Exchange BSSID Independent (PAME-BI) bit, which is used by an AP to indicate whether the AP indicates that the Advertisement Server can return a query response that is independent of the BSSID used for the GAS Frame exchange.
`query-response-length-limit <query-response-length-limit>`	GAS enables advertisement services that lets clients query multiple 802.11 neworks at once, while also allowing the client to learn more about a network's 802.11 infrastructure before associating. If a client transmits a GAS Query using a GAS Initial Request frame, the responding AP will provide the query response (or information on how to receive the query response) in a GAS Initial Response frame. This parameter sets the maximum length of the GAS query response, in octets. The supported range is 1-255 octets.
`radius-cui`	Include this parameter to enable the Chargeable-User-Identity RADIUS attribute defined by RFC 4372. Home networks can use this attribute to identify a user for the roaming transactions that take place outside of that home network.
`radius-loc-data`	Include this parameter to enable the Location Data RADIUS attribute defined by RFC 5580. Enabling this parameter allows the RADIUS server to use location data.
`release number`	Hotspot 2.0 Release Number: ■ Release #1 ■ Release #2 ■ Reserved

`time-advt-cap`
`no-std-ext-timesrc`
`timestamp-offset-utc`
`reserved`
	This parameter specifies the AP's source of external time, and the current condition of its timing estimator.
	■ **no-std-ext-time-src**: The AP using this profile has no standardized external time source.
	■ **timestamp-offset-utc**: The AP has a timestamp offset based on UTC.
	■ **reserved**: This setting is reserved for future use, and should not be used.

Parameter	Description
`time-error`	The standard deviation of error in time value estimate, in milliseconds. The default value is 0 milliseconds, and the supported range is 0- 2,147,483,647 milliseconds.
`time-zone`	The time zone in which the AP is operating, in the format `<std><offset>[dst[offset][,start[/time],end[/time]]` Where the <std> string specifies the abbreviation of the time zone, **<dst>** is the abbreviation of the timezone in daylight savings time, and the **<offset>** string specifies the time value you must add to the local time to arrive at UTC. **NOTE:** For complete details on configuring the timezone format, refer to section 8.3 of IEEE Std 1003.1, 2004 Edition.
`venue-group <venue-group>`	Specify one of the following venue groups to be advertised in the IEs from APs associated with this hotspot profile. The default setting is **unspecified**. ■ assembly ■ business ■ educational ■ factory-or-industrial ■ institutional ■ mercantile ■ outdoor ■ reserved ■ residential ■ storage ■ unspecified ■ utility-misc ■ vehicular **NOTE:** This parameter only defines the venue group advertised in the IEs from hotspot APs. To define the venue group to be included in ANQP responses, use anqp-venue-name-profile <profile-name>.
`venue-type <venue-type>`	Specify a venue type to be advertised in the IEs from APs associated with this hotspot profile. The complete list of supported venue types is described in Venue Types on page 2625 **NOTE:** This parameter only defines the venue type advertised in the IEs from hotspot APs. To define the venue type to be included in ANQP responses, use anqp-venue-name-profile <profile-name>.

Usage Guidelines

Hotspot 2.0 is a WFA specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

Mobility Master supports Hotspot 2.0 with enhanced network discovery and selection. Clients can receive general information about the network identity, venue and type via management frames from the Aruba AP. Clients can also query APs for information about the network's available IP address type (IPv4 or IPv6), roaming partners, and supported authentication methods, and receive that information in Information Elements from the AP.

Generic Advertisement Service Queries

An Organization Identifier is a unique identifier assigned to a service provider when it registers with the IEEE registration authority. An AP can include its service provider OI in beacons and probe responses to clients. If a client recognizes an AP's OI, it will attempt to associate to that AP using the security credentials corresponding to that service provider.

If the client does *not* recognize the AP's OI, that client can send a GAS query to the AP to request more information more about the network before associating.

ANQP Information Elements

ANQP IEs are additional data that can be sent from the AP to the client to identify the AP's network and service provider. If a client requests this information via a GAS query, the hotspot AP then sends the ANQP Capability list in the GAS Initial Response frame indicating support for the following IEs:

- **Venue Name**: defined using the wlan hotspot anqp-venue-name-profile command.
- **Domain Name**: defined using the wlan hotspot anqp-domain-name-profile command.
- **Network Authentication Type**: defined using the wlan hotspot anqp-nwk-auth-profile command.
- **Roaming Consortium List**: defined using the wlan hotspot anqp-roam-cons-profile command.
- **NAI Realm**: defined using the wlan hotspot anqp-nai-realm-profile command.
- **Cellular Network Data**: defined using the wlan hotspot anqp-3gpp-nwk-profile command.
- **Connection Capability**: defined using the wlan hotspot h2qp-conn-capability-profile command.
- **Operator Class**: defined using the wlan hotspot h2qp-op-cl-profile command.
- **Operator Friendly Name**: defined using the wlan hotspot h2qp-operator-friendly-name-profile command.
- **WAN Metrics**: defined using the wlan hotspot h2qp-wan-metrics-profile.

Roaming Consortium OIs

Organization Identifiers (OIs) are assigned to service providers when they register with the IEEE registration authority. You can specify the OI for the hotspot's service provider in the ANQP Roaming Consortium profile using the wlan hotspot anqp-roam-cons-profile command. This Hotspot profile also allows you to define and send up to three additional roaming consortium OIs for the service provider's top three roaming partners. To send this additional data to clients, you must specify the number of roaming consortium elements a client can query using the **addtl-roam-cons-ois <1-3>** parameter, then define those elements using the following parameters:

- **roam-cons-oi-1** and **roam-cons-len 1**
- **roam-cons-oi-2** and **roam-cons-len 2**
- **roam-cons-oi-3** and **roam-cons-len 3**

The configurable values for each additional OI include the Organization Identifier itself, the OI length, and the venue group and venue type associated with those OIs.

Venue Types

The following list describes the different venue types that may be configured in a hotspot profile:

■ assembly-amphitheatre ■ assembly-amusement-park ■ assembly-arena ■ assembly-bar ■ assembly-coffee-shop ■ assembly-convention-center ■ assembly-emer-coord-center ■ assembly-library ■ assembly-musuem ■ assembly-passenger-terminal ■ assembly-restaurant ■ assembly-stadium ■ assembly-theater ■ assembly-worship-place ■ assembly-zoo ■ business-attorney ■ business-bank ■ business-doctor	■ business-fire-station ■ business-police-station ■ business-post-office ■ business-professional-office ■ business-research-and-development ■ educational-primary-school ■ educational-secondary-school ■ educational-university ■ industrial-factory ■ institutional-alcohol-or-drug-rehab ■ institutional-group-home ■ institutional-hospital ■ institutional-prison ■ institutional-terminal-care ■ mercantile-automotive-service-station ■ mercantile-gas-station ■ mercantile-grocery ■ mercantile-retail	■ mercantile-shopping-mall ■ outdoor-bus-stop ■ outdoor-city-park ■ outdoor-kiosk ■ outdoor-muni-mesh-nwk ■ outdoor-rest-area ■ outdoor-traffic-control ■ residential-boarding-house ■ residential-dormitory ■ residential-hotel ■ residential-private-residence ■ unspecified ■ vehicular-airplane ■ vehicular-automobile ■ vehicular-bus ■ vehicular-ferry ■ vehicular-motor-bike ■ vehicular-ship ■ vehicular-train

Example

The following command configures a hotspot profile with one additional roaming consortium OI for the service provider's top roaming partner:

```
(host) [md] (config) #wlan hotspot hs2-profile profile2
(host) [md] (Hotspot 2.0 Profile "profile2") #venue-group mercantile(host) [md] (Hotspot 2.0
Profile "profile2") #venue-type mercantile-shopping-mall
(host) [md] (Hotspot 2.0 Profile "profile2") #addtl-roam-cons-ois
(host) [md] (Hotspot 2.0 Profile "profile2") #roam-cons-len 3
(host) [md] (Hotspot 2.0 Profile "profile2") #roam-cons-oi1 415B8C
{host) [md] (Hotspot 2.0 Profile "profile2") #hotspot-enable
```

Related Commands

Use the following commands to configure the Hotspot feature:

Command	Description
wlan hotspot anqp-3gpp-nwk-profile	This profile defines information for a 3GPP Cellular Network for hotspots that have roaming relationships with cellular operators
wlan hotspot anqp-domain-name-profile	This command defines the domain name to be sent in an ANQP information element in a GAS query response.
wlan hotspot anqp-ip-addr-avail-profile	This command defines available IP address types to be sent in an ANQP information element in a GAS query response.
wlan hotspot anqp-nai-realm-profile	This command defines a Network Access Identifier realm whose information can be sent as an ANQP information element in a GAS query response
wlan hotspot anqp-nwk-auth-profile	This command configures an ANQP Network Authentication profile to define authentication type being used by the hotspot network.
wlan hotspot anqp-roam-cons-profile	This command configures the Roaming Consortium OI information to be sent in an ANQP information element in a GAS query response
wlan hotspot anqp-venue-name-profile	This command defines venue information be sent in an ANQP information element in a GAS query response.
wlan hotspot h2qp-conn-capability-profile	Defines a H2QP profile that advertises hotspot protocol and port capabilities.
wlan hotspot h2qp-op-cl-profile	Defines a H2QP profile that defines the Operating Class to be sent in the ANQP IE.
wlan hotspot h2qp-operator-friendly-name-profile	Defines a H2QP operator-friendly name profile.
wlan hotspot h2qp-wan-metrics-profile	Creates a H2QP profile that specifies the hotspot WAN status and link metrics.
wlan hotspot hs2-profile	This command configures a hotspot profile for an 802.11u public access service provider.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan ht-ssid-profile

```
wlan ht-ssid-profile <profile-name>
   40MHz-enable
   80MHz-enable
   ba-amsdu-enable
   clone <profile-name>
   high-throughput-enable
   ldpc
   legacy-stations
   max-rx-a-mpdu-size {8191|16383|32767|65535}
   max-tx-a-mpdu-size <bytes>
   max-tx-a-msdu-count-be {0-15}
   max-tx-a-msdu-count-bk {0-15}
   max-tx-a-msdu-count-vi {0-15}
   max-tx-a-msdu-count-vo {0-15}
   max-vht-mpdu-size
   min-mpdu-start-spacing {0|.25|.5|1|2|4|8|16}
   mpdu-agg
   no...
   short-guard-intvl-20MHz
   short-guard-intvl-40MHz
   short-guard-intvl-80MHz
   stbc-rx-streams
   stbc-tx-streams
   supported-mcs-set <mcs-list>
   temporal-diversity
   very-high-throughput-enable
   vht-mu-txbf-enable
   vht-supported-mcs-map
   vht-txbf-explicit-enable
   vht-txbf-sounding-interval
```

Description

This command configures a high-throughput SSID profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`40MHz-enable`	Enables or disables the use of this high-throughput SSID in 40 MHz mode.	—	enabled
`80MHz-enable`	Enables or disables the use of 80 MHz channels on VHT APs.	—	enabled
`ba-amsdu-enable`	Enables or disables Receive AMSDU in Block ACK (BA) negotiation. If enabled, AP denies clients from sending AMSDU using BA agreement.	—	enabled

Parameter	Description	Range	Default
clone	Name of an existing high-throughput SSID profile from which parameter values are copied.	—	—
high-throughput-enable	Enables or disables high-throughput SSID to allow high-throughput (802.11n) stations to associate. Enabling high-throughput in an ht-ssid-profile enables WMM base features for the associated SSID.	—	enabled
ldpc	If enabled, the AP will advertise LDPC support. LDPC improves data transmission over radio channels with high levels of background noise.	—	enabled
legacy-stations	Controls whether or not legacy (non-HT) stations are allowed to associate with this SSID. By default, legacy stations are allowed to associate. This setting has no effect on a BSS in which HT support is not available.	—	enabled
max-rx-a-mpdu-size	Controls the maximum size, in bytes, of an A-MPDU that can be received on this high-throughput SSID.	8191 16383 32767 65535	65535
8191	Maximum size of 8191 bytes.	—	—
16383	Maximum size of 16383 bytes.	—	—
32767	Maximum size of 32767 bytes.	—	—
65535	Maximum size of 65535 bytes.	—	—
max-tx-a-mpdu-size	Controls the maximum size, in bytes, of an A-MPDU that can be sent on this high-throughput SSID.	1576-65535	65535
max-tx-a-masdu-count-be	Sets the maximum number of MSDUs in a TX A-MSDU on best effort AC. **NOTE:** In tunnel and decrypt-tunnel forwarding mode, TX A-MSDU is disabled if the value is set to 0. If the value is set to non-zero, TX A-MSDU is enabled and set to this value.	0-15	2
max-tx-a-masdu-count-bk	Sets the maximum number of MSDUs in a TX A-MSDU on background AC. **NOTE:** TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on background AC is disabled and assigning any value has no effect.	0-15	2

Parameter	Description	Range	Default
`max-tx-a-masdu-count-vi`	Sets the maximum number of MSDUs in a TX A-MSDU on video AC. **NOTE:** TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on video AC is disabled and assigning any value has no effect.	0-15	2
`max-tx-a-masdu-count-vo`	Sets the maximum number of MSDUs in a TX A-MSDU on voice AC. **NOTE:** TX A-MSDU is disabled if the value is set to 0. In decrypt-tunnel forwarding mode, TX A-MSDU on voice AC is disabled and assigning any value has no effect.	0-15	0
`max-vht-mpdu-size`	Maximum size of a VHT MPDU.	3895, 7991, or 11454 bytes	11454 bytes
`min-mpdu-start-spacing`	Minimum time between the start of adjacent MDPUs within an aggregate MDPU in microseconds.	0, .25, .5, 1, 2,4, 8,16	0
`0`	No restriction on MDPU start spacing.	—	—
`.25`	Minimum time of .25 µsec.	—	—
`.5`	Minimum time of .5 µsec.	—	—
`1`	Minimum time of 1 µsec.	—	—
`2`	Minimum time of 2 µsec.	—	—
`4`	Minimum time of 4 µsec.	—	—
`8`	Minimum time of 8 µsec.	—	—
`16`	Minimum time of 16 µsec.	—	—
`mpdu-agg`	Enables or disables MAC protocol data unit (MDPU) aggregation. High-throughput APs are able to send aggregated MDPUs, which allow an AP to receive a single block acknowledgment instead of multiple ACK signals. This option, which is enabled by default, reduces network traffic overhead by effectively eliminating the need to initiate a new transfer for every MPDU.	—	enabled
`no`	Negates any configured parameter.	—	—

Parameter	Description	Range	Default
`short-guard-intvl-20MHz`	Enables or disables use of short guard interval (400 ns) in 20 MHz mode. A guard interval is a period of time between transmissions that allows reflections from the previous data transmission to settle before an AP transmits data again. An AP identifies any signal content received inside this interval as unwanted inter-symbol interference, and rejects that data. The 802.11n standard specifies two guard intervals: 400 ns (short) and 800 ns (long). Enabling a short guard interval can decrease network overhead by reducing unnecessary idle time on each AP. Some outdoor deployments, may, however require a longer guard interval. If the short guard interval does not allow enough time for reflections to settle in your mesh deployment, inter-symbol interference values may increase and degrade throughput.	—	enabled
`short-guard-intvl-40MHz`	Enables or disables use of short guard interval (400 ns) in 40 MHz mode of operation.	—	enabled
`short-guard-intvl-80MHz`	Enables or disables use of short guard interval (400 ns) in 80 MHz mode of operation.	—	enabled
`stbc-rx-streams`	Control the maximum number of spatial streams usable for STBC reception. 0 disables STBC reception, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on the AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.) **NOTE:** If transmit beamforming is enabled, STBC will be disabled for beamformed frames.	0-1	1
`stbc-tx-streams`	Control the maximum number of spatial streams usable for STBC transmission. 0 disables STBC transmission, 1 uses STBC for MCS 0-7. Higher MCS values are not supported. (Supported on AP-105, 130 Series, and 170 Series only. The configured value will be adjusted based on AP capabilities.) **NOTE:** If transmit beamforming is enabled, STBC will be disabled for beamformed frames.	0-1	1

Parameter	Description	Range	Default
supported-mcs-set	A list of MCS values or ranges of values to be supported on this SSID. The MCS you choose determines the channel width (20 MHz vs. 40 MHz vs. 80 MHz) and the number of spatial streams used by the mesh node. To specify a smaller range of values, enter a hyphen between the lower and upper values. To specify a series of different values, separate each value with a comma. Examples: 2–10 1,3,6,9,12 MCS value of 16-23 are supported on 130 Series/RAP-155/11ac APs only. MCS value of 24-31 are supported on 320 Series APs only.	0-31	0-31
temporal-diversity	Enable or disable temporal diversity. When this setting is enabled and the client is not responding to 802.11 packets, the AP will launch two hardware retries; if the hardware retries are not successful then it attempts software retries.	—	disabled
very-high-throughput-enable	Enable or disable support for VHT (802.11ac) on the SSID.	—	enabled
vht-mu-txbf-enable	Enable or disable VHT Multi-User Transmit Beamforming. If this parameter is disabled, all other Multi-User Transmit Beamforming configuration parameters have no effect. **NOTE:** This parameter is applicable for 320 Series APs only.	—	enabled
vht-supported-mcs-map	Comma separated list of maximum supported MCS for spatial streams 1 through 4. Valid values for maximum MCS are 7, 8, 9, and '-' (if spatial stream is not supported). Maximum MCS of a spatial stream cannot be higher than the previous streams. If an MCS is not valid for a particular combination of bandwidth and number of spatial streams, it will not be used for Tx and Rx.	7, 8, 9, or -	9,9,9,9
vht-txbf-explicit-enable	Enable or disable VHT Explicit Transmit Beamforming for the 802.11ac-capable APs. When this feature is enabled, the AP requests information about the MIMO channel and uses that information to transmit data over multiple transmit streams using a calculated steering matrix. The result is higher throughput due to improved signal at the beamformee (the receiving client). If this parameter is disabled, all other transmit beamforming settings will not take effect.	—	Enabled

Parameter	Description	Range	Default
`vht-txbf-sounding-interval`	Time interval in milliseconds between channel information updates between the AP and the beamformee client. **NOTE:** This is applicable for 802.11ac-capable APs only.	1-1000 msec	25 msec

Usage Guidelines

The ht-ssid profile configures the high-throughput SSID. Stations are not allowed to use HT with TKIP stand-alone encryption, although TKIP can be provided in mixed-mode BSSIDs that support HT. HT is disabled on a BSSID if the encryption mode is stand-alone TKIP or WEP.

You can also use this profile to configure explicit transmit beamforming for 130 Series access points. When this feature is enabled, the AP coordinates the signals sent from each antenna so the signals focus on the receiver, improving radio range and performance. The 130 Series AP can advertise transmit beamforming capabilities in beacon, probe response and association responses in the HT capabilities IE, then use the compressed or noncompressed beamforming report from clients to form a steering matrix. The AP ensures that the steering matrix stays current by updating and recalibrating the steering matrix at regular intervals.

By default, 130 Series access points support both compressed and non-compressed steering information from clients. If you have many clients that can send only non-compressed steering reports, best practices are to retain the default settings, allowing the AP to support both types of steering reports. If all (or nearly all) of the AP's clients are capable of sending compressed steering reports, best practices are to disable non-compressed steering in the AP's HT SSID profile.

De-aggregation of MSDUs is supported with a maximum frame transmission size of 4 KBs; however, this feature is always enabled and is not configurable. Aggregation is not currently supported.

Example

The following command configures the maximum size of a received aggregate MDPU to be 8191 bytes for the high-throughput SSID named htcorpnet:

```
(host) [md] (config) #wlan ht-ssid-profile htcorpnet
(host) [md] (High-throughput SSID profile "htcorpnet") #max-rx-a-mpdu-size 8191
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms, but only operates with 802.11n-capable APs. The following parameters are supported on 802.11ac-capable APs only: ■ **80-MHz-enable** ■ **very-high-throughput-enable** ■ **vht-supported-mcs-map** ■ **vht-txbf-explicit-enable** ■ **vht-txbf-sounding-interval**	Base operating system.	Config mode on Mobility Master.

wlan rrm-ie-profile

```
wlan rrm-ie-profile <profile-name>
   bss-aac-ie
   clone
   country-ie
   enabled-capabilities-ie
   no
   pwr-constraint-ie
   qbss-load-ie
   quiet-ie
   tpc-report-ie
```

Description

This command configures a radio resource management (RRM) IE profile to define the information elements advertised by an AP with 802.11k support enabled.

Syntax

Parameter	Description
`bss-aac-ie`	The AP will advertise in beacon and probe responses the BSS Available Admission Capacity IE, which contains information about the admission capabilities for each User Priority or AC.
`clone`	Copy the settings of an existing RRM IE profile.
`country-ie`	The AP will advertise in beacon and probe responses the device's regulatory domain.
`enabled-capabilities-ie`	The AP will advertise in beacon and probe responses support for radio measurements in a device.
`no ...`	Disables the transmission of an IE in this profile.
`pwr-constraint-ie`	The AP will advertise in beacon and probe responses the regulatory maximum transmit power for that current channel.
`qbss-load-ie`	The AP will advertise in beacon and probe responses the QBSS Load IE, which contains information on the current station count, channel utilization and available admission capacity levels in the QBSS.
`quiet-ie`	The AP will advertise in beacon and probe responses the Quiet IE, which is used to silence the channel for measurement purposes. When an AP uses a quiet IE to schedule a quiet interval, stations may not transmit on that channel during the quiet interval.
`tpc-report-ie`	The AP will advertise in beacon and probe responses information about its TCP.

Usage Guidelines

ArubaOS supports RRM IEs for APs with 802.11k support enabled. All IEs are sent by default.

Example

The following command prevents the AP from advertising the country IE:

```
(host) [md] (config) #wlan rrm-ie-profile default
```

```
(host) [md] (RRM IE Profile "default") #no country-ie
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

wlan ssid-profile

```
wlan ssid-profile <profile-name>
   a-basic-rates <mbps>
   a-beacon-rate
   a-tx-rates <mbps>
   advertise-ap-name
   advertise-location
   ageout <seconds>
   auth-req-thresh <auth-req-thresh>
   battery-boost
   clone <profile-name>
   deny-bcast
   disable-probe-retry
   dot11r-profile
   dtim-period <milliseconds>
   eapol-rate-opt
   edca-parameters-profile {ap|station} <profile-name>
   enforce-user-vlan
   essid <name>
   g-basic-rates <mbps>
   g-beacon-rate
   g-tx-rates <mbps>
   hide-ssid
   ht-ssid-profile <profile-name>
   local-probe-req-thresh
   max-clients <number>
   max-retries <number>
   max-tx-fail <number>
   mcast-rate-opt
   mfp-capable
   mfp-required
   multicast-rate
   no ...
   okc
   opmode {bSec-128|bSec-256|dynamic-wep|opensystem|static-wep|wpa-aes|wpa-psk-aes|wpa-psk-
   tkip|wpa-tkip|wpa2-aes|wpa2-psk-aes|wpa2-psk-tkip|wpa2-tkip|xSec}
   qbss-load-enable
   rts-threshold <number>
   short-preamble
   ssid-enable
   strict-svp
   wepkey1 <key>
   wepkey2 <key>
   wepkey3 <key>
   wepkey4 <key>
   weptxkey <index>
   wmm
   wmm-be-dscp <best-effort>
   wmm-bk-dscp <background>
   wmm-ts-min-inact-int <milliseconds>
   wmm-uapsd
   wmm-vi-dscp <video>
   wmm-vo-dscp <voice>
   wpa-hexkey <psk>
   wpa-passphrase <string>
```

Description

This command configures an SSID profile.

Syntax

	Description	Range	Default
`<profile-name>`	Name of this instance of the profile. The name must be 1-63 characters.	—	“default”
`a-basic-rates`	List of supported 802.11a rates, in Mbps, that are advertised in beacon frames and probe responses.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 12, 24 Mbps
`a-beacon-rate`	Sets the beacon rate for 802.11a (use for DAS only). Using this parameter in normal operation may cause connectivity problems.	default, 6, 9, 12, 18,24,36,48,54 Mbps	minimum valid rate
`a-tx-rates`	Set of 802.11a rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error or loss rate of the client.	6, 9, 12, 18, 24, 36, 48, 54 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps
`advertise-ap-name`	If enabled, APs that are part of this VAP will broadcast the AP Name information in the beacons frames.	—	—
`advertise-location`	If enabled, APs that are part of this VAP will broadcast their GPS coordinates in the beacons and probe response frames as part of a vendor-specific Information Element.	—	disabled
`ageout`	Time, in seconds, that a client is allowed to remain idle before being aged out.		1000 seconds
`auth-req-thresh`	The SNR threshold below which incoming authentication requests are ignored. Use this parameter instead of the local probe request threshold parameter to filter out low SNR authentication request. **NOTE:** Use this parameter with caution. Consult technical support before configuring this parameter.	0-100 dB	0 dB
`battery-boost`	Converts multicast traffic to unicast before delivery to the client, thus allowing you to set a longer DTIM interval. The longer interval keeps associated wireless clients from activating their radios for multicast indication and delivery, leaving them in power-save mode longer and thus lengthening battery life. **NOTE:** This parameter requires the PEFNG license. This parameter should not be enabled if you plan on using the Push-To-Talk feature for Polycom SpectraLink devices.	—	disabled

	Description	Range	Default
clone	Name of an existing SSID profile from which parameter values are copied.	—	—
deny-bcast	When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls whether or not the system responds for this SSID. When enabled, no response is sent and clients have to know the SSID in order to associate to the SSID. When disabled, a probe response frame is sent for this SSID.	—	disabled
disable-probe-retry	Enables or disables battery MAC level retries for probe response frames. By default this parameter is enabled, which mean that MAC level retries for probe response frames is disabled. **NOTE:** This parameter is not supported for 200 Series, 210 Series, 220 Series, 270 Series access points.		enabled
dot11r-profile	Associates the dot11r-profile with the SSID profile.	—	—
dtim-period	Specifies the interval, in milliseconds, between the sending of DTIMs in the beacon. This is the maximum number of beacon cycles before unacknowledged network broadcasts are flushed. When using wireless clients that employ power management features to sleep, the client must revive at least once during the DTIM period to receive broadcasts.		1
eapol-rate-opt	Uses a more conservative rate for more reliable delivery of EAPOL frames.	—	enabled
edca-parameters-profile	Name of the EDCA profile that applies to this SSID. **NOTE:** This parameter requires the PEFNG license. Configure this parameter only under the guidance of your Aruba representative.	—	—
ap|station	Assigns the specified EDCA profile to AP or station (client).	—	—
enforce-user-vlan	Enforces data traffic only in user's assigned vlan (Open stations only).	—	—
essid	Name that uniquely identifies a wireless network. The ESSID can be up to 32 characters. If the ESSID includes spaces, you must enclose it in quotation marks.	—	aruba-ap
g-basic-rates	List of supported 802.11b/g rates that are advertised in beacon frames and probe responses.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2 Mbps

	Description	Range	Default
g-beacon-rate	Sets the beacon rate for 802.11g (use for DAS only). Using this parameter in normal operation may cause connectivity problems.	default, 1,2,5, 6 9, 11, 12, 18, 24, 36, 48, 54 Mbps	minimum valid rate
g-tx-rates	Set of 802.11b/g rates at which the AP is allowed to send data. The actual transmit rate depends on what the client is able to handle, based on information sent at the time of association and on the current error or loss rate of the client.	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
hide-ssid	Enables or disables hiding of the SSID name in beacon frames. Note that hiding the SSID does very little to increase security.	—	disabled
ht-ssid-profile	Name of high-throughput SSID profile to use for configuring high-throughput support. See wlan ht-ssid-profile on page 2628.	—	"default"
local-probe-req-thresh	APs will not respond to client probe requests if the SNR value in the probe request is less than the specified threshold value.	0-100 dB	0 dB
max-clients	Maximum number of wireless clients for the AP. This parameter is limited to 255 clients per radio.	0-255	64
max-retries	Maximum number of retries allowed for the AP to send a frame.	0-15	4
max-tx-fail	The AP assumes the client has left and should be deauthorized when the AP detects this number of consecutive frames were not delivered because the **max-retries** threshold was exceeded.	0 - 2,147,483,647	0
mcast-rate-opt	Enables or disables scanning of all active stations currently associated to an AP to select the lowest transmission rate for broadcast and multicast frames. This option only applies to broadcast and multicast data frames; 802.11 management frames are transmitted at the lowest configured rate. **NOTE:** Do not enable this parameter unless instructed to do so by your Aruba technical support representative.	—	disabled
mfp-capable	When enabled, the SSID supports management frame protection (MFP) capable clients and traditional clients.	—	disabled
mfp-required	When enabled, the SSID only supports MFP capable clients.	—	disabled

	Description	Range	Default
multicast-rate	When configured, the Mobility Master chooses the rate for video multicast frames. You can configure MCS rates as well. MCS is an important setting because it provides for potentially greater throughput. **NOTE:** The following information displays the MCS rate if the **short-guard-intvl-20MHz** parameter in **ht-ssid-profile** is either enabled or disabled: MCS Streams 20 MHz 20 MHz SGI --- ------- ------ ---------- 0 1 6.5 7.2 1 1 13.0 14.4 2 1 19.5 21.7 3 1 26.0 28.9 4 1 39.0 43.3 5 1 52.0 57.8 6 1 58.5 65.0 7 1 65.0 72.2 8 2 13.0 14.4 9 2 26.0 28.9 10 2 39.0 43.3 11 2 52.0 57.8 12 2 78.0 86.7 13 2 104.0 115.6 14 2 117.0 130.0 15 2 130.0 144.4 **NOTE:** The MCS rates for video multicast are supported in all 802.11n -capable APs. This is not supported in 320 Series AP.	default, 6, 9, 12, 18, 24, 36, 48, 54 Mbps mcs0-mcs15	default
multiple-tx-replay-co	Enables Multiple Tx Replay Counters.	—	—
no	Negates any configured parameter.	—	—
okc	OKC is a similar technique, not defined by 802.11i, available for authentication between multiple APs in a network where those APs are under common administrative control. An Aruba deployment with multiple APs under the control of a single controller is one such example. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.	—	Enabled
opmode	The layer-2 authentication and encryption to be used on this ESSID to protect access and ensure the privacy of the data transmitted to and from the network.	—	opensystem
bSec-128	WPA2 with AES GCM-128 encryption and dynamic keys using 802.1X	—	—
bSec-256	WPA2 with AES GCM-256 encryption and dynamic keys using 802.1X	—	—

	Description	Range	Default
dynamic-wep	WEP with dynamic keys.	—	—
opensystem	No authentication and encryption.	—	—
static-wep	WEP with static keys.	—	—
wpa-aes	WPA with AES encryption and dynamic keys using 802.1X.	—	—
wpa-psk-aes	WPA with AES encryption using a preshared key.	—	—
wpa-psk-tkip	WPA with TKIP encryption using a preshared key.	—	—
wpa-tkip	WPA with TKIP encryption and dynamic keys using 802.1X.	—	—
wpa2-aes	WPA2 with AES encryption and dynamic keys using 802.1X.	—	—
wpa2-psk-aes	WPA2 with AES encryption using a preshared key.	—	—
wpa2-psk-tkip	WPA2 with TKIP encryption using a preshared key.	—	—
wpa2-tkip	WPA2 with TKIP encryption and dynamic keys using 802.1X.	—	—
wpa-psk-aes	WPA with AES encryption using a preshared key.	—	—
wpa2-psk-tkip	WPA2 with TKIP encryption using a preshared key.	—	—
wpa2-tkip	WPA2 with TKIP encryption and dynamic keys using 802.1X.	—	—
xSec	Encryption and tunneling of Layer-2 traffic between the managed device and wired or wireless clients, or between managed devices. To use xSec encryption, you must use a RADIUS authentication server. For clients, you must install the Funk Odyssey client software. Requires installation of the xSec license. For xSec between managed devices, you must install an xSec license in each managed device.	—	—

	Description	Range	Default
qbss-load-enable	Enables the AP to advertise the QBSS load element. The element includes the following parameters that provide information on the traffic situation: ■ **Station count**: The total number of stations associated to the QBSS. ■ **Channel utilization**: The percentage of time (normalized to 255) the channel is sensed to be busy. The access point uses either the physical or the virtual carrier sense mechanism to sense a busy channel. ■ **Available admission capacity**: The remaining amount of medium time (measured as number of 32us/s) available for a station via explicit admission control. The QAP uses these parameters to decide whether to accept an admission control request. A wireless station uses these parameters to choose the appropriate access points. **NOTE:** Ensure that wmm is enabled for legacy APs to advertise the QBSS load element. For 802.11n APs, ensure that either wmm or high throughput is enabled.	—	disabled
rts-threshold	Wireless clients transmitting frames larger than this threshold must issue RTS and wait for the AP to respond with CTS. This helps prevent mid-air collisions for wireless clients that are not within wireless peer range and cannot detect when other wireless clients are transmitting.		2333 bytes
short-preamble	Enables or disables short preamble for 802.11b/g radios. Network performance may be higher when short preamble is enabled. In mixed radio environments, some 802.11b wireless client stations may experience difficulty associating with the AP using short preamble. To use only long preamble, disable short preamble. Legacy client devices that use only long preamble generally can be updated to support short preamble.	—	enabled
ssid-enable	Enables or disables this SSID.	—	enabled
strict-svp	Enable Strict Spectralink Voice Protocol (SVP)	—	disabled
wepkey1 - wepkey4	Static WEP key associated with the key index. Can be 10 or 26 hex characters in length.	—	—
weptxkey	Key index that specifies which static WEP key is to be used. Can be 1, 2, 3, or 4.	1, 2, 3, 4	1

	Description	Range	Default
wmm	Enables or disables WMM, also known as IEEE 802.11e Enhanced Distribution Coordination Function. WMM provides prioritization of specific traffic relative to other traffic in the network.	—	disabled
wmm-be-dscp	DSCP value used to map WMM best-effort traffic.	0-63	—
wmm-bk-dscp	DSCP used to map WMM background traffic.	0-63	—
wmm-ts-min-inact-int	Specifies the minimum inactivity time-out threshold of WMM traffic. This setting is useful in environments where low inactivity interval time-outs are advertised, which may cause unwanted timeouts.	0-3,600,000	0 milliseconds
wmm-uapsd	Enable WMM UAPSD powersave.	—	enabled
wmm-vi-dscp	DSCP used to map WMM video traffic.	0-63	—
wmm-vo-dscp	DSCP used to map WMM voice traffic.	0-63	—
wpa-hexkey	WPA PSK.	—	—
wpa-passphrase	WPA passphrase with which to generate a PSK.	—	—

Usage Guidelines

The SSID profile configures the SSID. Default WMM mappings exist for all SSIDs. After you customize an WMM mapping and apply it to the SSID, the Mobility Master overwrites the default mapping values and uses the user-configured values.

Suite-B Cryptography

The **opmode** parameters for Suite-B encryption, **wpa2-aes-gcm-128** and **wpa2-aes-gcm-256**, require the ACR license. All 7000 Series and 7200 Series support Suite-B encryption.

Multicast Rate Optimization

The Multicast Rate Optimization feature dynamically selects the rate for sending broadcast/multicast frames on any BSS. This feature determines the optimal rate for sending broadcast and multicast frames based on the lowest of the unicast rates across all associated clients.

When the Multicast Rate Optimization option (mcast-rate-opt) is enabled, the Mobility Master scans the list of all associated stations in that BSS and finds the lowest transmission rate as indicated by the rate adaptation state for each station. If there are no associated stations in the BSS, it selects the lowest configured rate as the transmission rate for broadcast and multicast frames.

This feature is disabled by default. Multicast Rate Optimization applies to broadcast and multicast frames only. 802.11 management frames are not affected by this feature and will be transmitted at the lowest configured rate.

The Multicast Rate Optimization feature should only be enabled on a BSS where all associated stations are sending or receiving unicast data. If there is no unicast data to or from a particular station, then the rate adaptation state may not accurately reflect the current sustainable transmission rate for that station. This could result in a higher packet error rate for broadcast or multicast packets at that station.

Example

The following command configures an SSID for WPA2 AES authentication:

```
(host) [md] (config) #wlan ssid-profile corpnet
(host) [md] (SSID Profile "corpnet") #essid Corpnet
(host) [md] (SSID Profile "corpnet") #opmode wpa2-aes
```

Command History

Release	Description
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	Licensing	Command Mode
All platforms, except for the noted **opmode** parameters.	Base operating system, except for the noted parameters.	Config mode on Mobility Master.

wlan traffic-management-profile

```
wlan traffic-management-profile <profile-name>
   bw-alloc virtual-ap <virtual-ap> share <percent>
   clone <profile-name>
   no ...
   report-interval <minutes>
   shaping-policy default-access|fair-access|preferred-access
```

Description

This command configures a traffic management profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this profile. The name must be 1-63 characters.	—	default
`bw-alloc`	Minimum bandwidth, as a percentage of available bandwidth, allocated to a Virtual AP when there is congestion on the wireless network. An virtual AP can use all available bandwidth if no other virtual APs are active.		
`virtual-ap <virtual-ap>`	Name of the virtual AP to which you will allocate a share of bandwidth.	—	—
`share <percent>`	Percentage of available bandwidth allocated to this virtual AP.	0-100	—
`clone <profile-name>`	Name of an existing traffic management profile from which parameter values are copied.	—	—
`no`	Negates any configured parameter.	—	—
`report-interval <minutes>`	Number of minutes between bandwidth usage reports.	1 - 999999 minutes	5 minutes

Parameter	Description	Range	Default
`shaping-policy`	Defines the Station Shaping Policy This feature has the following three options: ■ **default-access**: Traffic shaping is disabled, and client performance is dependent on MAC contention resolution. This is the default traffic shaping setting. ■ **fair-access**: Each client gets the same airtime, regardless of client capability and capacity. This option is useful in environments like a training facility or exam hall, where a mix of 802.11a/g, 802.11g and 802.11n clients need equal to network resources, regardless of their capabilities. The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network.You must set traffic shaping to f**air-access** to use this bandwidth allocation value for an individual virtual AP. ■ **preferred-access**: High-throughput (802.11n) clients do not get penalized because of slower 802.11a/g or 802.11b transmissions that take more air time due to lower rates. Similarly, faster 802.11a/g clients get more access than 802.11b clients.	default-access fair-access preferred-access	default-access

Usage Guidelines

The traffic management profile allows you to allocate bandwidth to SSIDs. When you enable the band-steering feature, an AP keeps track of all BSSIDs active on a radio, all clients connected to the BSSID, and 802.11a/g, 802.11b, or 802.11n capabilities of each client. Every sampling period, airtime is allocated to each client, giving it opportunity to get and receive traffic. The specific amount of airtime given to an individual client is determined by;

- Client capabilities (802.11a/g, 802.11b or 802.11n)
- Amount of time the client spent receiving data during the last sampling period
- Number of active clients in the last sampling period
- Activity of the current client in the last sampling period

The **bw-alloc** parameter of a traffic management profile allows you to set a minimum bandwidth to be allocated to a virtual AP profile when there is congestion on the wireless network. You must set traffic shaping to fair-access to use this bandwidth allocation value for an individual virtual AP.

Example

The following command configures a traffic management profile that allocates bandwidth to the corpnet virtual AP:

```
(host) [md] (config) #wlan traffic-management-profile best
(host) [md] (Traffic management profile "best") #bw-alloc virtual-ap corpnet share 75
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system on Mobility Master.	Config mode on Mobility Master.

wlan tsm-req-profile

```
wlan tsm-req-profile <profle-name>
   bin0-range <bin0-range>
   clone
   dur-mandatory
   measure-duration <measure-duration>
   no
   num-repeats <num-repeats>
   random-interval <random-interval>
   request-mode {normal | triggered}
   traffic-id <traffic-id>
```

Description

This command configures a TSM Report Request Profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this profile. The name must be 1-63 characters.	—	default
`bin0-range <bin0-range>`	This value is used to set the 'Bin 0 Range' field in the Transmit Stream or Category Measurement Request frame. Bin 0 Range indicates the delay range of the first bin (Bin 0) of the Transmit Delay Histogram, expressed in units of TUs.	0- 255	6
`clone <source>`	Creates a copy of the Transmit Stream Measurement Request Report Request Profile. <source> is the name of an existing TSM Profile from which parameter values are copied.	—	—
`dur-mandatory`	This parameter is used to set the "Duration Mandatory" bit of the Measurement Request Mode field of the Transmit Stream or Category Measurement Request frame.	–	Enabled
`measure-duration <measure-duration>`	This parameter is used to set the Measurement Duration field in the Transmit Stream or Category Measurement Request frame. The Measurement Duration is set to the duration of the requested measurement. It is expressed in units of TUs. When the request mode for the Transmit Stream or Category Measurement Request frame is set to triggered, the Measurement Duration field should be set to 0.	0-65535	9776

Parameter	Description	Range	Default
`no`	Negates any configured parameter	—	—
`num-repeats <num-repeats>`	This parameter is used to set the Number of Repetitions field in the Transmit Stream or Category Measurement Request frame. The Number of Repetitions field contains the requested number of repetitions for all the Measurement Request elements in this frame. A value of zero in the Number of Repetitions field indicates Measurement Request elements are executed once without repetition. A value of 65535 in the Number of Repetitions field indicates Measurement Request elements are repeated until the measurement is canceled or superseded.	0-65535	65535
`random-interval <random-interval>`	This parameter is used to set the Randomization Interval field in the Transmit Stream or Category Measurement Request frame. The Randomization Interval is used to specify the desired maximum random delay in the measurement start time. It is expressed in units of TUs (Time Units). When the request mode for the Transmit Stream or Category Measurement Request frame is set to "triggered", the Randomization Interval is not used and is set to 0. A Randomization Interval of 0 in a measurement request indicates that no random delay is to be used.	0-65535	0
`request-mode {normal | triggered}`	This parameter is used to determine the request mode for the Transmit Stream or Category Measurement Request frame. There are two options for this field: ■ normal ■ triggered	–	normal
`traffic-id <traffic-id>`	The parameter is used to set the Traffic Identifier field in the Transmit Stream or Category Measurement Request frame. The Traffic Identifier field contains the TID subfield. The TID subfield indicates the TC or TS for which traffic is to be measured.	0-255	96

Usage Guidelines

The tsm-req-profile is a part of the 802.11K profile. It is used to configure the parameters for the Transmit Stream or Category Measurement frames. It takes effect only when the 802.11K feature is enabled.

Example

```
(host) [md] (config) #wlan tsm-req-profile default
(host) [md] (TSM Report Request Profile "default") #bin0-range 1
```

```
(host) [md] (TSM Report Request Profile "default") #dur-mandatory
(host) [md] (TSM Report Request Profile "default") #measure-duration 25
(host) [md] (TSM Report Request Profile "default") #num-repeats 0
(host) [md] (TSM Report Request Profile "default") #random-interval 0
(host) [md] (TSM Report Request Profile "default") #request-mode normal
(host) [md] (TSM Report Request Profile "default") #traffic-id 96
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Configuration mode on Mobility Master.

wlan virtual-ap

```
wlan virtual-ap <profile-name>
   aaa-profile <profile-name>
   allowed-band <band>...
   anyspot-profile <profile>
   auth-failure-blacklist-time <seconds>
   band-steering
   blacklist
   blacklist-time <seconds>
   broadcast-filter all|arp
   cellular-handoff-assist
   clone <profile-name>
   deny-inter-user-traffic
   deny-time-range <range>
   dos-prevention
   dot11k-profile
   dynamic-mcast-optimization
   dynamic-mcast-optimization-threshold
   fdb-update-on-assoc
   forward-mode {tunnel|bridge|split-tunnel|decrypt-tunnel}
   ha-disc-onassoc
   hs2-profile
   mobile-ip
   no ...
   openflow-enable
   preserve-vlan
   rap-operation {always|backup|persistent|standard}
   ssid-profile <profile-name>
   steering-mode band-balancing|force-5ghz|prefer-5ghz
   strict-compliance
   vap-enable
   vlan <vlan>...
   vlan-mobility
   wan-operation
   wmm-traffic-management-profile
```

Description

This command configures a virtual AP profile.

Syntax

Parameter	Description	Range	Default
`<profile-name>`	Name of this profile. The name must be 1-63 characters.	—	“default”
`aaa-profile`	Name of the AAA profile that applies to this virtual AP.	—	“default”
`allowed-band`	The band(s) on which to use the virtual AP: **a**—802.11a band only (5 GHz) **g**—802.11b/g band only (2.4 GHz) **all**—both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz)	a, g, all	all

Parameter	Description	Range	Default
anyspot-profile	Anyspot Profile associated with this Virtual AP Profile. The anyspot client probe suppression feature decreases network traffic by suppressing probe requests from clients attempting to locate and connect to other known networks.	–	–
auth-failure-blacklist-time	Time, in seconds, a client is blocked if it fails repeated authentication. A value of 0 blocks a client iindefinitely.	0-2,147,483,647 seconds	0
band-steering	ARM's band steering feature can encourage or require dual-band capable clients to stay on the 5 GHz band on dual-band APs. This frees up resources on the 2.4 GHz band for single band clients like VoIP phones. Band steering reduces co-channel interference and increases available bandwidth for dual-band clients, because there are more channels on the 5 GHz band than on the 2.4 GHz band. Dual-band 802.11n-capable clients may see even greater bandwidth improvements, because the band steering feature will automatically select between 40MHz or 20 MHz channels in 802.11n networks. This feature is disabled by default, and must be enabled in a Virtual AP profile. The band steering feature supports three steering modes, which can be configured via the steering-mode parameter: Band steering can be configured on both campus APs and remote APs that have a virtual AP profile set to tunnel, decrypt-tunnel, split-tunnel or bridge forwarding mode. Note, however, that if a campus or remote APs has virtual AP profiles configured in bridge or split-tunnel forwarding mode but no virtual AP in tunnel mode, those APs will gather information about 5G-capable clients independently and will not exchange this information with other APs that also have bridge or split-tunnel virtual APs only.	—	disabled
blacklist	Enables detection of DoS attacks, such as ping or SYN floods, that are not spoofed deauth attacks.	—	enabled
blacklist-time	Number of seconds that a client is quarantined from the network after being blacklisted.	0-2,147,483,647 seconds	3600 seconds (1 hour)

Parameter	Description	Range	Default
`broadcast-filter`	Filter out broadcast and multicast traffic in the air. ■ all **NOTE:** Do not enable this option for virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the managed device, so the managed device is able to drop all broadcast traffic. When a virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the managed device is not able to filter out that broadcast traffic. **IMPORTANT:** If you enable this option, you must also enable the **Broadcast-Filter ARP** parameter in the stateful firewall configuration to prevent ARP requests from being dropped. Note also that although a virtual AP profile can be replicated from a Mobility Master to managed device, stateful firewall settings do not. If you select the **broadcast-filter all** option for a Virtual AP Profile on a Mobility Master, you must enable the **broadcast-filter arp** setting on each individual managed device. ■ arp If enabled, all broadcast ARP requests are converted to unicast and sent directly to the client. You can check the status of this option using the **show ap active** and the **show datapath tunnel** command. If enabled, the output will display the letter **a** in the flags column. Do not enable this option for virtual APs configured in bridge forwarding mode. This configuration parameter is only intended for use for virtual APs in tunnel mode. In tunnel mode, all packets travel to the managed device, so the managed device is able to convert ARP requests directed to the broadcast address into unicast. When a virtual AP is configured to use bridge forwarding mode, most data traffic stays local to the AP, and the managed device is not able to convert that broadcast traffic.	—	For the option **all**, the default value is disabled. For the option **arp**, the default value is enabled.

Parameter	Description	Range	Default
`cellular-handoff-assist`	When both the client match and cellular handoff assist features are enabled, the cellular handoff assist feature can help a dual-mode, 3G or 4G-capable Wi-Fi device such as an iPhone, iPad, or Android client at the edge of Wi-Fi network coverage switch from Wi-Fi to an alternate 3G or 4G radio that provides better network access. This feature is disabled by default, and is recommended only for Wi-Fi hotspot deployments.	—	disabled
`clone`	Name of an existing traffic management profile from which parameter values are copied.	—	—
`deny-inter-user-traffic`	Select this check box to deny traffic between the clients using this virtual AP profile. The **firewall** command includes an option to deny all inter-user traffic, regardless of the Virtual AP profile used by those clients. If the global setting to deny inter-user traffic is enabled, all inter-user traffic between clients will be denied, regardless of the settings configured in the virtual AP profiles. If the setting to deny inter-user traffic is disabled globally but enabled on an individual virtual ap, only the traffic between un-trusted users and the clients on that particular virtual AP will be blocked.	–	disabled
`deny-time-range`	Specify the name of the time range for which the AP will deny access. Time ranges can be defined using the CLI command time-range.	—	—
`dos-prevention`	If enabled, APs ignore deauthentication frames from clients. This prevents a successful deauth attack from being carried out against the AP. This does not affect third-party APs.	—	disabled
`dot11k-profile`	Name of an 802.11k profile to be associated with this VAP.	—	default
`dynamic-mcast-optimization`	Enable or /Disable dynamic multicast optimization. This parameter can only be enabled on a managed device with a PEFNG license.	—	disabled

Parameter	Description	Range	Default
`dynamic-mcast-optimization-threshold`	Maximum number of high-throughput stations in a multicast group beyond which dynamic multicast optimization stops.	2-255 stations	6 stations
`fdb-update-on-assoc`	This parameter enables seamless failover for silent clients, allowing them to re-associate. If you select this option, the managed device will generate a Layer 2 update on behalf of client to update forwarding tables in bridge devices. Default: Disabled	—	disabled

Parameter	Description	Range	Default
`forward-mode`	Controls whether 802.11 frames are tunneled to the managed device using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). Select one of the following forward modes: ■ **Tunnel**: When an AP is in tunnel forwarding mode, the AP handles all 802.11 association requests and responses. The AP sends all 802.11 data packets, action frames and EAPOL frames over a GRE tunnel to the managed device for processing. The managed device removes or adds the GRE headers, decrypts or encrypts 802.11 frames and applies firewall rules to the user traffic as usual. ■ **Bridge**: When an AP is in bridge mode, data is bridged onto the local Ethernet LAN. When in bridge mode, the AP handles all 802.11 association requests and responses, encryption or decryption processes, and firewall enforcement. 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in bridge mode supports only the 802.1X authentication type. ■ **Split-Tunnel**: Data frames are either tunneled or bridged, depending on the destination (corporate traffic goes to the managed device, and Internet access remains local). The AP handles all 802.11 association requests and responses, encryption or decryption, and firewall enforcement. 802.11e and 802.11k action frames are also processed by the AP, which then sends out responses as needed. An AP in split-tunnel mode supports only the 802.1X authentication type. ■ **Decrypt-Tunnel:** An AP in decrypt-tunnel forwarding mode decrypts and decapsulates all 802.11 frames from a station and sends the 802.3 frames through the GRE tunnel to the managed device, which then applies	tunnel bridge split-tunnel decrypt-tunnel	tunnel

Parameter	Description	Range	Default
	firewall policies to the user traffic. This mode allows a network to utilize the encryption or decryption capacity the AP while reducing the demand for processing resources on the managed device. APs in decrypt-tunnel forwarding mode also manage all 802.11 association requests and responses, and process all 802.11e and 802.11k action frames. **NOTE:** Virtual APs in bridge or split-tunnel mode using static WEP should use key slots 2-4 on the managed device. Key slot 1 should only be used with Virtual APs in tunnel mode.		
`ha-disc-onassoc`	If enabled, home agent discovery is triggered on client association instead of home agent discovery based on traffic from client. Mobility on association can speed up roaming and improve connectivity for clients that do not send many uplink packets to trigger mobility (VoIP clients). Best practices is to leave this parameter disabled, as it increases IP mobility control traffic between managed devices in the same mobility domain. Enable this parameter only when voice issues are observed in VoIP clients. **NOTE:** `ha-disc-onassoc` parameter works only when IP mobility is enabled and configured on the managed device.	—	disabled
`hs2-profile`	Enables or disables a hotspot profile. This is enabled by default.	–	enabled
`mobile-ip`	Enables or disables IP mobility on a virtual AP. This is enabled by default. L3 mobility service is active on a VAP only if **router mobile** is also enabled on the managed device.	—	enabled
`no`	Negates any configured parameter.	—	—
`openflow-enable`	Enables OpenFlow on AP forwarding path.	—	—
`preserve-vlan`	This parameter allows clients to retain their previous VLAN assignment if the client disassociates from an AP and then immediately re-associates either with same AP or another AP on same managed device.		

Parameter	Description	Range	Default
`rap-operation`	Configures when the virtual AP operates on a remote AP: ■ **always**—Permanently enables the virtual AP (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ **backup**—Enables the virtual AP if the remote AP cannot connect to the managed device (Bridge Mode only). This option can be used for non-802.1X bridge VAPs. ■ **persistent**—Permanently enables the virtual AP after the remote AP initially **connects** to the managed device (Bridge Mode only). This option can be used for any (Open or PSK or 802.1X) bridge VAPs. ■ **standard**—Enables the virtual AP when the remote AP connects to the managed device. This option can be used for any (bridge or split-tunnel or tunnel or d-tunnel) VAPs.	always or backup or persistent or standard	standard
`ssid-profile`	Name of the SSID profile that applies to this virtual AP.	—	default

Parameter	Description	Range	Default
`steering-mode`	Band steering supports three different band steering modes. ■ **Force-5GHz**: When the AP is configured in **force-5GHz** band steering mode, the AP will try to force 5 GHz-capable APs to use that radio band. ■ **Prefer-5GHz** (Default): If you configure the AP to use **prefer-5GHz** band steering mode, the AP will try to steer the client to 5G band (if the client is 5G capable) but will let the client connect on the 2.4G band if the client persists in 2.4G association attempts. ■ **Balance-bands**: In this band steering mode, the AP tries to balance the clients across the two radios in order to best utilize the available 2.4G bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz while the 2.5 GHz band operates in 20 MHz. **NOTE:** Steering modes do not take effect until the band steering feature has been enabled. The band steering feature in ArubaOS versions 3.3.2-5.0 does not support multiple band-steering modes. The band-steering feature in these versions of ArubaOS functions the same way as the default **prefer-5GHz** steering mode available in ArubaOS 6.0 and later.	Force-5 GHz prefer-5 GHz balance-bands	prefer-5 GHz
`strict-compliance`	If enabled, the AP denies client association requests if the AP and client station have no common rates defined. Some legacy client stations which are not fully 802.11-compliant may not include their configured rates in their association requests. Such non-compliant stations may have difficulty associating with APs unless strict compliance is disabled.	—	disabled
`vap-enable`	Enable or disable the virtual AP.	—	enabled

Parameter	Description	Range	Default
`vlan`	The VLAN(s) into which users are placed in order to obtain an IP address. Enter VLANs as a comma-separated list of existing VLAN IDs *or* VLAN names. A mixture of names and numeric IDs are not allowed. **NOTE:** You must add an existing VLAN ID to the Virtual AP profile.		1
`vlan-mobility`	VLAN mobility retains the client VLAN on roaming irrespective of the VAP VLAN, provided the user VLANs are extended. VLAN mobility and mobile IP are mutually exclusive. VLAN mobility does not re-use user firewall sessions on roaming as the sessions will have to be recreated locally on the roamed managed device.	—	disabled
`wan-operation`	Specify the wan-operation to enable Virtual AP depending on the state of the WAN link.	always backup primary	always
`wmm-traffic-management-profile`	Specify the WMM Traffic Management Profile to be associated with this Virtual AP Profile.	—	—

Usage Guidelines

WLAN profiles configure WLANs in the form of virtual AP profiles. A virtual AP profile contains an SSID profile which defines the WLAN and an AAA profile which defines the authentication for the WLAN. You can configure and apply multiple instances of virtual AP profiles to an AP group or to an individual AP.

A named VLAN can be deleted although it is configured in a virtual AP profile. If this occurs the virtual AP profiles becomes invalid. If the named VLAN is added back later the virtual AP becomes valid again.

The **broadcast-filter arp** parameter is enabled by default. If your Mobility Master supports clients behind a wireless bridge or virtual clients on VMware devices, you must disable the broadcast-filter arp setting to allow those clients to obtain an IP address. In previous releases of ArubaOS, the virtual AP profile included two unique broadcast filter parameters; the **broadcast-filter all** parameter, which filtered out all broadcast and multicast traffic in the air except DHCP response frames (these were converted to unicast frames and sent to the corresponding client) and the **broadcast-filter arp** parameter, which converted broadcast ARP requests to unicast messages sent directly to the client.

The **broadcast-filter arp** setting includes the additional functionality of broadcast-filter all parameter, where DHCP response frames are sent as unicast to the corresponding client. This can impact DHCP discover or requested packets for clients behind a wireless bridge and virtual clients on VMware devices. Disable the broadcast-filter arp setting using the **wlan virtual-ap <profile> no broadcast-filter arp** command to resolve this issue and allow clients behind a wireless bridge or VMware devices to receive an IP address.

If there is only one VLAN defined, then the Mobility Master will send IPv6 RAs as usual. If, however, there are multiple VLANs, then the Mobility Master will automatically convert 802.11 multicast frames to unicast. This conversion prevents RA frames from being sent with a multicast key to all clients on the BSSID, which could lead to clients having multiple IPv6 addresses.

Example

The following command configures a virtual AP:

```
(host) [md] (config) #wlan virtual-ap corpnet
(host) [md] (Virtual AP profile "corpnet") #vlan 1
(host) [md] (Virtual AP profile "corpnet") #aaa-profile corpnet
```

Command History

Version	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system.	Config mode on Mobility Master.

wlan wmm-traffic-management-profile

```
wlan wmm-traffic-management-profile <profile-name>
   background <share>
   best-effort <share>
   clone <source>
   enable-shaping
   no
   video <share>
   voice <share>
```

Description

This command configures bandwidth shaping for WMM access categories.

Bandwidth shaping is only applied on the down-link traffic.

Syntax

Parameter	Description	Range	Default
`background <share>`	Bandwidth allocation, in percentage (%), for WMM background access traffic category.	0-100%	5%
`best-effort <share>`	Bandwidth allocation, in percentage (%), for WMM best effort access traffic category.	0-100%	5%
`clone <source>`	Copies the configuration from another WMM Traffic management profile.	—	—
`enable-shaping`	Enables a bandwidth shaping policy so that the allocated bandwidth share is appropriately used.	—	disabled
`no`	Negates any configured parameter.	—	—
`video <share>`	Bandwidth allocation, in percentage (%), for video access traffic category.	0-100%	55%
`voice <share>`	Bandwidth allocation, in percentage (%), for voice access traffic category.	0-100%	35%

Usage Guidelines

After you configure the WMM traffic management profile, apply it to the virtual AP profile. For WMM traffic management to take effect, you must enable **fair-access** or **preferred-access** parameter under wlan traffic-management-profile.

Example

The following command configures a WMM traffic management profile:

```
(host) [md] (config) #wlan wmm-traffic-management-profile test
(host) [md] (WMM Traffic management profile "test") #enable-shaping
(host) [md] (WMM Traffic management profile "test") #background 7
(host) [md] (WMM Traffic management profile "test") #best-effort 10
(host) [md] (WMM Traffic management profile "test") #voice 40
(host) [md] (WMM Traffic management profile "test") #video 43
```

Apply the WMM traffic management profile to the virtual AP profile.

```
(host) [md] (config) #wlan virtual-ap employee
(host) [md] (Virtual AP profile "employee") #wmm-traffic-management-profile test
```

Enable the **fair-access** or **preferred access** parameter under **wlan traffic-management-profile**.

```
(host) [md] (config) #wlan traffic-management-profile test
(host) [md] (Traffic management profile "test") #shaping-policy fair-access
```

OR

```
(host) [md] (Traffic management profile "test") #shaping-policy preferred-access
```

Apply the traffic management profile to an ap group.

```
(host) [md] (config) #ap-group default
(host) [md] (AP group "default") #dot11a-traffic-mgmt-profile test
```

Related Commands

Command	Description
show wlan wmm-traffic-management-profile	Displays the WMM traffic management profile(s) configured on the managed device.
wlan traffic-management-profile	Configures a traffic management profile.

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	PEFNG license	Config mode on Mobility Master

wms ap

```
wms ap <bssid> mode {interfering|manually-contained|neighbor|rogue|suspected-rogue|valid}
```

Description

This command allows you to classify an AP into one of several categories.

Syntax

Parameter	Description
`<bssid>`	BSSID of the AP.
`mode`	Classify the AP into one of the following categories.
`interfering`	An AP seen in the RF environment but is not connected to the wired network.
`manually-contained`	Manually enables denial of service from this AP
`neighbor`	An neighboring AP whose BSSID is known.
`rogue`	A rogue AP that is unauthorized and is plugged into the wired side of the network. You can configure automatic shutdown of rogue APs in the IDS unauthorized device detection profile.
`suspected-rogue`	A suspected rogue AP that is plugged into the wired side of the network but may not be an unauthorized device. Automatic shutdown of rogue APs does not apply to these devices.
`valid`	An AP that is part of the enterprise providing WLAN service.

Usage Guidelines

If AP learning is enabled (with the **ids-wms-general-profile learn-ap** command), non-Aruba APs connected on the same wired network as Aruba APs are classified as valid APs. If AP learning is disabled, a non-Aruba AP is classified as an unsecure or suspect-unsecure AP.

Example

The following command classifies an interfering AP as a known-interfering AP:

```
(host) [mynode] #wms ap 01:00:00:00:00:00 mode known-interfering
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms clean-db

```
wms clean-db
```

Description

This command deletes the WMS database.

Syntax

Parameter	Description
`clean-db`	Cleans the WMS database.

Usage Guidelines

This command deletes all entries from the WMS database. Do not use this command unless instructed to do so by an Aruba representative.

Example

The following command cleans the WMS database:

```
(host) [mynode] #wms clean-db
   WMS Database will be deleted. Do you want to proceed with this action [y/n]:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms client

```
wms client <mac>
   mode {interfering|manually-contain|valid}
   valid-exempt {insert|remove}
```

Description

This command allows you to classify a wireless client into one of several categories.

Syntax

Parameter	Description
`<mac>`	MAC address of the client.
`mode`	Classifies the client into one of the following categories:
`interfering`	Setting the client mode to *interfering* makes it part of clients outside the enterprise
`manually-contain`	Manually enables denial of service to this client.
`valid`	A client that is part of the enterprise.
`valid-exempt`	Classifies the client under this option to exempt from Valid Station Protection and Valid Station Misassociation Detection.
`insert`	Adds the client to the valid-exempt list and exempt from Valid Station Protection and Valid Station Misassociation Detection. If the client exists in the WMS, the classification is set to valid. In case the client does not exist in the WMS, a client entry is created and then the classification is set to valid.
`remove`	Removes the client from the list of valid-exempt clients.

Usage Guidelines

ArubaOS can automatically determine client classification based on client behavior, but this command allows you to explicitly classify a client. The classification of a client is used in certain policy enforcement features. For example, if **protect-valid-sta** is enabled in the IDS Unauthorized Device Profile, then clients that are classified as valid cannot connect to non-valid APs.

Example

The following command classifies a client as valid:

```
(host) [mynode] #wms client 00:00:A4:34:C9:B3 mode valid
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms export-class

```
wms export-class <filename>
```

Description

This command exports classification information into a file.

Syntax

Parameter	Description
`<filename>`	Name of the file into which you want to export classification information.

Usage Guidelines

This command writes classification data into comma separated values (CSV) files—one for APs and one for clients. You can import these files into the Aruba Mobility Manager system.

Example

The following command exports classification data into an AP and a client file:

```
(host) [mynode] #wms export-class class

Exported data to class_ap.csv and class_sta.csv
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms export-db

```
wms export-db <filename>
```

Description

This command exports the WMS database to a specified file.

Syntax

Parameter	Description
`<filename>`	Name of the file into which you want to export the database. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.

Usage Guidelines

The file is exported as an ASCII text file.

Example

The following command exports the WMS database to a file:

```
(host) [mynode] #wms export-db database

Exported WMS DB to database
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms import-db

```
wms import-db <filename>
```

Description

This command imports the specified file into the WMS database.

Syntax

Parameter	Description
`<filename>`	Name of the file into which you want to import into the database. The filename plus any extensions must be no longer than 32 characters and may contain only keyboard characters.

Usage Guidelines

The imported file replaces the WMS database. The imported file must be a valid WMS database file that you previously exported using the **wms export-db** command.

Example

The following command imports the WMS database from a file:

```
(host) [mynode] #wms import-db database
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms reinit-db

```
wms reinit-db
```

Description

This command reinitializes the WMS database to its factory default setting.

Syntax

No parameters.

Usage Guidelines

When you use this command, there is no automatic backup of the current database.

Example

The following command reinitializes the WMS database:

```
(host) [mynode] #wms reinit-db
WMS Database will be re-initialized. Do you want to proceed with this action [y/n ]:
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms restart-snapshot

```
wms restart-snapshot {ap|rogue-ap|sta}
```

Description

This command restarts periodic snapshot messaging by the WLAN Management System (WMS).

Syntax

Parameter	Description
`ap`	Restarts the monitored AP snapshot.
`rogue-ap`	Restarts the monitored rogue AP snapshot.
`sta`	Restarts the monitored client snapshot.

Example

The following command restarts snapshot messaging for monitored APs:

```
(host) [mynode] #wms restart-snapshot ap
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

wms test

```
wms test {busy <interval>|lc-poll-interval <interval-time>}
```

Description

This command configures WLAN Management System (WMS) test settings.

Syntax

Parameter	Description
`busy <interval>`	Sets a time interval, in seconds, that the WMS is busy.
`lc-poll-interval <interval-time>`	Sets a polling interval, in minutes, for communication between the WMS and managed devices. The time interval must be between 10-360 minutes.

Example

The following command sets a polling interval of 15 minutes:

```
(host) [mynode] (config) #wms test lc-poll-interval 15
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Config mode on Mobility Master.

write

```
write {erase [all]|memory|terminal}
```

Description

This command saves the running configuration to memory or displays the running configuration on the screen. This command can also be used to erase the running configuration and return Mobility Master to factory defaults.

Syntax

Parameter	Description
`erase`	Erases the running system configuration file. Rebooting Mobility Master resets it to the factory default configuration. If you specify `all`, the configuration and all data in Mobility Master databases (including the license, WMS, and internal databases) are erased.
`memory`	Saves the current system configuration to memory. Any configuration changes made during this session will be made permanent.
`terminal`	Displays the current system configuration.

Usage Guidelines

Configuration changes made using the CLI affect only the current session. You must save your changes for them to be retained across system reboots. Changes are lost if the system reboots before saving the changes. To save your configuration changes, use the **write memory** command.

If you use the **write erase** command, the license key management database on Mobility Master is not affected. If you use the **write erase all** command, all databases on Mobility Master are deleted, including the license key management database. If you reset Mobility Master to the factory default configuration, perform the Initial Setup as described in the *ArubaOS Quick Start Guide*.

If you use the **write terminal** command, all of the commands used to configure Mobility Master appear on the terminal. If paging is enabled, there is a pause mechanism that stops the output from printing continuously to the terminal. To navigate through the output, use any of the commands displayed at the bottom of the output, as described in below. If paging is disabled, the output prints continuously to the terminal. For more information about the **paging** command, see paging on page 774.

Key	Description
Q	Exit the display.
U	Page up through the output.
spacebar	Page down through the output.
/	Enter a text string to search for.
N	Repeat the text string to search for.

Example

The following command saves your changes so they are retained after a reboot:

```
(host) [mynode] #write memory
```

The following command deletes the running configuration and databases and returns Mobility Master to the factory default settings:

```
(host) [mynode] #write erase
```

Command History

Release	Modification
ArubaOS 8.0.0.0	Command introduced.

Command Information

Platforms	License	Command Mode
All platforms	Base operating system	Enable or Config mode on Mobility Master.

The following table lists the acronyms and abbreviations used in Aruba documents.

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
3G	Third Generation of Wireless Mobile Telecommunications Technology
4G	Fourth Generation of Wireless Mobile Telecommunications Technology
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Access Category
ACC	Advanced Cellular Coexistence
ACE	Access Control Entry
ACI	Adjacent Channel interference
ACL	Access Control List
AD	Active Directory
ADO	Active X Data Objects
ADP	Aruba Discovery Protocol
AES	Advanced Encryption Standard
AIFSN	Arbitrary Inter-frame Space Number
ALE	Analytics and Location Engine
ALG	Application Layer Gateway
AM	Air Monitor
AMON	Advanced Monitoring
AMP	AirWave Management Platform
A-MPDU	Aggregate MAC Protocol Data Unit
A-MSDU	Aggregate MAC Service Data Unit
ANQP	Access Network Query Protocol
ANSI	American National Standards Institute
AP	Access Point

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
API	Application Programming Interface
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
AVF	AntiVirus Firewall
BCMC	Broadcast-Multicast
BGP	Border Gateway protocol
BLE	Bluetooth Low Energy
BMC	Beacon Management Console
BPDU	Bridge Protocol Data Unit
BRAS	Broadband Remote Access Server
BRE	Basic Regular Expression
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certification Authority
CAC	Call Admission Control
CALEA	Communications Assistance for Law Enforcement Act
CAP	Campus AP
CCA	Clear Channel Assessment
CDP	Cisco Discovery Protocol
CDR	Call Detail Records
CEF	Common Event Format
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CN	Common Name
CoA	Change of Authorization

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
CoS	Class of Service
CPE	Customer Premises Equipment
CPsec	Control Plane Security
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Channel Switch Announcement
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSR	Certificate Signing Request
CSV	Comma Separated Values
CTS	Clear to Send
CW	Contention Window
DAS	Distributed Antenna System
dB	Decibel
dBm	Decibel Milliwatt
DCB	Data Center Bridging
DCE	Data Communication Equipment
DCF	Distributed Coordination Function
DDMO	Distributed Dynamic Multicast Optimization
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DFT	Discreet Fourier Transform
DHCP	Dynamic Host Configuration Protocol
DLNA	Digital Living Network Alliance
DMO	Dynamic Multicast optimization
DN	Distinguished Name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specification

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
DoS	Denial of Service
DPD	Dead Peer Detection
DPI	Deep Packet Inspection
DR	Designated Router
DRT	Downloadable Regulatory Table
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DST	Daylight Saving Time
DTE	Data Terminal Equipment
DTIM	Delivery Traffic Indication Message
DTLS	Datagram Transport Layer Security
DU	Data Unit
EAP	Extensible Authentication Protocol
EAP-FAST	EAP-Flexible Authentication Secure Tunnel
EAP-GTC	EAP-Generic Token Card
EAP-MD5	EAP-Method Digest 5
EAP-MSCHAP EAP-MSCHAPv2	EAP-Microsoft Challenge Handshake Authentication Protocol
EAPoL	EAP over LAN
EAPoUDP	EAP over UDP
EAP-PEAP	EAP-Protected EAP
EAP-PWD	EAP-Password
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECC	Elliptical Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EIGRP	Enhanced Interior Gateway Routing Protocol

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
EIRP	Effective Isotropic Radiated Power
EMM	Enterprise Mobility Management
ESI	External Services Interface
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
EULA	End User License Agreement
FCC	Federal Communications Commission
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FQLN	Fully Qualified Location Name
FRER	Frame Receive Error Rate
FRR	Frame Retry Rate
FSPL	Free Space Path Loss
FTP	File Transfer Protocol
GBps	Gigabytes per second
Gbps	Gigabits per second
GHz	Gigahertz
GIS	Generic Interface Specification
GMT	Greenwich Mean Time
GPP	Guest Provisioning Page
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GVRP	GARP or Generic VLAN Registration Protocol
H2QP	Hotspot 2.0 Query Protocol

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
HA	High Availability
HMD	High Mobility Device
HSPA	High-Speed Packet Access
HT	High Throughput
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IKE PSK	Internet Key Exchange Pre-shared Key
IoT	Internet of Things
IP	Internet Protocol
IPM	Intelligent Power Monitoring
IPS	Intrusion Prevention System
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
JSON	JavaScript Object Notation
KBps	Kilobytes per second
Kbps	Kilobits per second
L2TP	Layer-2 Tunneling Protocol
LACP	Link Aggregation Control Protocol

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
LAG	Link Aggregation Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDPC	Low-Density Parity-Check
LEA	Law Enforcement Agency
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode
LEEF	Log Event Extended Format
LI	Lawful Interception
LLDP	Link Layer Discovery Protocol
LLDP-MED	LLDP–Media Endpoint Discovery
LMS	Local Management Switch
LNS	L2TP Network Server
LTE	Long Term Evolution
MAB	MAC Authentication Bypass
MAC	Media Access Control
MAM	Mobile Application Management
MBps	Megabytes per second
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MD5	Message Digest 5
MDM	Mobile Device Management
mDNS	Multicast Domain Name System
MFA	Multi-factor Authentication
MHz	Megahertz
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
MLD	Multicast Listener Discovery
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Maximum Segment Size
MSSID	Mesh Service Set Identifier
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
MVRP	Multiple VLAN Registration Protocol
NAC	Network Access Control
NAD	Network Access Device
NAK	Negative Acknowledgment Code
NAP	Network Access Protection
NAS	Network Access Server Network-attached Storage
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NIC	Network Interface Card
Nmap	Network Mapper
NMI	Non-Maskable Interrupt
NMS	Network Management Server
NOE	New Office Environment
NTP	Network Time Protocol
OAuth	Open Authentication
OCSP	Online Certificate Status Protocol
OFA	OpenFlow Agent

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OKC	Opportunistic Key Caching
OS	Operating System
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
OVA	Open Virtual Appliance
OVF	Open Virtualization Format
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PAPI	Proprietary Access Protocol Interface
PCI	Peripheral Component Interconnect
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PEAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card
PEF	Policy Enforcement Firewall
PFS	Perfect Forward Secrecy
PHB	Per-hop behavior
PIM	Protocol-Independent Multicast
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMK	Pairwise Master Key
PoE	Power over Ethernet
POST	Power On Self Test
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
PPTP	PPP Tunneling Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PSU	Power Supply Unit
PVST	Per VLAN Spanning Tree
QoS	Quality of Service
RA	Router Advertisement
RADAR	Radio Detection and Ranging
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAP	Remote AP
RAPIDS	Rogue Access Point and Intrusion Detection System
RARP	Reverse ARP
REGEX	Regular Expression
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFID	Radio Frequency Identification
RIP	Routing Information Protocol
RRD	Round Robin Database
RSA	Rivest, Shamir, Adleman
RSSI	Received Signal Strength Indicator
RSTP	Rapid Spanning Tree Protocol
RTCP	RTP Control Protocol
RTLS	Real-Time Location Systems
RTP	Real-Time Transport Protocol
RTS	Request to Send
RTSP	Real Time Streaming Protocol

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
RVI	Routed VLAN Interface
RW RoW	Rest of World
SA	Security Association
SAML	Security Assertion Markup Language
SAN	Subject Alternative Name
SCB	Station Control Block
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDN	Software Defined Networking
SDR	Software-Defined Radio
SDU	Service Data Unit
SD-WAN	Software-Defined Wide Area Network
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIRT	Security Incident Response Team
SKU	Stock Keeping Unit
SLAAC	Stateless Address Autoconfiguration
SMB	Small and Medium Business
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SNIR	Signal-to-Noise-Plus-Interference Ratio
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SoC	System on a Chip
SoH	Statement of Health
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STBC	Space-Time Block Coding
STM	Station Management
STP	Spanning Tree Protocol
STRAP	Secure Thin RAP
SU-MIMO	Single-User Multiple-Input Multiple-Output
SVP	SpectraLink Voice Priority
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-length-value
ToS	Type of Service
TPC	Transmit Power Control
TPM	Trusted Platform Module
TSF	Timing Synchronization Function
TSPEC	Traffic Specification
TTL	Time to Live

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
TTLS	Tunneled Transport Layer Security
TXOP	Transmission Opportunity
U-APSD	Unscheduled Automatic Power Save Delivery
UCC	Unified Communications and Collaboration
UDID	Unique Device Identifier
UDP	User Datagram Protocol
UI	User Interface
UMTS	Universal Mobile Telecommunication System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VA	Virtual Appliance
VBN	Virtual Branch Networking
VBR	Virtual Beacon Report
VHT	Very High Throughput
VIA	Virtual Intranet Access
VIP	Virtual IP Address
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over IP
VoWLAN	Voice over Wireless Local Area Network
VPN	Virtual Private Network
VRD	Validated Reference Design
VRF	Visual RF
VRRP	Virtual Router Redundancy Protocol
VSA	Vendor-Specific Attributes

Table 11: *List of Acronyms and Abbreviations*

Acronym or Abbreviation	Definition
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WebUI	Web browser User Interface
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIDS	Wireless Intrusion Detection System
WINS	Windows Internet Naming Service
WIPS	Wireless Intrusion Prevention System
WISPr	Wireless Internet Service Provider Roaming
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMI	Windows Management Instrumentation
WMM	Wi-Fi Multimedia
WMS	WLAN Management System
WPA	Wi-Fi Protected Access
WSDL	Web Service Description Language
WWW	World Wide Web
WZC	Wireless Zero Configuration
XAuth	Extended Authentication
XML	Extensible Markup Language
XML-RPC	XML Remote Procedure Call
ZTP	Zero Touch Provisioning

The ArubaOS CLI offers different levels of user access by differentiating between different command modes.

When you first log in to the CLI, you start your session in *User* mode, which provides only limited access for basic operational testing. You must enter an additional password to access *Enable* mode, which allows you to issue show commands run certain management functions. Configuration commands can only be issued in *Configuration* mode. You can access Config mode by entering **configure terminal** at the command prompt. You can exit your current command mode and return to a lower-level command mode at any time by entering **exit** at the command prompt.

The following sections describes how to access each command mode, the command prompt for each mode, and links to its available commands:

- Enable Mode on page 2692
- Config Mode on page 2692

Enable Mode

On logging onto the Mobility Master, the user mode is presented.

The command prompt for a CLI session in enable mode is a pound (**#**) symbol:

```
(host) [mynode]#
```

To view a list of commands available in enable mode, access the CLI in enable mode and enter a question mark (?):

```
(host) [mynode]#?
```

Some top-level commands have different sets of sub-commands available in Enable or Config mode. To view a list of available sub-commands in Enable mode, access the CLI in Enable mode, enter the top level command, then enter a question mark (?). For example, the following example shows which aaa commands are available in Enable mode:

```
(host) [mynode]#aaa ?
authentication          Authentication
inservice               Bring authentication server into service
ipv6                    Internet Protocol Version 6
query-user              Query User
test-server             Test authentication server
user                    User commands
```

Config Mode

To move from enable mode to config mode, enter the command **config terminal**. Users in config mode may return to enable mode at any time by entering the command **exit**.

When you are in config mode, **(config)** appears before the # prompt:

```
(host) [mynode] (config) #
```

Some top-level commands have different sets of sub-commands available in the Enable or Config mode. To view a list of available sub-commands in the Config mode, access the CLI in the Config mode, enter the top level

command, then enter a question mark (?). For example, the following example shows which **aaa** commands are available in the Config mode:

```
(host) [mynode] (config) #aaa ?
alias-group             Configure an Alias Group
auth-survivability      Configure Auth Surivability
auth-trace              Set parameters for debug tracing in AUTH (light weight tracing)
authentication          Authentication
authentication-server   Authentication Servers
bandwidth-contract      Configure bandwidth contract (256 Kbps - 2 Gbps)
derivation-rules        Configure rules to derive user role or vlan
dns-query-interval      Set DNS query interval
log                     Enable debugging on per-user basis
password-policy         Password policy for locally configured management users
profile                 Configure an AAA Profile
radius-attributes       Configure RADIUS attribute
rfc-3576-server         Configure an RFC 3576 Server
server-group            Configure a Server Group
tacacs-accounting       Configure accounting
timers                  Configure authentication timers
user                    User commands
xml-api                 External XML API server
```

Configuration Sub-modes

Some Config mode commands can enter you into a sub-mode with a limited number of available commands specific to that mode. When you are in a configuration sub-mode, the (config) that appears before the command prompt will change to indicate your current mode; e.g (config-submode).

You can exit a sub-command mode and return to the basic configuration mode at any time by entering the exit command.