

Monitoring Clients and System Operations

The **Monitoring** web configuration screen accesses settings for displaying system messages and associated client information, and is also used for configuring simple network management protocols (SNMP).

Monitoring Settings

Monitoring settings are arranged on the following configuration pages:

- **Monitoring>System Messages** - View system events and define where to store the system event log.
- **Monitoring>SNMP Monitoring** - Enable SNMP and configure communities, users, and traps.
- **Monitoring>Associated Clients** - View a dynamic listing of clients associating with each wireless interface.

Monitoring>System Messages

This page is used to view system event messages and define the remote log server.

System Logging Configuration	
Local Logging	DISABLED
Remote Logging	DISABLED None
Commit	

System Messages	
1	Jul 8 08:25:32 (none) user.info klogd: http://www.scyld.com/network/natsemi.html
2	Jul 8 08:25:32 (none) user.info klogd: 2.4.x kernel port by Jeff Garzik, Tjeerd Mulder
3	Jul 8 08:25:32 (none) user.info klogd: eth0: NatSemi DP8381[56] at 0xc307d000, 00:0b:33:00:60:00, IRQ 16.
4	Jul 8 08:25:32 (none) user.info klogd: eth1: NatSemi DP8381[56] at 0xc307f000, 00:0b:33:00:60:01, IRQ 24.
5	Jul 8 08:25:32 (none) user.info klogd: Intel(R) PRO/1000 Network Driver - version 5.0.43-k1
6	Jul 8 08:25:32 (none) user.info klogd: Copyright (c) 1999-2003 Intel Corporation.
7	Jul 8 08:25:32 (none) user.info init: Starting pid 329, console /dev/ttyS0: '/bin/login'
8	Jul 8 08:25:32 (none) user.info klogd: eth2: Intel(R) PRO/1000 Network Connection
9	Jul 8 08:25:32 (none) user.info klogd: eth3: Intel(R) PRO/1000 Network Connection

System Logging Configuration

System messages can be saved (logged) on the Wi-Fi AP/Bridge and on a remote device.

- **Local Logging:** Select **ENABLED** to save system messages in dynamic memory on the Wi-Fi AP/Bridge. The logged events can be viewed through the command line interface (CLI) using the **show logging** command. The log file is cleared any time the Wi-Fi AP/Bridge is rebooted. The default is **DISABLED**; displaying system messages on this web page but not saving them in the Wi-Fi AP/Bridge.
- **Remote Logging:** Select **ENABLED** to send system messages to a remote host located at the IP address entered in the box next to this field. The remote host must first be configured to accept remote logging (syslogd -r at a minimum).
- **Commit:** Select this field to put these settings into effect.

Monitoring>SNMP Monitoring

Simple network management protocols (SNMP) use pre-defined sets of data for the Wi-Fi AP/Bridge called a management information base (MIB) to monitor network operations. The MIBs are defined in a way that allows third-party developers of network monitoring software to use them with their products. The Vivato Wi-Fi AP/Bridge has its own MIB, and also supports several industry standard MIBs. Refer to "**Network Monitoring**" on page 145 for more operation on using SNMP with the Vivato Wi-Fi AP/Bridge.

The Vivato Wi-Fi AP/Bridge supports SNMP versions 1, 2c, and 3. Some configuration settings are only used by a specific SNMP version. These settings are separated on the configuration web pages.

Base SNMP Options

These settings do not take effect until **Make Base SNMP Changes** is selected after entering your information:

- **Status:** Select **enable** or **disable** to turn SNMP on or off, respectively.
- **System Name:** Enter the name of the system that you are monitoring.
- **System Location:** Enter the physical location of the Wi-Fi AP/Bridge you are monitoring, such as "Shilshoal Marina" or "Museum of Flight".
- **System Contact:** Enter the name of the person(s) supporting this Wi-Fi AP/Bridge.
- **Current SNMP Community Settings:** To remove a community that had previously been added, you can select that setting to be removed when **Make Base SNMP Changes** is selected. To de-select a community, hold the **Ctrl** key down and click on it again.
- **Current Trap Sinks:** To remove a trap sink that had previously been added, you can select that setting to be removed when **Make Base SNMP Changes** is selected. To de-select a trap, hold the **Ctrl** key down and click on it again.

SNMP Configuration	
[Base SNMP Options]	[Community Options] [V3 Options] [V2 Options] [V1 Options]
Configure Base SNMP	
Status:	DISABLED ▼
System Name:	Unknown System Name
System Location:	Unknown Location
System Contact:	Unknown System Contact
Current SNMP Community Settings (select for removal)	Current Trap Sinks (select for removal)
public RO private RW	NO TRAP SINKS
Make Base SNMP Changes	

Figure 16—Base SNMP Options

Create an SNMP Community

Selecting Community Options accesses the following settings to create a new SNMP community. Settings are not configured until **Create New Community** is selected after entering your information.

SNMP Configuration	
[Base SNMP Options]	[Community Options] [V3 Options] [V2 Options] [V1 Options]
Create SNMP Community	
Community Name:	
Type:	RO ▼
IP Address (Optional):	
Create New Community	

Figure 17—Create an SNMP Community

- **Community Name:** Enter the name of an SNMP community to create.
- **Type:** Specify whether to create a read only (RO) or a read/write (RW) community.
- **IP Address (Optional):** Enter the IP address to use to access this community. If this option is used, only SNMP requests from the specified IP address are honored.

SNMP Version 3 Configuration Settings

The following settings are used to create an SNMPv3 trap sink and user.

Create an SNMP Version 3 Trap Sink

These settings are used to create an SNMPv3 trap sink. Settings do not take effect until **Create Trap Sink** is selected after entering your information.

The image shows a web-based configuration interface titled "SNMP Configuration". It has five tabs: "[Base SNMP Options]", "[Community Options]", "[V3 Options]", "[V2 Options]", and "[V1 Options]". The "[V3 Options]" tab is selected. Below the tabs, there are two main sections: "Create v3 Trap Sink" on the left and "Create v3 User" on the right. The "Create v3 Trap Sink" section includes fields for "Hostname/IP Address:", "Trap Sink Type:" (a dropdown menu currently showing "traps"), "Username:", "Optional Settings", "Authentication Type:" (a dropdown menu), "Password:", "Privacy Type:" (a dropdown menu), and another "Password:". At the bottom of this section is a yellow button labeled "Create Trap Sink". The "Create v3 User" section includes fields for "Username:", "Optional Settings", "Authentication Type:" (a dropdown menu currently showing "MD5"), "Password:", "Privacy Type:" (a dropdown menu currently showing "DES"), and another "Password:". At the bottom of this section is a yellow button labeled "Create SNMP User".

Figure 18—SNMP Version 3 Options

- **Hostname/IP Address:** Enter the host name or the IP address for creating the trap.
- **Trap Sink Type:** Specify whether to trap or to inform when a condition is detected.
- **Username:** Enter the user name.
- **Authentication Type:** Select the type of authentication: MD5 or SHA.
- **Password:** Enter the authentication password.
- **Privacy Type:** Select the encryption type to use (currently on DES is supported).
- **Password:** Enter the DES encryption password.

Create an SNMP Version 3 User

These settings create an SNMP version 3 user. Settings do not take effect until **Create SNMP User** is selected after entering your information.

- **Username:** Enter a user name.
- **Authentication Type:** Select the type of authentication to use with this user: MD5 or SHA.
- **Password:** Enter the password for this user.
- **Privacy Type:** Select the encryption type to use for this user (currently on DES is supported).

- **Password:** Enter the DES encryption password.

SNMP Version 2 Trap Sinks

The following settings are used to configure a trap or an inform for SNMP version 2. Changes do not take effect until **Create Trap Sink** is selected after entering your information.

SNMP Configuration				
[Base SNMP Options]	[Community Options]	[V3 Options]	[V2 Options]	[V1 Options]
SNMP v2 Options				
Hostname/IP Address:				
Trap Sink Type:		traps v		
Community Name:				
Create Trap Sink				

Figure 19—Creating an SNMP Version 2 Trap

- **Hostname/IP Address:** Enter the host name or the IP address for creating the trap.
- **Trap Sink Type:** Select the type of sink to create: **trap** or **inform**.
- **Community Name:** Enter the community name for the SNMP Trap to allow it to record traps from the Wi-Fi AP/Bridge.

SNMP Version 1 Traps

The following settings are used to configure a trap for SNMP version 1. Changes do not take effect until **Create Trap Sink** is selected after entering your information.

SNMP Configuration				
Base SNMP Options	[Community Options]	[V3 Options]	[V2 Options]	[V1 Options]
SNMP v1 Options				
Hostname/IP Address:				
Traps:				
Community Name:				
Create Trap Sink				

- **Hostname/IP Address:** Enter the host name or the IP address for creating the trap.
- **Community Name:** Enter the community name for the SNMP Trap to allow it to record traps from the Wi-Fi AP/Bridge.

Monitoring>Associated Clients

This table displays the number of clients that are currently associating with the Wi-Fi AP/Bridge on each wireless interface. Selecting the value displays a table of information for each client. This is helpful in understanding which clients are being serviced, the MAC address and IP address of each client, and the data rate of the connection to each client.

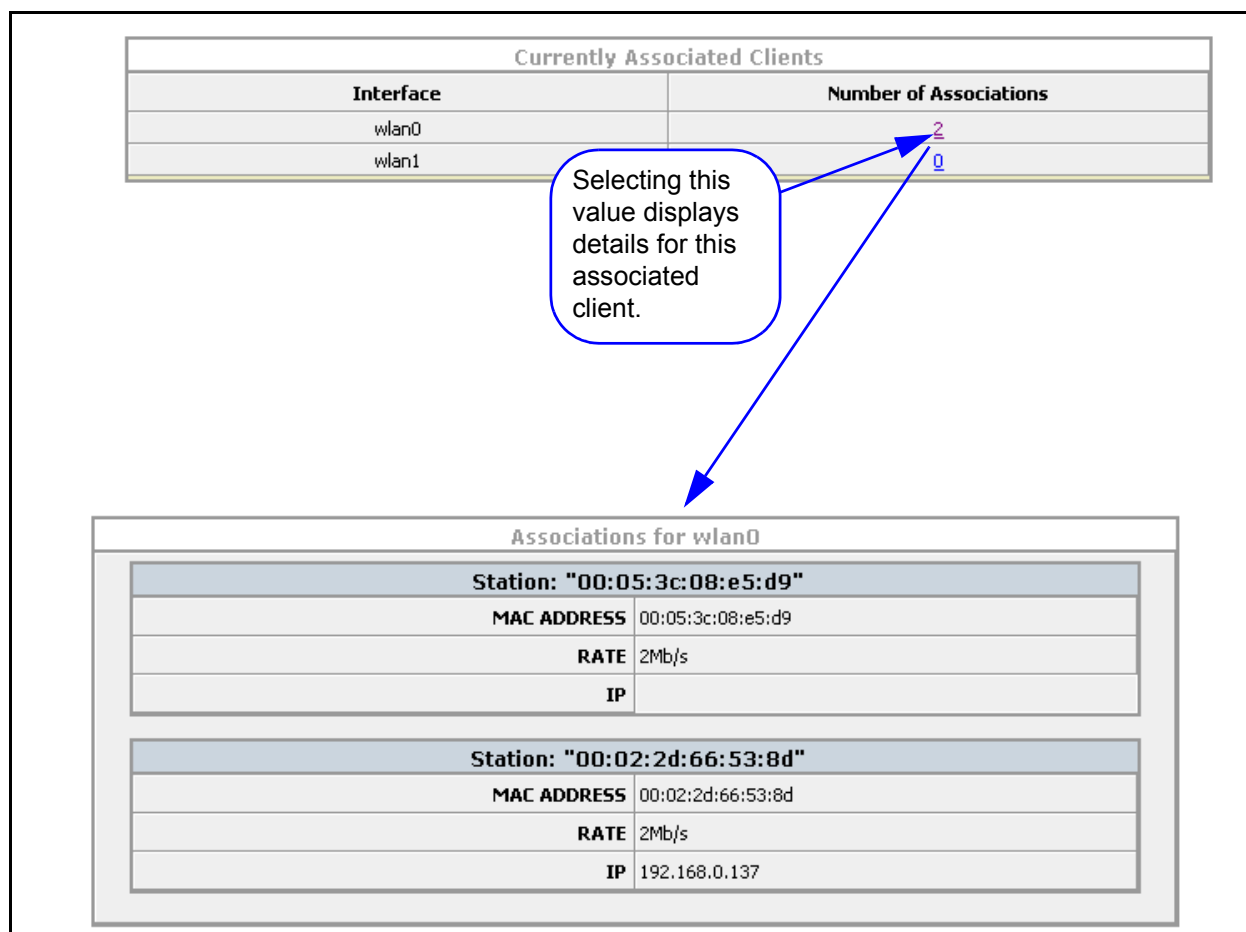


Figure 20—Example Associated Clients Information

Services, Password, Config, and Firmware Web Pages

The **System** web screens are used to view the current running configuration, enable and disable HTTP and SSH connections to the Wi-Fi AP/Bridge, change the system passwords, save and transfer configuration files, and install new firmware in the Wi-Fi AP/Bridge.

System Settings

System settings are arranged on the following configuration pages:

- [System>Summary](#)
- [System>Services](#)
- [System>Password](#)
- [System>Config](#)
- [System>Firmware](#)
- [System>Quick Setup](#)

System>Summary

This screen displays some current configuration information, such as the host name, the current firmware revision in the Wi-Fi AP/Bridge, and the web server software version. When in enable mode, the command line interface listing of the current (running) configuration is also displayed.

System Configuration Summary	
Hostname:	Vivato
Firmware Version:	vino.br.1.0.b17
WebServer Software:	VIVATO::vino_httpd
Running Configuration:	<pre>username admin secret 5 D3fQLm6oWlMqA ! ip hostname Vivato ! interface ethernet 0 no shutdown ! interface wireless 0 channel 1 ssid spongebob key s:gmV8a18436572 1 wep 1 no shutdown ! interface wireless 1 channel 11 ssid Vivato key s:gmV8b81345627 1 wep 1 wds 1 peer-address 00:0b:33:00:60:0e</pre>

Figure 21—Example System Summary Screen

System>Services

Services lets you set or change the Wi-Fi AP/Bridge's host name, reboot the Wi-Fi AP/Bridge, return to the AP/Bridge to its default configuration, and enable or disable communications using secure shell or HTTPS protocols.

Set System Hostname New Hostname: Commit Reboot System To reboot the system please enter the current enable password for verification Enter Enable Password [?]: Reboot Reset System to Default Settings To reset the system please enter the current enable password for verification Enter Enable Password [?]: Reset	SSH Services Configuration SSH Enabled: ENABLED SSH User Enabled: Bind Interface: br0 Generate SSH-Keys: ☐ Make SSH Changes HTTP Services Configuration HTTPS Enabled [?]: ENABLED Make HTTP Changes
---	---

Set System Hostname

Enter a host name for the Wi-Fi AP/Bridge. The host name can also be set using the Quick Setup web pages. See ["Basic Network Setup"](#) on page 46.

Reboot System

Entering the enable password and selecting Reboot causes the Wi-Fi AP/Bridge to reboot using the last configuration saved as "startup-config".

Rebooting causes any unsaved configuration changes to be discarded. To preserve your current configuration, use Configuration File Options to save your configuration (see ["System>Config"](#) on page 88).

Reset System to Default Settings

Entering the enable password and selecting **Reset** causes the Wi-Fi AP/Bridge to reboot using the original factory configuration. This is used to clear the current settings and start with a "clean" configuration. After resetting, the default IP address (169.254.20.1) must be used to access the AP/Bridge.

This function renames the last saved configuration "startup-config.bak" and reboots the AP/Bridge. Since the AP/Bridge cannot find the "startup-config" file on reboot, it uses the initial product settings.

To use the "startup-config.bak" file to restore the last saved configuration, rename the file to "startup-config" and reboot.

Important 	Reset sets the IP address of the Wi-Fi AP/Bridge to 169.254.20.1, and all other configurations are returned to their factory defaults, including disabling all security settings. See "Steps to Configuring the Vivato Wi-Fi AP/Bridge" on page 35 to begin re-configuring the Wi-Fi AP/Bridge.
--	---

SSH Services Configuration

The secure shell (SSH) configuration effects access to the Wi-Fi AP/Bridge using a secure shell client. Changes do not take effect until **Make SSH Changes** is selected.

- **SSH Enabled:** Enable or disable the use of a secure shell to access the configuration settings.
- **SSH User Enabled:** (*Reserved for future operation.*)
- **Bind Interface:** Specify the interface on the Wi-Fi AP/Bridge to use for secure shell (SSH) access. When this feature is issued, only the IP address on that interface can be used to access the AP/Bridge through SSH. If an IP address has not been assigned to this interface, SSH access is not restricted.
- **Generate SSH-Keys:** Check this box to regenerate keys required for secure shell operation. These keys are generated whenever a new firmware image is booted for the first time, so your Wi-Fi AP/Bridge has the proper SSH keys when delivered.

HTTP Services Configuration

HTTP services configuration enables and disables the ability to access the Wi-Fi AP/Bridge's built-in configuration web pages. Changes do not take effect until **Make HTTP Changes** is selected.

HTTPS Enabled: Enable or disable hyper-text transfer protocol secure (HTTPS) access to the configuration web pages.

System>Password

This page is used to change the passwords that let you read the current configuration and enable access to change the configuration. These are the same passwords that are configured on the Quick Setup pages. For both passwords, you need to enter the existing password once and then enter the new password twice. The new password(s) do not take effect until **Change Password** is selected for the associated password.

No enable password is set until you create it. If you did not create an enable password during the initial configuration using the Quick Setup pages, leave the “Current Password” field blank the first time you set the enable password.

Password Settings	
Change "Read" Password Current Password: New Password: New Password Verification: Change Password	Change "Enable" Password Current Password: New Password: New Password Verification: Change Password

Figure 22—Changing the Read and Enable Passwords

System>Config

The Configuration page is used to save the current Wi-Fi AP/Bridge configuration for later use, rename or delete a configuration file, load a previously saved configuration, and send a configuration to a remote Wi-Fi AP/Bridge. Whenever you change configuration settings that you intend to use, you should always save those settings in your configuration file to prevent losing those changes if power to the Wi-Fi AP/Bridge is momentarily lost or if the AP/Bridge is rebooted.

The Wi-Fi AP/Bridge always uses the default configuration file entitled “startup-config” *whenever a reboot occurs*.

Switch Configuration Options	
Save Running Configuration to Flash Save	Save Running Configuration to File Filename: Save
Configuration Management Configuration File: startupbak Rename File to: Rename Delete	Copy Configuration File to Remote Switch Remote Host: Remote Password: Local File: startupbak Remote Filename: Push Config File

- **Save Running Configuration to Flash:** Save the current configuration settings as the default “startup-config” file. The next time you reboot the Wi-Fi AP/Bridge, these configuration settings are automatically used.
- **Configuration Management:** Rename or delete an existing configuration file. Multiple configuration files can be saved and retrieved for later use if desired.
 - ◇ **Configuration File:** Select the configuration file to rename or delete.
 - ◇ **Rename File To:** Enter the name to use for renaming the selected configuration file.
 - ◇ **Rename:** Select to rename the specified configuration file.
 - ◇ **Delete:** Select to delete the specified configuration file.
- **Save Running Configuration to File:** Enter a file name for saving the current configuration when **Save** is selected.
- **Copy Configuration File to Remote Switch:** *(Reserved for future operation.)*

System>Firmware

(Firmware Updates Using the Web Interface Are Not Supported in This Firmware Release - Use the Command Line Interface for Updating Firmware. See "Commands for Managing Configuration Files" on page 114.)

The firmware in the Wi-Fi AP/Bridge determines which features are available and how they operate. As improvements to the firmware are developed by Vivato, the newer version can be loaded into your Wi-Fi AP/Bridge to provide new features and increase performance.

Images are saved as binary (.bin) files.

The following functions are used to manage the firmware in your Wi-Fi AP/Bridge.

Firmware Download Options - Temporarily Unavailable	
Download Firmware Image from SSH Server	Download Firmware Image from TFTP Server
Remote Host:	Remote File:
Remote Username:	TFTP Server:
Remote Password:	
Remote Path:	
Remote FW Image:	

Local Firmware Options

Local Firmware Options are used to load and manipulate firmware images for the Wi-Fi AP/Bridge to which you are connected.

Download Firmware Image From TFTP Server

This function is used to download a new firmware image from a TFTP server to the Wi-Fi AP/Bridge.

- **Remote File:** Enter the file name of the firmware image that you want to download.
- **Save File To Flash as:** Enter the name to use when saving the firmware image on the Wi-Fi AP/Bridge.
- **TFTP Server:** Enter the host name or IP address of the TFTP server where the firmware file resides.
- **Download:** Download the firmware file to the Wi-Fi AP/Bridge's flash memory.

Important	DO NOT INTERRUPT THE COPYING PROCESS!
	The AP/Bridge can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the AP/Bridge to operate.

Download Firmware Image From SSH Server

This function is used to download a new firmware image from a secure server to the Wi-Fi AP/Bridge.

- **Remote Host:** Enter the host name or IP address of the server where the firmware file resides.
- **Remote User Name:** Enter a user name configured on the remote server.
- **Remote Password:** Enter the password for the entered user name.
- **Remote Path:** Enter the directory path for the image to download, using the format in the following example: **//vivato/bridge_router/firmware_images**
- **Remote FW Image:** Enter the file name of the firmware image (.bin file) that you want to download.
- **Download:** Download the firmware file to the Wi-Fi AP/Bridge's flash memory.

Important



DO NOT INTERRUPT THE COPYING PROCESS!

The AP/Bridge can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the AP/Bridge to operate.

System>Quick Setup

Displays the initial Quick Setup screen to access the quick setup pages and make any changes. See ["Steps to Configuring the Vivato Wi-Fi AP/Bridge"](#) on page 35.

System Settings

Services, Password, Config, and Firmware Web Pages

Diagnostics Web Screen and Help

A **Diagnostics** web page is available to troubleshoot communications problems, and a **Help** link is provided to access the Vivato Customer Support website (requires Internet access).

Diagnostics

Diagnostics settings are used to verify and troubleshoot packet transfer between the Wi-Fi AP/Bridge and connected networks.

Diagnostics>Tools

The Ping and Traceroute functions are used to verify access to selected hosts and to see the route used to access them.

Ping

Pinging tests to see if you can communicate with another device on the network. Packets are sent to the device, which in turn responds by sending return packets if communication is successful. If communication fails, an “unknown host” message is displayed or the command times out with no reply. An example successful ping result is shown below.

- **Host:** Enter the IP address or host name for the device you are trying to access. When specifying the host name, the name and IP address must first be entered into the Wi-Fi AP/Bridge’s host table. See ["Create a New Host"](#) on page 59.
- **Ping Count:** Select the number of 64-byte packets to send during the pinging operation.
- **Start Ping:** Ping the specified host.

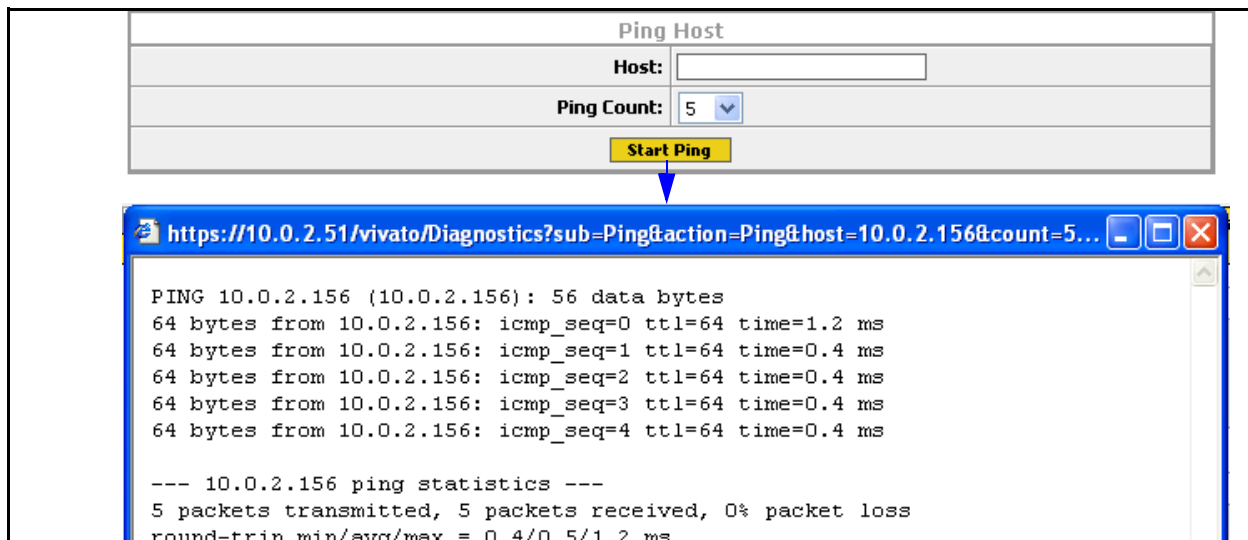


Figure 23—Example Results of Pinging a Host With Five Packets

Traceroute

Traceroute displays the IP addresses of devices used to access a device at a specified destination IP address or host name, the size of the packets transmitted, and the amount of time used for each “hop” between network devices.

Traceroute

Host:

Start Traceroute

```

traceroute to 192.165.0.165 (192.165.0.165), 30 hops max, 40 byte packets
 1  192.165.0.165 (192.165.0.165)  0.731 ms  0.936 ms  0.609 ms
            
```

Diagnostics>Arp

Address resolution protocol (ARP) associates a device’s IP address with its unique hardware medium access control (MAC) address. When the Wi-Fi AP/Bridge sends an ARP request for a specific IP address, the MAC of the device with that address is returned and is entered into the ARP Information table (see below).

ARP Information					
IP Address	Type	Flags	Hardware Address	Mask	Interface
192.165.20.4	ARPA	0x2	00:09:6B:10:5A:C6	*	br0
192.165.20.45	ARPA	0x2	00:50:70:52:0B:14	*	br0

Help

Selecting the **Help** tab causes the Wi-Fi AP/Bridge to access the Vivato Customer Support sign-in screen. After entering your Customer Support user name and password, you can access a variety of support information and firmware downloads for your Wi-Fi AP/Bridge.

Configuration Using The Command Line Interface

Refer to "[Default Configuration](#)" on page 36 before performing additional configuration using the CLI.

Refer to the *CLI Quick Reference.pdf* file on the Vivato CD-ROM for a concise listing of all CLI commands.

The command line interface (CLI) is used to change settings and query values in the Vivato Wi-Fi AP/Bridge; it is an alternative to using the web page interface. The CLI can be used to initially configure the Wi-Fi AP/Bridge for operation and to update the configuration after installation. Configuration files can be saved and retrieved to backup the configuration or to reconfigure the AP/Bridge. The CLI can also be used to monitor activity during AP/Bridge operation. Passwords are used to prevent unauthorized access to the CLI.

Caution



To prevent unauthorized access to the AP/Bridge's configuration, the system administrator should use the [enable secret \[<password type \(0|5\)>\] <password text>](#) and [username admin secret \[<password type \(0|5\)> <password text>](#) commands to set and save new passwords before putting the AP/Bridge into service.

Understanding How the CLI is Used

[Command Levels](#)

[Connections and Terminal Settings](#)

[Accessing the CLI](#)

[Configuration Example](#)

[Navigating the CLI](#)

Command Descriptions

[Read Level Command Descriptions](#)

[Enable Level Command Descriptions](#)

Command Levels

The commands are arranged in a hierarchical structure. The top level is the “**read**” level. Read level commands access system information and utilities used to monitor the overall status of the AP/Bridge and perform some troubleshooting operations.

The second command level is the “**enable**” level. Enable level commands are used to configure the AP/Bridge. Almost every function in the Vivato Wi-Fi AP/Bridge can be accessed using these commands. The enable level is accessed when you enter the **enable** command at the read level prompt. An additional password is required to access the enable level commands. Enable level commands are arranged in a number of sub-levels for configuring specific operations.

Important	Configuration changes are not saved until you issue the write network flash: or write [memory] command. Turning the Wi-Fi AP/Bridge off causes the last saved configuration to be used when power is restored. If power is interrupted before saving your changes, those changes are lost.
-----------	--

Connections and Terminal Settings

Commands can be entered on a computer using either of following methods:

- Running a Secure Shell (SSH) session configured for TCP/IP, and connected to the Wi-Fi AP/Bridge's Ethernet port (use the supplied crossover cable when connecting the AP/Bridge directly to your computer's network interface card). Use the AP/Bridge's IP address when configuring communications. The default IP address when shipped is 169.254.20.1, which is assigned to the default bridge: br0. The user name is "admin" and the password is "vivato". Your network interface's IP address must be set to be able to work with the Wi-Fi AP/Bridge. See ["Enabling Your Computer's Network Adapter to Access the Wi-Fi AP/Bridge"](#) on page 37.
- Running a terminal emulator and connecting to the AP/Bridge's RS-232 serial (console) port with the supplied DB-9 null modem cable.

Emulating a VT100 terminal with the following settings typically works well:

- Baud: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Xon/Xoff

If the **vivato** prompt does not appear immediately after starting your terminal emulator, press the **Enter** key on your computer a few times to get a prompt. If no prompt appears, check your cable connections and terminal emulator settings.

Accessing the CLI

After connecting the AP/Bridge to your computer and initiating communications, a command prompt should be displayed on your computer. The following example illustrates how to access the read level using the SSH Secure Shell® client:

- 1 Using the Quick Connect feature of the secure shell client, enter the IP address of the Wi-Fi AP/Bridge and enter “**admin**” for the user name, and select **Connect** to begin the session.
- 2 Enter the read level password . The password is not displayed as you enter it.

Note: Until you change it, the password is **vivato**.

- 3 If you enter a question mark at the prompt, a list of the available read level commands is displayed (as shown in the example below).

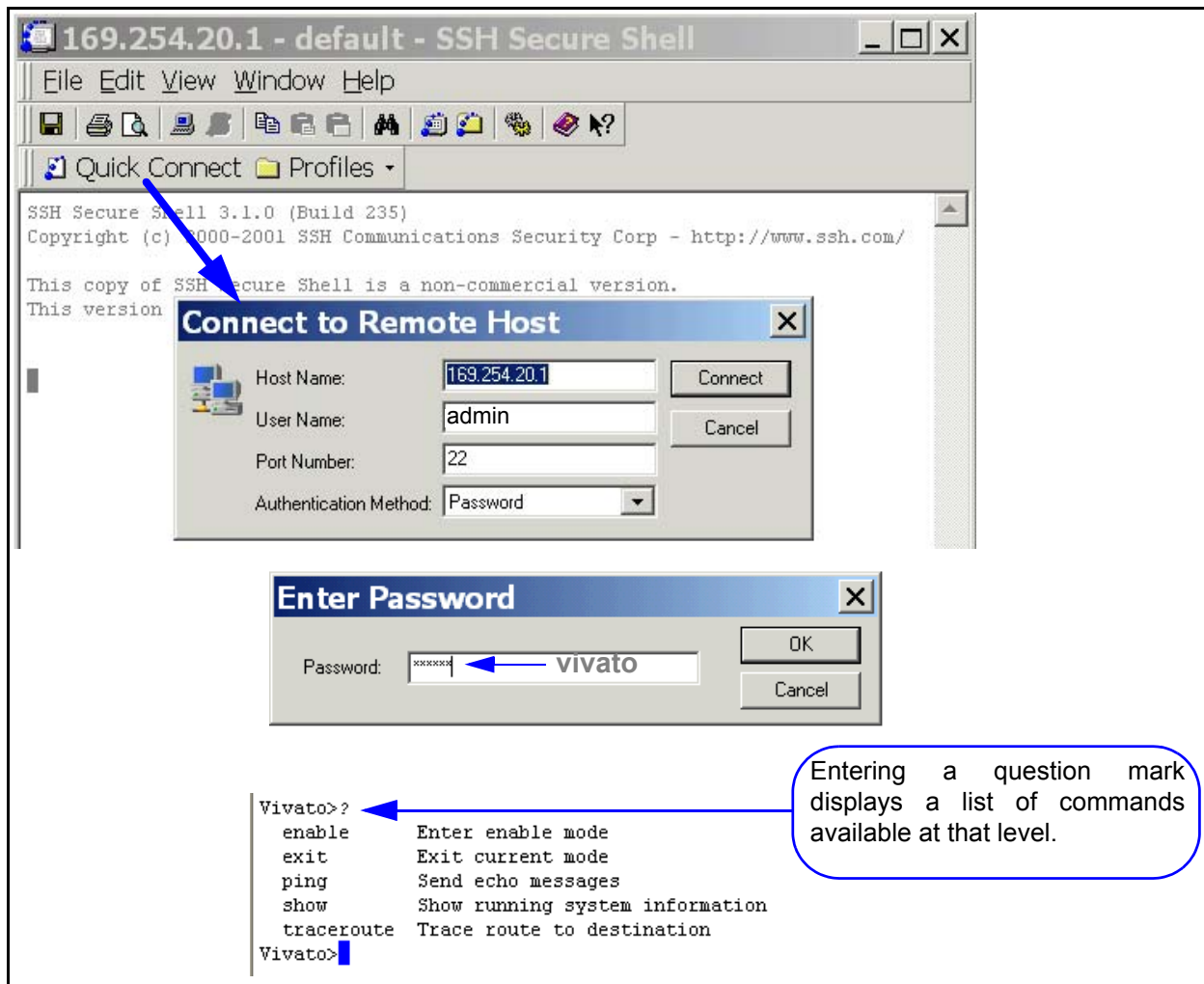


Figure 24—Using Secure Shell to Access the CLI and Display Read Level Commands

Accessing the Configuration Level

Use the following steps to access the enable level from the read level, and then access the global level of the configuration settings:

- 1 At the **vivato>** prompt, enter **enable**.
- 2 The Wi-Fi AP/Bridge is shipped without an enable password. If you have created an enable password (when using the Quick Setup web pages or by using the CLI), enter that password when prompted.
- 3 Enter **configure terminal** to access the global configuration level. The prompt changes to **vivato (config)#**. At this point you can start configuring the Wi-Fi AP/Bridge.

```
Vivato>
Vivato>enable
Password:
Vivato#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Vivato(config)#
```

Figure 25—Accessing the Global Configuration Level

Configuration Example

This example configures the Wi-Fi AP/Bridge as an access point using WEP security. Some settings are already provided in the default configuration, but are shown here to illustrate how they are set.

Change settings as needed for your desired configuration. The example begins at the initial command prompt:

login: admin	Enter the user name.
password: vivato	Enter the default read password.
vivato> enable	Enter the enable mode.
vivato# configure terminal	Enter the configuration mode.
vivato (config)# interface wireless all	Configure all wireless interfaces (wlans).
vivato (config-wlan-all)# essid jims_java	Set ESSID to "jims_java".

Configure WEP security

vivato (config-wlan-all)# key s:jimsgr8coffee 1	Enter a 104-bit WEP key 1 as a string.
vivato (config-wlan-all)# wep 1	Enable WEP operation using key #1.
vivato (config-wlan-all)# exit	Stop configuring all wlans together.

Configure the wireless interfaces to provide one channel operation (default).

```
vivato (config)# interface wireless 0
vivato (config-wlan0)# channel 1
vivato (config-wlan0)# exit
vivato (config)# interface wireless 1
vivato (config-wlan1)# shutdown
vivato (config-wlan1)# exit
```

Create the default bridge (br0), and add each Ethernet and wireless interface to the bridge.

```
vivato (config)# interface bridge br0
vivato (config-br0)# add interface ethernet 0
vivato (config-br0)# add interface wireless 0
vivato (config-br0)# add interface wireless 1
vivato (config-br0)# no shutdown
```

Specify the IP address and netmask for bridge 0 (br0). This sets the IP address for the Wi-Fi AP/Bridge in your network.

```
vivato (config-br0)# ip address 192.165.0.10 255.255.255.0
vivato (config-br0)# exit
```

Generate the secure shell key and enable the secure shell daemon (default).

```
vivato (config)# ip ssh genkey
vivato (config)# ip ssh server
```

Enable the HTTP daemon for web access (default).

```
vivato (config)# http-server
```

Define the basic network settings

vivato (config)# ip domain-name javaplanet	Set the domain name to “javaplanet”.
vivato (config)# ip routing	Enable global IP routing.
vivato (config)# ip name-server 192.165.0.99	Specify a name server on your LAN.
vivato (config)# ip hostname french_roast	Set the host name to “french_roast”

Set the read and enable passwords. After an enable password has been specified, you will need to enter that password anytime you attempt to access the enable level.

french_roast (config) username admin secret coffeem8	Set read level password.
french_roast (config) enable secret sixty6flavors	Set enable level password.

Save the configuration inside the Wi-Fi AP/Bridge (as “startup-config”) and end the configuration session.

```
french_roast (config)# exit
french_roast# write
french_roast# exit
```

Navigating the CLI

Several keystroke sequences are available to move between levels on the CLI and move the cursor on the command line, and to get helpful information online.

Moving the Cursor Around on the Command Line

You can use the following commands to move the cursor on the command line when making changes to settings:

Table 1—Command Line Shortcuts

Keystrokes	Function
Ctrl-B or left arrow key*	Moves the cursor back one character without erasing the character.
Ctrl-F or right arrow key*	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Ctrl-U	Removes all text on the command line.
* The arrow keys may not work with some terminal emulators.	

Using the “?” to Get Online Command Help

At any prompt on the command line you can enter a question mark (?) to get a list of the available commands at that level, along with a short description of each command. This can be helpful when you enter a command and get an “Invalid command due to syntax or parameter” error.

To get information on a specific command, such as the format of the command or additional specifiers used by that command, type the command, a single space, and then the question mark. For example: **enable**<space>? displays information on the enable commands.

Using the Tab Key to Complete a Command

Instead of individually keying-in every character of a command, you can enter the first few characters and press the **Tab** key to automatically fill in the remainder of that command. For example, to enter the “show running-configuration” command, you could enter “sh **Tab** ru **Tab**”. This feature increases the rate at which you can enter commands, and often reduces the number of keystroke errors.

Command Mode Access and Prompts

The following table lists the various commands and keystrokes used to access the main command levels:

Table 2—Command Mode Navigation

Command Level	How to Access	Resulting Command Line Prompt	To Go Back to the Previous Level
Read	Default state.	vivato>	
Enable	From the read level, enter enable and the enable password	vivato#	Type “disable”.
Enable (Global Configuration)	From the Enable level, enter configure terminal	vivato (config)#	Type “exit”.
Configure Specific Functions	At the global configuration prompt, enter the appropriate configuration command. For example, entering interface ethernet 0 accesses the configuration settings for the ethernet 0 port.	Depends on the configuration function. For configuring the wireless interface, the prompt would be vivato (config-eth0)#	Type “exit” to return to the global configuration prompt. You also enter Ctrl-z to exit the global configuration mode are return to the initial enable prompt.

Command Conventions

Use the following conventions when entering commands and to understand the command listing used in this manual.

Entering Commands on the Command Line

*Most commands are entered using lower case letters, such as **configure terminal**. Do not substitute upper case letters, such as CONFIGURE TERMINAL or Configure Terminal. When upper case letters are shown in the command listing, use the upper case letters where indicated.*

Reading the Command Listing

Command list headings with initial upper case letters identify a group of related commands that are listed under it. For example, **Configure Interface Commands** is the heading for the list of all of the commands that are used to configure the ethernet and wireless interfaces. The actual commands used to configure the interfaces are listed under this heading using all lower case letters (such as **interface wireless**).

Entering Variables

Some commands only perform an immediate action (such as the **enable** command) or always require text or a number to be entered (such as the **interface wireless** command). It is assumed that you press the **Enter** key after typing in these commands .

Some commands may use a default of just pressing **Enter** after issuing the command, but also provide the use of specifying a file name or other text. These commands are listed in both forms, such as **write** and **write file <filename>**.

Optional Entries

Some commands use optional specifiers or entries. These are indicated by using brackets, [], in the command listing. For example, the following command contains optional entries:

snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> [auth MD5|SHA <password> [priv DES <password>]]

Read Level Command Descriptions

The following commands are available at the read level.

enable

Enter the enable mode. This command must be issued any time you are going to change any AP/Bridge configuration settings. The enable password is required before access to configuration settings is allowed.

exit

Exit the configuration session to stop using the command line interface.

Ping

Send an echo message to another device. Pinging a device is used to see if you can communicate with a device at a specified IP address or that has a local host name. A packet is sent to the device, which in turn responds by sending return packets if communication is successful. If communication fails, an “unknown host” message is displayed or the command times out with no reply.

Ping commands are available at both the read and enable levels.

ping <ipaddress|hostname>

Specify the IP address to ping using 5 packets.

ping flood <ipaddress|hostname>

Specify the IP address or host name of a device to ping without waiting for a response before sending each packet. Packets are sent continuously as fast as possible until you press **Ctrl-C** on your computer. *This command should be used with caution, since it causes a very high level of network traffic while executing.*

ping flood

Enter this command to ping a host computer named “flood”.

ping flood count <1-100000> <ipaddress|hostname>

Specify the IP address or host name of a device to ping, and the number of packets to send, without waiting for a response before sending each packet. Packets are sent as fast as possible until the count has elapsed or until you press **Ctrl-C** on your computer.

ping count <1-100000> <ipaddress|hostname>

Specify the number of packets to use, and the IP address or host name, to ping a device. The Wi-Fi AP/Bridge waits for a reply from the host after each packet is sent before another packet is sent.

ping count <1-100000> flood <ipaddress|hostname>

Specify the number of packets to send, and the IP address or host name of a device, to ping without waiting for a response before sending each packet. Packets are sent as fast as possible until the count has elapsed or until you press **Ctrl-C** on your computer.

Show Commands

Show commands display system information. Some Show commands are available at the read level, but all show commands are available at the enable level.

Some commands, such as “show interfaces”, may display more than one page of information on your screen. To view all of the contents, you may need to use the Shift+PageUp and Shift+PageDown keys.

Read Level Show Commands

The following Show commands are available at the read level:

show arp

Displays a list of the IP addresses and the corresponding medium access control (MAC) addresses for associated devices using address resolution protocol (ARP).

```
Vivato#show arp
IP address      HW type  Flags      HW address    Mask        Device
195.145.0.240   0x1      0x2        00:09:6B:8C:2D:F2  *          br0
195.145.0.99    0x1      0x2        00:50:70:52:0B:14  *          br0
195.145.0.107   0x1      0x2        00:09:6B:10:5A:C6  *          br0
195.145.0.57    0x1      0x2        00:02:2D:66:53:8D  *          br0
Vivato#
```

Figure 26—Example “show arp” Output

show cpu

Displays central processor unit information.

show dhcp-server interface bridge <0-4094>

Enter the bridge number to display the DHCP settings for that interface.

```
Vivato#show dhcp-server interface bridge 0
DHCP status for br0:
 ip-pool 192.163.0.20 192.163.0.100 255.255.255.0
 broadcast-address 192.163.0.255
 gateway 192.163.0.199
 name-server 192.163.0.198
 ntp-server 192.163.0.197
 lease 36000
 domain-name vivato
 status UP
Vivato#
```

Figure 27—Example “show dhcp-server interface bridge 0” Output

show dhcp-server interface ethernet <0>

Display the DHCP settings for the Ethernet interface.

show dhcp-server interface wireless <0-1>

Enter the wireless interface number to display the DHCP settings for that interface.

show eap

Displays the current settings and configuration for extensible application protocol (EAP). This command is only available at the wireless interface prompt.

```
Vivato(config-wlan0)#show eap
Eap Status:Enabled
Eap Rekey Period:60
Primary Radius Server :192.168.10.24 1812
Primary Secret String :XXXXXXX
Secondary Radius Server :192.168.10.252 1812
Secondary Secret String :XXXXXXX
Vivato(config-wlan0)#
```

Figure 28—Example “show eap” Output

show http-server

Displays the state of the http daemon: enabled or disabled.

show iccf

Displays the state of inter-client communication filtering (ICCF) for the currently selected interface (wlan0, wlan1, or br0).

show interfaces

Displays information about bridge, ethernet, and wireless interfaces, including their MAC addresses, IP addresses, and packets transmitted and received through each interface.

show interfaces bridge [0-4094]

Displays the configuration of all or (optionally) a specific bridge, including the IP and MAC addresses for that bridge, the transmit and receive statistics, whether spanning tree protocol (STP) is enabled, and which interfaces are part of each bridge.

Also shown is the status of that interface. When the interface is enabled, “UP BROADCAST RUNNING MULTICAST” is displayed. If the interface is disabled, the “UP” part is removed (“BROADCAST RUNNING MULTICAST”).

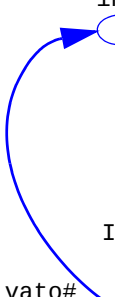
The Bridge ID consists of two values: the bridge’s priority setting is the value to the left of the decimal point (default is 8000), the lowest MAC address in the Wi-Fi AP/Bridge is to the right of the decimal point. The priority setting is used by spanning tree protocol to determine which bridge has priority when multiple AP/Bridges are used in a network. If the priority setting of all bridges is the same, the lowest MAC address is used to determine priority.

For information on RX and TX packet statistics, see [show interfaces wireless <0-1>](#).

```
Vivato#show interfaces bridge 0
br0      Link encap:Ethernet  HWaddr 00:0B:33:00:60:00
         inet addr:192.163.20.1 Bcast:192.163.20.255 Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500
         RX packets:3779 error:0 dropped:0 overruns:0 frame:0
         TX packets:42 error:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         Interrupt:0 Base address::

         Bridge ID:8000.000b33006000, STP:Disabled
         Interface: eth0, eth1, wlan1, wlan2, wlan3, wlan4, wlan5, wlan6

Vivato#
```



“UP” Signifies that this interface is enabled.

Figure 29—Example “show interfaces bridge” Output

[show interfaces bridge <0-4094> fdb](#)

Enter the number of a bridge to display the source MAC addresses of packets that have been forwarded through that bridge over any of its interfaces; also called the forwarding data base. The length of time that the data is stored in that data base is determined by the [aging-time <10-1000000 seconds>](#) command. A “local” device indicates an interface that is part of this bridge.

```
Vivato#show interfaces bridge 0 fdb
br0:
port no mac addr          is local?      ageing timer
1    00:09:6b:e0:9e:bf     no             7.59
1    00:09:7c:45:5b:8f     no             0.27
1    00:0b:33:00:60:00     yes            0.00
2    00:0b:33:00:60:01     yes            0.00
3    00:0b:33:00:60:09     yes            0.00
```

Figure 30—Example “show interfaces bridge 0 fdb” Output

[show interfaces bridge <0-4094> stp](#)

Enter the number of a bridge to display the status of spanning tree protocol (STP) on that bridge: enabled or disabled.

[show interfaces ethernet \[0\]](#)

Displays the configuration for the ethernet interface, including the IP address (if assigned) and broadcast address, MAC address (HWaddr), bridges that this interface is part of, and transmit and receive packet statistics.

Also shown is the status of that interface. When the interface is enabled, “UP BROADCAST RUNNING MULTICAST” is displayed. If the interface is disabled, the “UP” part is removed (“BROADCAST RUNNING MULTICAST”).

For information on RX and TX packet statistics, see [show interfaces wireless <0-1>](#).

```
vivato(config)#show interfaces ethernet 0
eth0      Link encap:Ethernet  HWaddr 00:0B:33:00:60:00
          inet  addr:192.163.20.6    Bcast:192.163.20.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:6131 error:0 dropped:0 overruns:0 frame:0
          TX packets:236 error:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:16  Base address::0xd000
          Bridged : [br0]

vivato(config)#
“UP” Signifies that this
interface is enabled.
```

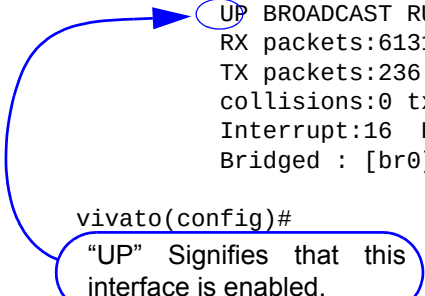


Figure 31—Example “show interfaces ethernet” Output

show interfaces wireless [associations]

Displays the configuration of all wireless interfaces or, optionally, information about clients associating through all wireless interfaces.

Configuration information includes the ESSID and WEP encryption key value (if used), channel assignment, association with any bridges, and bit rate for each wireless interface. See [Figure 32—Example “show interfaces wireless 1” Output](#), for an example of what is displayed for each interface.

show interfaces wireless <0-1> associations

Displays information about clients associating through the specified wireless interface, including the MAC address, connection rate of the last packet received, and the IP address of the client.

```
Vivato#show interfaces wireless 0 associations
Associations on wlan0:
1  00:02:2d:66:53:8d 2Mb/s 192.168.0.118

Vivato#
```

WDS connection information is not included (see [show interfaces wireless <0-1> wds <1-6>](#)).

show interfaces wireless <0-1>

Displays the configuration and operating statistics of a specified wireless interface. The following information is reported:

- Link encap: Ethernet - Always indicates Ethernet packet encapsulation is used.
- HWaddr: The MAC address for this wireless interface.
- UP BROADCAST RUNNING MULTICAST - Displayed when this interface is up (not shut down).
- BROADCAST MULTICAST - Displayed when this interface is shut down.
- MTU 1500: The maximum transmission unit (MTU) is the maximum number of bytes sent per packet on this interface. This value is fixed at 1500.
- RX packets: The total number of frames received on this interface since the Wi-Fi AP/Bridge was last booted. The following received packet statistics are also displayed:
 - error: The number of frame check sequence (FCS) errors in received frames. This value includes errors detected in ALL packets received on that interface, whether they are from an intended client or broadcast from another source. In an environment with several clients or other Wi-Fi devices, this number can seem larger than expected, but it does not necessarily indicate a problem with this wireless interface or the intended clients.
 - dropped: The number of frames that were not buffered and were discarded, not counting WEP and WEP ICV errors.
 - overruns and frame: Not used at this time.
- TX packets: The total number of frames transmitted on this interface since the Wi-Fi AP/Bridge was last booted. The following transmitted packet statistics are also displayed:
 - error: The number of transmission retries that exceeded the retry limit.
 - dropped: The number of packets that have been discarded.
 - overruns and carrier: Not used at this time.
- Interrupt and Base address: Internal hardware interface settings.
- Bridged: Displays the bridge (if any) that this interface is part of.
- ESSID: The extended service set identifier for this interface.
- Beacon ESSID: Enabled or disabled. See "[disable beacon-ssid](#)" on page 128.
- Channel: The channel that this interface is using to transmit and receive.
- Access Point: See HWaddr above.

- Bit Rate: This is the maximum bit rate supported on this interface. This value cannot be changed.
- Beacon Interval: See "[beacon-interval <0-8191>](#)" on page 128.
- Sensitivity: See "[sensitivity <1-3>](#)" on page 132.
- Encryption key: "Off" means that WEP is disabled. "XXXX" means that WEP is enabled and the "Encryption mode:" is set to restricted.
- RX invalid nwid, invalid crypt, RX invalid frag, Tx excessive retries, and Invalid misc, are not used at this time.

```
Vivato#show interfaces wireless 1
wlan1    Link encap:Ethernet  HWaddr 00:0B:33:00:60:09
          UP BROADCAST RUNNING MULTICAST  MTU:1500
          RX packets:23 error:553 dropped:0 overruns:0 frame:0
          TX packets:1228 error:54 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:21  Base address::0xd140
          Bridged : [br0]

          Essid:tripacer
          Beacon Essid: Enabled
          Channel:1  Access Point:00:0B:33:00:60:09
          Bit Rate:11Mb/s
          Beacon Interval: 0  Sensitivity:0
          Encryption key:XXXX  Encryption mode:restricted
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0 Invalid misc:0

Vivato#
```

Figure 32—Example “show interfaces wireless 1” Output

show interfaces wireless < 0-1> wds <1-6>

Enter the wireless interface number and wireless distribution system (WDS) port number to display that WDS configuration and operating statistics. The “HWaddr” shown is the MAC address that is automatically assigned for spanning tree protocol operation on that wireless interface and port. See [show interfaces wireless <0-1>](#) for a description of the other reported values.

The following example shows the WDS settings for wireless interface 1, port 2:

```
Vivato#show interfaces wireless 1 wds 2
wds1-2    Link encap:Ethernet  HWaddr 00:0B:33:31:80:09
          BROADCAST MULTICAST  MTU:1500
          RX packets:25 error:897 dropped:0 overruns:0 frame:0
          TX packets:1673 error:78 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:21  Base address::0xd140
          Bridged : [no]

Vivato#
```

show ip domainname

Displays the domain name for the Wi-Fi AP/Bridge.

show ip host

Displays the host table for the Wi-Fi AP/Bridge, containing host names and their IP addresses.

show ip hostname

Displays the host name for the Wi-Fi AP/Bridge.

show ip nameserver

Displays the IP address for any name servers that have been specified using the **ip name-server <ipaddress>** command.

show ip route

Displays IP routing information for the Wi-Fi AP/Bridge. Routes determine how packets with IP addresses within specified subnets are directed.

In the example below, host 145.88.47.9 can be accessed through gateway 195.145.3.150, by way of interface br0. All hosts on the 195.145.0.0 network can be accessed directly through interface br0. Destination 127.0.0.0 is the local host. The 127.0.0.0 route is the local host loop-back route. The flags “U” and “G” stand for “up” (status of the route) and “gateway”, respectively.

Table 3—Example IP Routing Information

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
145.88.47.9	195.145.3.150	255.255.255.0	UG	0	0	0	br0
195.145.0.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo

show ip ssh

Displays the state of the secure shell (SSH) daemon: enabled or disabled. If SSH operation has been bound to a particular interface using the **ip ssh bind interface (wireless <0-1>|ethernet 0|bridge <0-4094>)** command, that interface is also listed.

show logging

Displays a list of locally logged system events if logging has been enabled.

show memory

Displays information about installed memory and memory usage in the AP/Bridge.

show serial

Displays the product serial number.

show snmp-server

Displays simple network management protocol (SNMP) server status and configuration, such as the name, location, contact name, public and private community names, and host IP addresses.

```
harvey(config)#show snmp-server
snmp-server contact george
snmp-server location upstairs closet
snmp-server name clydesdale
snmp-server community public RO
snmp-server community private RW
snmp-server community icehouse RW 192.163.20.1
snmp-server engineID A52D
snmp-server
!
harvey(config)#
```

Figure 33—Example “show snmp-server” Output

show uptime

Displays the of day, how long the AP/Bridge has been up since it was last rebooted (days, hours, minutes), the number of users that have accessed the AP/Bridge, and the average load through the AP/Bridge.

show version

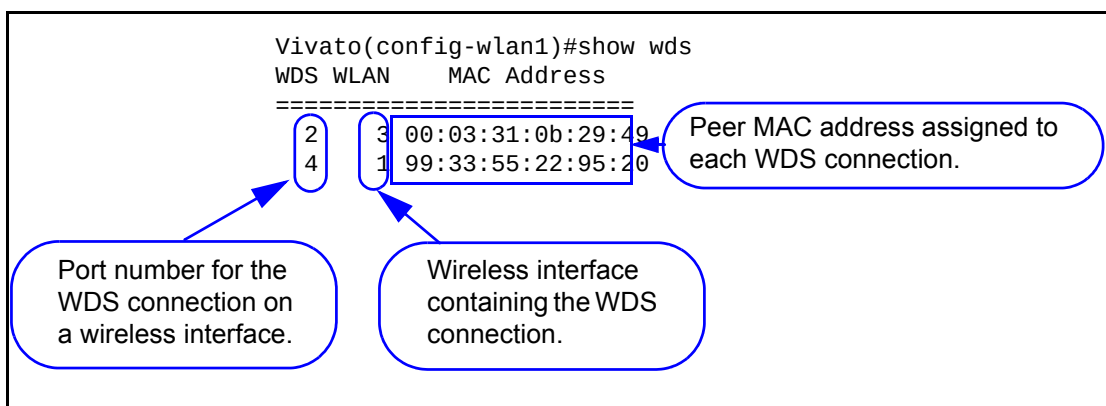
Displays the product serial number, base MAC address for the Wi-Fi AP/Bridge, and the versions of software (“Vino Version”).

Enable Level Show Commands

The following Show commands are only available at the enable level:

show wds

Display the wireless distribution system (WDS) connections that have been created and the peer MAC addresses that have been assigned to them.



show flash:

Displays the names of configuration files that have been saved in the Wi-Fi AP/Bridge. Configuration files are saved using the **write network flash:**.

show running-config

Displays the current running configuration of the Wi-Fi AP/Bridge, including any dynamic settings that are in effect.

traceroute <ipaddress|hostname>

Displays information about the network route used to access the specified destination address or host name. If the specified address or host is not found, the Wi-Fi AP/Bridge continues to try to locate it until you press the **Ctrl-C** keys.

Enable Level Command Descriptions

Refer to these sections for descriptions of commands that are available at the “enable” level (see **"enable"** on page 102).

Table 4—Enable Level Commands

configure [terminal]	Configure No Interface Commands
Commands for Managing Configuration Files	Configure Crypto (Generate Keys) Commands
EAP Commands (802.1x security)	
Configure Enable Secret Commands	Configure Log Commands
Configure HTTP-Server Commands	Configure IP Commands
Configure Interface Commands	Configure SNMP-Server Commands
interface bridge <0-4094>	
interface ethernet 0	
interface wireless < 0-1 all>	
Configure No SNMP-Server Commands	Configure Username Admin (Read Level) Secret
Configure WDS (Wireless Distribution System)	disable
edit flash:	edit flash:
exit	reboot
support	

[configure \[terminal\]](#)

This command tells the CLI to use your terminal to configure the AP/Bridge after accessing the enable level (see **"enable"** on page 102). After entering this command, the command prompt changes to vivato (config)# to indicate that you can now enter the following configuration commands.

Commands for Managing Configuration Files

The following commands are used to copy, write (save), delete, and retrieve firmware and configuration files on the Wi-Fi AP/Bridge. All of these commands are available at the enable level prompt, **Vivato#**, but are not available at the configuration prompt, **Vivato(config)#**.

[configure network flash:](#)

This command is used to configure the AP/Bridge using a saved configuration file. To view the currently saved configuration files, use the [show flash:](#) command. After entering this command, you are prompted to enter the name of the configuration file to use. The default is “startup-config”.

Important 	The default configuration file name is “startup-config”, and is created the first time you use the Quick Setup web pages for the initial configuration or when you save a configuration using that default file name. Once startup-config is created, the Wi-Fi AP/Bridge is <i>always</i> configured using that file whenever a reboot occurs by cycling power or by issuing the “reboot” command. To use a different configuration file as the default reboot configuration, use the copy flash: flash: command to rename that file “startup-config”. When you reboot the Wi-Fi AP/Bridge, the settings in the new startup-config file are used. The copy flash: flash: command can be used to save a copy of the current startup-config file before replacing it. See also "Reset System to Default Settings" on page 86.
--	---

copy flash: flash:

This command is used to make a copy of an existing configuration file on the Wi-Fi AP/Bridge using a different name. After entering this command, you are prompted to enter the name of the existing configuration file and the file name to use for the copy (as shown below):

Vivato#**copy flash: flash:**

Source file: **startup-config**

Destination file: **old-config**

Vivato>

copy flash: scp:

This command is used to copy a configuration file from the Wi-Fi AP/Bridge to a secure remote host. After entering this command, you are prompted to enter the name of the configuration file on the Wi-Fi AP/Bridge, the user name and password for an account on the remote host, the host name (or IP address) of the remote host, and the full directory path and file name for storing the file.

Vivato#**copy flash: scp:**

Source file: **startup-config** (The name of the file on this AP/Bridge that you are copying.)

Username: **tealc** (Enter the account name on the remote host.)

Password: (Enter the password for the account on the remote host.)

Hostname: **172.220.0.35** (Enter the host's IP address, or a host name if a DNS server is present.)

Directory [/]: **/Vivato/Bridge_Routers/**

Destination file [startup-config]: **northbridge_router_config**

copy flash: tftp:

This command is used to copy a file on the AP/Bridge to a remote host that is running a TFTP server program. After entering this command, you are prompted to enter the name of the file to copy, the host name (or IP address) of the remote host, and the name to use when saving the file.

For example, when using the **support** command to send in a copy of your configuration when requesting customer support for your AP/Bridge, you would use the following commands:

Vivato# **copy flash: tftp:**

Source file: **VSupport_Vivato_08062003.tar**

Hostname: **192.165.20.2**

Destination file [VSupport_Vivato_08062003.tar]: <enter>

!! (appears during file transfer)

copy scp: firmware:

This command copies a Wi-Fi AP/Bridge firmware image stored on a secured external host to the AP/Bridge's flash memory. This is done to upgrade the firmware. After the image has been copied, reboot the AP/Bridge to use this image.

Important	DO NOT INTERRUPT THE COPYING PROCESS!
	The AP/Bridge can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the AP/Bridge to operate.

After entering this command, you are prompted to enter the user name and password on the remote host, the hostname (or IP address) where the file is stored, the full directory path and file name of the file to copy, and the file name to use for storing the copy of the configuration file to the AP/Bridge (as shown below):

Vivato#**copy scp: firmware:**

Username: **gerry**

Hostname: **192.165.20.68**

Directory [/]: **vivatoimages**

Source file: **vino.br.1.2.bin**

Password:

copy scp: flash:

This command is used to copy a configuration file from a secure remote host to the Wi-Fi AP/Bridge. After entering this command, you are prompted to enter the user name and password on the remote host, the hostname (or IP address) where the file is stored, the full directory path and file name of the file to copy, and the file name to use for storing the copy of the configuration file to the Wi-Fi AP/Bridge (as shown below):

Vivato#**copy scp: flash:**

Username: **gerry**

Password:

Hostname: **gardenhose**

Directory [/]: **wifibackups**

Source file: **north_bridge_router_config**

Destination file [north_bridge_router_config]: **renew_config**

copy tftp: firmware:

This command copies a AP/Bridge firmware image stored on a remote host running a trivial file transfer protocol (TFTP) server program to flash memory. This is done to upgrade the firmware in the AP/Bridge. After the image has been copied, reboot the AP/Bridge to use this image. See "[Wi-Fi Base Station Firmware Updates](#)" on page 209 for more information on performing firmware updates.

Important	DO NOT INTERRUPT THE COPYING PROCESS!
	The AP/Bridge can contain only one firmware image. Copying a new image into flash memory replaces the current firmware image. Interrupting the copying process can result in a corrupted image that will not allow the AP/Bridge to operate.

After entering this command, you are prompted to enter the hostname (or IP address) where the file is stored and the name of the image file:

Vivato#**copy tftp: firmware:**

Hostname: **192.165.20.68**

Source file: **vino.br.1.2.bin**

copy tftp: flash:

This command is used to copy a configuration file from a remote host to the Wi-Fi AP/Bridge using TFTP. After entering this command, you are prompted to enter the hostname (or IP address) of the other device, the source file name to download, and the destination file name to use when saving it to the Wi-Fi AP/Bridge. A TFTP server must be running on the source device to enable the file transfer. See "[Wi-Fi Base Station Firmware Updates](#)" on page 209 for more information on using a TFTP server.

delete flash: <filename>

Enter the name of a configuration file to remove from the Wi-Fi AP/Bridge's memory. Use the **show flash:** command to see what configuration files have been saved.

dir

List the contents of the Wi-Fi AP/Bridge's flash memory (duplicate function of the **show flash:** command).

rename flash:<filename> flash:<new filename>

Enter the name of an existing file and a new name to rename it. For example; **rename flash:startup-config flash:old-config**

write [memory]

Use this command to save the current configuration as “startup-config (the default configuration file name). If this file already exists, the file is overwritten with the new settings.

write network flash:

This command saves the current configuration to the Wi-Fi AP/Bridge’s flash memory. After entering this command, you are prompted to specify a file name to save the current configuration. The default configuration file is “startup-config”.

write network scp:

This command saves the current configuration to a remote device. After entering this command, you are prompted to specify the user name and password for the device, the host name (or IP address), the full directory path, and the filename to use for storing the configuration (as shown below):

RV-7#**write network scp:**

Username: **gerry**

Password:

Hostname: **gardenhose**

Directory [/]: **bridge_router/backups**

Destination file [startup-config]: **north_bridge_router_config**

write terminal

This command causes the current configuration settings to be displayed on your terminal (just like the **show running-config** command).

Configure Crypto (Generate Keys) Commands

Use the following commands to configure the Wi-Fi AP/Bridge to allow remote access using a secure connection.

crypto key generate <dsa|rsa|rsa1>

Select the type of encryption key to re-generate. These keys are used when accessing the Wi-Fi AP/Bridge through a secure shell. These keys are automatically generated whenever the Wi-Fi AP/Bridge is rebooted, but you can regenerate these keys using this command.

See **"ip ssh genkey"** on page 135 to enable secure shell operation on the Wi-Fi AP/Bridge. This command also provides regeneration of the encryption keys.

Configure Enable Secret Commands

The enable password must be entered before the configuration of the Wi-Fi AP/Bridge can be changed.

This is the only password requested when using a terminal program and an RS-232 connection to the Wi-Fi AP/Bridge.

When using a secure shell to access the Wi-Fi AP/Bridge, you must first enter the user name (default is "admin") and the read password (default is "vivato") to access the read level. To begin configuring the Wi-Fi AP/Bridge, you must then enter the "enable" command and the enable password.

See **username admin secret [<password type (0|5)> <password text>]** for information on setting the read level password.

enable secret [<password type (0|5)>] <password text>

This command sets the enable level password. When the "<password type (0|5)>" option is not used, it is assumed that the password you enter is unencrypted (clear text). The password type options allow you to specify that the password being entered is unencrypted, by specifying "0" for the password type, or is encrypted, by specifying "5" for the password type.

Configure HTTP-Server Commands

When enabled, the HTTP daemon provides access to the Wi-Fi AP/Bridge's configuration web pages.

http-server

Enable the httpd daemon. By default, the http daemon is enabled to allow access to the web user interface configuration pages.

no http-server

Disable the http daemon.

Configure Interface Commands

The following commands are used to configure the ethernet and wireless interfaces in the AP/Bridge.

DHCP Server Operation

Dynamic host configuration protocol (DHCP) is used to automatically assign IP addresses to clients associating through the Wi-Fi AP/Bridge. The bridge, Ethernet, and Wireless interfaces all support DHCP operation using the same command set. Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface.

For more information on configuring DHCP, see "[Dynamic Assignment of Client IP Addresses](#)" on page 153.

interface bridge <0-4094>

Enter the number of the bridge to create. Issuing this command changes the prompt to indicate which bridge you are configuring, such as **vivato (config -br1)#** if you entered **1** for the value. This prompt must be displayed when issuing any of the following bridge configuration commands.

Note: A default bridge (br0) exists between the Ethernet 0 interface (eth0) and the wireless interfaces (wlan1-wlan13) for wireless clients to communicate with the wired network.

An Ethernet or a wireless interface can only be assigned to one bridge. Therefore, you must first remove any Ethernet or wireless interfaces from the default bridge (br0) before they can be assigned to a new bridge. An interface can only be added to a bridge if that interface does not have an IP address assigned to it.

add interface ethernet <0>

Add the Ethernet interface to this bridge.

no add interface ethernet <0>

Remove the Ethernet interface from this bridge.

add interface wireless < 0-1>

Enter the number of the wireless interface to add to the bridge.

no add interface wireless < 0-1>

Remove the specified wireless interface from this bridge.

add interface wireless < 0-1> wds <1-6>

Enter the number of the wireless interface and the port number of a wireless distribution system (WDS) connection on that interface to add that WDS connection to the bridge. This adds the WDS connection residing on that wireless interface to the bridge, but does not add the wireless interface itself to the bridge. See "[Configure WDS \(Wireless Distribution System\)](#)" on page 139.

aging-time <10-1000000 seconds>

Enter the number of seconds that network addresses of devices using the bridge are stored in the bridge table after receiving a packet. The default value is 300 seconds.

dhcp-server

Enable dynamic host configuration protocol (DHCP) for automatic assignment of IP addresses to clients associating through this interface. This default state is disabled.

dhcp-server broadcast-address <ip address>

Enter the DHCP broadcast IP address. This is the address that is returned if a DHCP client requests the broadcast address from the DHCP server.

no dhcp-server broadcast-address <ip address>

Remove the specified DHCP broadcast address.

dhcp-server domain-name <domain name>

Enter a domain name to represent the range of IP addresses served by this DHCP server.

no dhcp-server domain-name <domain name>

Remove the specified name of the domain containing the DHCP server.

dhcp-server gateway <ip address>

Enter the IP address of the interface used as the gateway for DHCP clients to connect to your wired network. This is typically the Ethernet port connected to your wired network.

no dhcp-server gateway <ip address>

Remove the default gateway at the specified IP address.

dhcp-server ip-pool <start ip address> <end ip address> <netmask>

Enter the starting and ending IP address range and net mask for assigning IP addresses on this interface using DHCP.

no dhcp-server ip-pool <start ip address> <end ip address> <netmask>

Remove the specified starting and ending IP address range and net mask from being assigned to clients associating through this interface using DHCP.

dhcp-server lease <1-4294967295>

Enter the number of seconds that an assigned IP address can be leased by a client before it must be renewed. The default is 10 days (864,000 seconds).

no dhcp-server lease <1-4294967295>

Delete the previously set DHCP lease time.

dhcp-server name-server <ip address>

Enter the IP address of a name server. Up to three name servers can be specified by issuing this command for each entry.

no dhcp-server name-server <ip address>

Enter the IP address of a name server to remove from the list of name servers.

dhcp-server ntp-server <ip address>

Enter the IP address of a network time protocol (NTP) server. Up to three time servers can be specified by issuing this command for each entry.

no dhcp-server ntp-server <ip address>

Enter the IP address of a network time server to remove from the list of time servers.

dhcp-server wins <ip address>

Enter the IP address of a Windows internet naming service (WINS) server.

no dhcp-server wins <ip address>

Enter the IP address of a Windows internet naming service (WINS) server to remove it from DHCP configuration.

exit

Issue this command to stop configuring the specified bridge interface and return the command line prompt to the previous level.

forward-time <4-200 seconds>

The forward time specifies how much time a bridge spends in the listening and learning states before forwarding a packet. This is used to prevent a bridge from starting to forward data packets over a link until the bridged network has been informed of the topology change and the affected links have been turned on or off.

If you set this value too low, loops can exist until the spanning tree algorithm protocol reconfigures the topology. Setting the value too high can cause delays until the spanning tree protocol reconfigures the topology. The default setting is 15 seconds.

no forward-time

Reset the forward time to the default setting of 15 seconds.

hello-time <1-10 seconds>

The hello time is the period between the configuration messages generated by a root bridge. If you believe that configuration messages may be getting lost, shorten the hello time. To reduce the amount of overhead messages, increase the hello time. The default setting is 2 seconds.

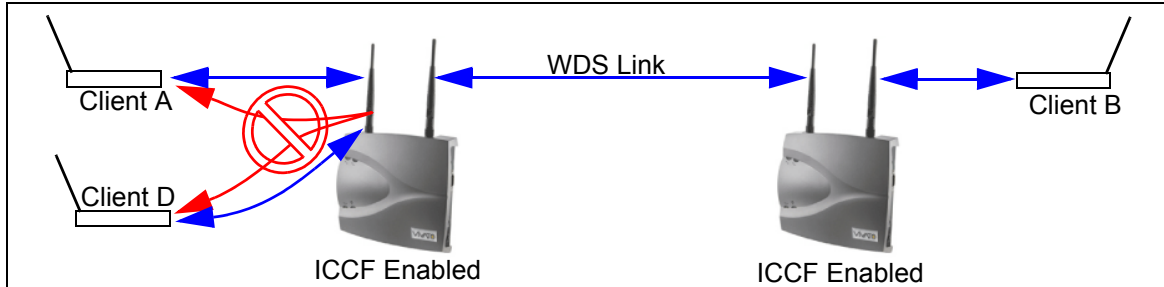
no hello-time

Reset the hello time to the default setting of 2 seconds.

iccf

When enabled, inter-client communication filtering (ICCF) prevents client to client communication through any of the wireless interfaces that are in the bridge.

Note: ICCF does *not* prevent wireless clients from communicating with each other through a WDS link between AP/Bridges. In the example below, client “A” cannot communicate with client “D” when ICCF is enabled. However, client “A” and client “D” can communicate through the WDS link to client “B”.



ICCF can also be enabled separately for the wireless interfaces only; independent of the bridge. See "[iccf](#)" on page 130.

no iccf

Disable inter-client communication filtering (ICCF).

ip address <ipaddress> <netmask> [secondary]

Enter an IP address and a subnet mask for the bridge. In the default configuration, an IP address is assigned to the default bridge (br0), which is the IP address that is used to access the Wi-Fi AP/Bridge. The optional “secondary” entry is used to create a secondary IP address for this bridge.

Alternatively, the IP address and netmask bits can be entered using the format in this example: 10.0.3.34/24.

no ip address <ipaddress> <netmask> [secondary]

Enter a previously entered IP address and subnet mask to remove them from the bridge. The optional “secondary” entry is used to delete a previously assigned secondary IP address. If a secondary IP address was assigned on this bridge, it must be removed before the primary IP address can be removed.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface* to assign it an IP address (client DHCP). If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server. The default state is disabled.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface and allow it to be reassigned.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip broadcast-address <ipaddress> [secondary]

Enter an IP address to use when sending broadcast messages over the bridge interface, and use the optional “secondary” entry to make this a secondary broadcast IP address for this interface.

ip routing

Enter this command to enable IP routing on this interface.

no ip routing

Disable IP routing on this interface.

max-age <6-200 seconds>

The maximum age is used to determine when the bridge’s stored configuration information is out of date and is removed. Setting the value too small causes the spanning tree protocol to reconfigure the bridge topology too often, which can cause a momentary loss of connectivity to the network.

Setting the value too large can slow down the network because it is taking longer than necessary to adjust to a new spanning tree configuration for the bridge. A conservative value assumes a delay variance of 2 seconds per hop. The default value is 20 seconds.

no max-age

Resets the max age to the default value of 20 seconds.

path-cost interface <ethernet 0|wireless 0-1> <0-65535>

Enter the path cost for a specific interface on this bridge. The spanning tree algorithm adds this value to the root cost in configuration messages that are received on this port, and is used to determine the path cost to the root through this interface.

Larger path cost values can result the LAN accessed through this interface to be lower in the spanning tree topology. This can result in less through traffic through this port. You should assign a large path cost to a LAN that has a lower bandwidth or where you want to minimize LAN traffic.

path-cost interface <wireless 0-1> wds <1-6> <0-65535>

Specify the wireless interface and its wireless distribution system (WDS) connection, and enter the path cost for the WDS connection on this bridge. Although the wireless interface for the WDS connection is used in this command, the path cost of the wireless interface itself is not affected; only the path cost of the WDS connection is affected. The spanning tree algorithm adds this value to the root cost in configuration messages that are received on this port, and is used to determine the path cost to the root through this connection.

Larger path cost values can result the LAN accessed through this interface to be lower in the spanning tree topology. This can result in less through traffic through this port. You should assign a large path cost to a LAN that has a lower bandwidth or where you want to minimize LAN traffic.

priority <0-65535>

The bridge priority is used to determine which bridge to use for the root bridge and which to use for the designated bridge. In general, a lower the bridge priority number results in the bridge being selected as the root bridge or a designated bridge.

shutdown

Disable the bridge interface.

no shutdown

Re-enable the bridge interface.

stp

Enable spanning tree protocol (STP) on this bridge.

no stp

Disable spanning tree protocol on this bridge.

show <text>

See "**show interfaces bridge [0-4094]**" on page 105.

shutdown

Disable the bridge.

source-nat interface <bridge <0-4094>|ethernet <0>|wireless < 0-1>|wireless <0-1> wds <1-6>>

Enter the type and number of an interface to use its IP address as the source IP address for network address translation (NAT). The IP address of this bridge, and the IP address of the desired source interface, must be configured before address translation can occur.

interface ethernet 0

Configure the ethernet interface. Issuing this command changes the prompt to **vivato (config-eth0)#**. This prompt must be displayed when issuing any of the following ethernet interface commands:

DHCP Server Operation

Refer to the bridge interface's DHCP command descriptions for DHCP operation on any interface. See "**dhcp-server**" on page 120.

exit

Issue this command to stop configuring the specified ethernet interface and return the command line prompt to the previous level.

ip address <ipaddress> <netmask>

Specify the IP address and the subnet mask used to access this ethernet interface. Alternatively, the IP address and netmask bits can be entered using the format in this example: 10.0.3.34/24.

Note: The IP address of the default bridge that bridges the Ethernet and wireless interfaces (bro) is initially used provide access to the Wi-Fi AP/Bridge. See "**interface bridge <0-4094>**" on page 120.

no ip address <ipaddress> <netmask> [secondary]

Enter a previously entered IP address and subnet mask to remove them from this interface. The optional "secondary" entry is used to delete a previously assigned secondary IP address. If a secondary IP address was assigned on this interface, it must be removed before the primary IP address can be removed.

ip broadcast-address <ipaddress> [secondary]

Enter the IP address to use for broadcast messages, and use the optional "secondary" entry to make this a secondary broadcast IP address for this interface.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface* to assign it an IP address (client DHCP). If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server. The default state is disabled.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface.

ip routing

Enter this command to enable IP routing on this interface. If you are at the Vivato(config)# prompt, IP routing is enabled globally.

no ip routing

Disable IP routing on this interface (or globally at the Vivato(config)# prompt).

show <text>

See "[show interfaces ethernet \[0\]](#)" on page 106.

shutdown

Disables the ethernet interface indicated in the command prompt.

no shutdown

Re-enables the interface after using the [shutdown](#) command to disable it.

source-nat interface <bridge <0-4094>|ethernet <0>|wireless <0-1>>

Enter the type and number of an interface to use its IP address as the source IP for network address translation (NAT). The IP address of this Ethernet interface, and the IP address of the desired source interface, must be configured before address translation can occur. The default state is disabled.

interface wireless <0-1|all>

This command selects the wireless interface for configuration. The Wi-Fi AP/Bridge contains 2 fully configurable wireless interfaces. Each interface can be configured individually, or all interfaces can be configured as a group.

Issuing this command changes the prompt to **vivato (config -wlanN)#**, where N is the specified interface number, or **vivato (config -wlan-all)#** when all interfaces are being configured together. One of these prompts must be displayed when issuing any of the following wireless interface commands.

By default, wireless interfaces are bridged to the Ethernet 0 (eth0) interface for wireless clients to be able to access the wired network. See "[interface bridge <0-4094>](#)" on page 120.

beacon-interval <0-8191>

Specify the amount of time, in milliseconds, between beacons. The default is 100, and should not be changed in most circumstances. This command can be used with an individual wireless interface, and can also be used to change all wireless interfaces at once when “**interface wireless all**” is specified. Entering either 0 or 8191 results in the maximum period between beacons.

Decreasing the interval generally has an adverse effect on performance, since beacons become a larger percentage of the traffic. Also, the “power-save” function on clients is alerted to a beacon more often, reducing power save benefits.

Increasing the interval may cause an excessive amount of data to be buffered before the beacon is sent, resulting in lost data. Also, some protocols may time out if packets are not delivered before the increased interval period has elapsed.

channel <1-11>

Enter a channel number for the wireless interface. The value must be in the range of 1 to 11. Whenever possible, you should use the default channels: 1 and 11.

DHCP Server Operation

Refer to the bridge interface’s DHCP command descriptions for DHCP operation on any interface. See “**dhcp-server**” on page 120.

disable beacon-ssid

This command prevents the ESSID from being sent in beacons issued by this wireless interface. Since the ESSID is no longer sent, clients cannot display it in their list of available networks. Therefore, only clients that have had the ESSID manually entered into their preferred wireless network list can associate with the Wi-Fi AP/Bridge. The default state is to send the ESSID in beacons until this command is issued.

no disable beacon-ssid

Issuing this command allows the ESSID to be transmitted in beacon messages from this interface, allowing all clients to see the ESSID in their list of available networks.

EAP Commands (802.1x security)

The following commands are available for setting up 802.1x security, including extensible authentication protocol (EAP), transport layer security (TLS), and protected EAP (PEAP). See “**Configuring 802.1x in Your Client**” on page 76 for setting up clients to use EAP/PEAP.

On the AP/Bridge, 802.1x security is enabled and disabled on a per wireless interface basis.

See “**no eap**” on page 130 to disable EAP security.

Windows 2000 Internet Access Server Setup

Use the following guidelines when configuring EAP/TLS/PEAP on your Windows 2000 IAS to work with the Vivato Wi-Fi AP/Bridge. For more information on configuring Microsoft® Windows® XP clients and a Windows 2000® Internet Access Server (Win2K IAS) for EAP or PEAP security, see Windows XP Win2kIAS Deployment.pdf© on the Vivato 2.4 GHz Wi-Fi AP/Bridge CD.

To work with Win2K IAS, users should be grouped based on the VLAN ID in the Active Directory. A policy for each user group must be added by, 1) setting the “Windows Group” as the “condition to match” and selecting the user group.

(1) Encryption Key Length - Set by Profile>Encryption: Use either (a) Basic : 64 bit key, or (b) Strongest: 128 bit key. Regardless of the type of RADIUS server used, encryption must conform to RFC 2548 MS-MPPE-Encryption-Types.

(2) Session Timeout - Set by Profile>Dial-in Constraint>Restrict Maximum Session To: Value: session timeout period (minutes). When a client reaches session timeout, the Wi-Fi AP/Bridge forces the client to re-authenticate and deliver new session key. Regardless of the type of RADIUS server used, operation must conform to RFC 2865 Attribute Type 27.

(3) Key Refresh Timeout - Set by Profile>Advanced>Vendor Specific Attribute: Vendor code: 14615 Confirm to RADIUS RFC: Yes. Vendor Type: 60. Attribute format: Decimal. Attribute value: key refresh period (minute). When a client reaches key refresh timeout, the Wi-Fi AP/Bridge delivers a new session key to the client.

The administrator may configure: (a) Key refresh and session timeout. (b) Key refresh only. (c) Session timeout only. If Key Refresh Timeout >= Session Timeout, the Key Refresh Timeout is ignored.

If item 1 is changed on the Windows 2000 IAS, then the Wi-Fi AP/Bridge needs to be rebooted in order to force all clients to re-authenticate using the new policy. Items 2 and 3 can be changed and applied to the next authenticated client without system reboot.

Wi-Fi AP/Bridge EAP Configuration Example

The following example shows how EAP may be configured on the Wi-Fi AP/Bridge to work with Windows 2000 IAS:

Note: When making changes to an existing EAP configuration, you should disable EAP before making the changes, and then re-enable EAP after making the changes to re-initialize EAP using the new configuration.

```
vivato (config)# no eap
vivato (config)# eap server 1 191.173.0.149 1812
vivato (config)# eap secret 1 eapsecretforpeap
vivato (config)# eap server 2 191.173.0.150 1812
vivato (config)# eap secret 2 secondaryeapsecret
vivato (config)# eap
```

eap

Enable the EAP security daemon. This command must be issued before EAP can be used, and re-issued after making any changes to the EAP configuration. The default EAP state is disabled.

eap secret <1-2> <secret string>

Enter the authentication server's priority number and its associated password. The secret appears as clear text as it is entered.

eap rekey-interval <60-1800>

Enter the interval (in seconds) between encryption key refreshes. The key is changed at each refresh, making it much more difficult for undesired clients to decipher the encryption key.

eap server <1-2> <ipaddress> <portnum>

This command specifies the RADIUS server(s) to use to authenticate clients. Enter the RADIUS Server priority number (1 or 2) , its IP address, and the port number. The priority number determines which server is used as the primary and secondary server. If the primary server (1) is not found, the Wi-Fi AP/Bridge attempts to use the secondary server (2). The password for each server must also be set using the **eap secret <1-2> <secret string>** command.

no eap

Disable EAP (802.1x) security.

no eap server <RADIUS Server ID (1-2)> <ipaddress> <portnum>

Enter the device number of the RADIUS server that is providing EAP security in order to stop authenticating through this server.

essid <text>

Enter an identifying name for the extended service set for this wireless interface. The name must be in the range of 1 to 32 characters long.

exit

Enter this command when you are done configuring this wireless interface.

iccf

When enabled, inter-client communication filtering (ICCF) prevents clients associating with the AP/Bridge from accessing each other through the selected wireless interface(s).

This command can be issued at the "wireless all" level (**Vivato(conf-wlan-all)# iccf**) to prevent inter-client communication between wireless interfaces. It can also be issued at the individual wireless interface level (such as **Vivato(conf-wlan0)# iccf**). If ICCF is already

enabled on an individual wireless interface, issuing the command at the “wireless all” level automatically enables ICCF on the other wireless interface as well.

ICCF cannot be enabled for an individual wireless interface if it is part of a bridge (such as br0). Wireless interfaces in a bridge take on the ICCF setting of the bridge. To prevent inter-client communication across all devices on a bridge, use the ICCF command at the bridge configuration level. See "**iccf**" on page 122.

The default state is disabled.

no iccf

Disable inter-client communication filtering (ICCF).

ip address <ipaddress> <netmask>

Assign an IP address and subnet mask to an individual wireless interface. This command is not used when all wireless interfaces are being configured at once by issuing the **interface wireless all** command.

ip address <ipaddress> <netmask> secondary

Enter an IP address and a subnet mask to create a secondary IP address for this interface. Alternatively, the IP address and netmask bits can be entered using the format in this example: 10.0.3.34/24.

no ip address <ipaddress> <netmask> [secondary]

Enter a previously entered IP address and subnet mask to remove them from this interface. The optional “secondary” entry is used to delete a previously assigned secondary IP address. If a secondary IP address was assigned on this interface, it must be removed before the primary IP address can be removed.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface* to assign it an IP address. If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface.

ip broadcast <ipaddress> [secondary]

Enter an IP address to use when sending broadcast messages over this interface, and use the optional “secondary” entry to make this a secondary broadcast IP address for this interface.

no ip broadcast-address [secondary]

Remove the broadcast IP address or, optionally, the secondary broadcast IP address, for this interface.

ip routing

Enter this command to enable IP routing on this interface. If you are at the Vivato(config)# prompt, IP routing is enabled globally.

no ip routing

Disable IP routing on this interface (or globally at the Vivato(config)# prompt).

key <value> <1-4>

This command specifies the wired equivalent privacy (WEP) encryption key value for the specified key assignment. The key value consists of 10 or 26 hex digits (0-9, a-f), or 5 or 13 alphanumeric ascii values (0-9, a-z), depending on the key length (40-bit or 128-bit). When using ascii values, enter **S:** at the start of the value to identify it as an ascii value. The key assignment value must be in the range of 1 to 4.

For example, 104-bit (13 digit ascii) WEP key assigned to key index 1 could be set up for all wireless interfaces by issuing the following command at the **vivato (config -wlans)#** prompt: **key s:gmV8a18436572 1**

sensitivity <1-3>

Change the receiver sensitivity for this wireless interface: 1 = most sensitive (default), 3 = least sensitive. Under most conditions this value should be left at “1” to receive signals from far away clients.

This command can be used with an individual wireless interface, and can also be used to change all wireless interfaces at once when “**interface wireless all**” is specified.

show <text>

See "**show interfaces wireless <0-1>**" on page 109.

shutdown

Issuing this command disables the wireless interface.

no shutdown

Issuing this command re-enables the wireless interface if it has been shut down.

source-nat interface <bridge <0-4094>|ethernet <0>|wireless < 0-1>>

Enter the type and number of an interface to use its IP address as the source IP for network address translation (NAT). The IP address of this wireless interface, and the IP address of the desired source interface, must be configured before address translation can occur.

wds <port (1-6)>

Enter a port number (1-6) to enable wireless distribution system (WDS) operation on this wireless interface and port. Each wireless interface can support up to six WDS connections.

When this command is issued, the Wi-Fi AP/Bridge automatically creates a unique MAC address for spanning tree protocol operation on this wireless interface and port. The command prompt is also changed to indicate that you are now configuring a WDS connection that represents a logical interface used only for WDS operation (see below). This new interface has its own set of configuration commands. See "[Configure WDS \(Wireless Distribution System\)](#)" on page 139.

```
Vivato(config-wlan1)#wds 1  
Vivato(config-wlan1wds1)#
```

Although the WDS interface shares the same physical layer properties as the wireless interface it resides on (such as channel number, receiver sensitivity, and transmit power), it is regarded as a totally separate logical interface. Therefore, to use a WDS connection in a bridge it must be added to the bridge just like any other interface.

The default state has no WDS connections enabled. Use the **no shutdown** command to enable the WDS connection after it is created.

wep <1-4>

This command selects the wired equivalent privacy (WEP) encryption key to use and enables WEP for the wireless interface. The value must be in the range of 1 to 4. Issuing this command restricts access through the wireless interface to clients using the correct WEP key and key assignment values. The default state is disabled.

Because EAP security automatically configures WEP as part of its operation, WEP cannot be configured on a wireless interface if EAP security is currently being used.

no wep

This command disables using wired equivalent privacy (WEP) encryption for the wireless interface.

Configure No Interface Commands

The following commands disable interfaces in the AP/Bridge.

no interface bridge <0-4094>

Specify the number of the bridge interface to disable.

Configure IP Commands

Use these commands to specify internet protocol (IP) addressing.

ip domainname <text>

Enter a name to refer to the domain that includes the IP addresses that you assigned to the interfaces within the AP/Bridge. No default domain name is configured.

ip host <hostname> <ipaddress>

Enter a host name and IP address to enter into the host table. Use the **"show ip host"** on page 111 to view the contents of the host IP table.

ip hostname <hostname>

Enter a host name for the AP/Bridge to use with a domain name service (DNS) server; the default host name is "Vivato. The host name is also displayed at the command line prompt.

```
Vivato(config)#ip hostname Mirabeau
Mirabeau(config)#
```

ip name-server <ipaddress>

Enter the IP address of the domain name service (DNS) server to use when looking for the IP address of a specified domain.

ip route <destination prefix> <destination mask> <forwarding router address>

Enter the IP address prefix and net mask of the destination network, and the IP address of the router used to access that network.

For example, entering **ip route 135.220.6.0 255.255.255.0 134.228.4.203** tells the AP/Bridge to route all IP datagrams destined for the 135.228.6.0/24 network through a gateway whose IP address is 135.228.4.203.

To create a default gateway, enter 0.0.0.0 for the destination prefix and mask, and the IP address of the gateway. For example, if the default gateway is at 192.163.20.240, enter **ip route 0.0.0.0 0.0.0.0 192.163.20.240**.

ip routing

Enter this command to enable IP routing globally (on all interfaces). The default state is disabled.

ip ssh genkey

Generate encryption keys for a secure shell connection to the AP/Bridge. This command re-generates the same cryptographic keys created by the **crypto key generate <dsa|rsa|rsa1>** command.

ip ssh server

Start the SSH daemon to enable secure shell access.

ip ssh bind interface (wireless <0-1>|ethernet 0|bridge <0-4094>)

Specify the interface on the AP/Bridge to use for SSH access. When this command is issued, only the IP address on that interface can be used to access the AP/Bridge through SSH. If an IP address has not been assigned to this interface, SSH access is not restricted.

no ip ssh bind [interface (wireless <0-1>|ethernet 0|bridge <0-4094>)]

Do not restrict SSH access to any interface or, optionally, to a previously bound interface.

Configure Log Commands

The following commands are used to specify where to send system message log information.

logging local

Enable logging and log system messages to the Wi-Fi AP/Bridge's memory. Use the **"show logging"** on page 111 to view the log. The default state is disabled.

logging remote <ipaddress|hostname>

To enable logging and display system information on a remote host, enter the IP address or host name of the remote host. The remote host must first be configured to accept remote logging (syslogd -r at a minimum). The default state is disabled.

no logging local

Disable local logging.

no logging remote

Disable remote logging.

Configure Multicast/Broadcast Rate Limiting

Rate limiting limits the amount of multicast or broadcast traffic through the AP/Bridge's Ethernet port to 75 packets per second. When levels of this type of traffic are excessive, other types of packets may not be forwarded to clients. Enabling rate limiting blocks some of this traffic to allow unicast traffic to get through to clients.

rate-limit <broadcast|multicast>

Enables rate limiting for the selected type of traffic: broadcast or multicast.

Configure SNMP-Server Commands

The following commands are used to configure simple network management protocol (SNMP) operation.

snmp-server

Enables the SNMP daemon. The default state is disabled.

snmp-server bind interface (wireless <0-1>|ethernet 0|bridge <0-4094>)

Specify the interface on the Wi-Fi AP/Bridge to use for SNMP access. When this command is issued, only the IP address on that interface can be used to access the AP/Bridge by and SNMP client. If an IP address has not been assigned to this interface, SNMP access is not restricted.

snmp-server community <community name> RO|RW [<source ip address>]

Enter the name of an SNMP community to create and whether it allows read only (RO) or read-write (RW) operation. If the [<source ipaddress>] option is used, only SNMP requests from the source IP address are honored.

snmp-server contact <text>

Enter text for system contact information, such as a person's name.

snmp-server engineID <engine identifier>

Enter an SNMP engine identifier (ID). An engine ID can only be created if there are no SNMPv3 users. Use the 'no snmp-server user' command to remove all users if you have any defined. Only hex characters (0-9 and a-f) can be used to define an SNMPv3 engineID.

snmp-server host <hostname|ipaddress> traps version 1 <community name>

Use this command to create a trap sink for SNMP version 1. Enter the host name or IP address and the community name. See [Table 5—Examples for Creating Traps/Informs Sinks on page 137](#).

snmp-server host <hostname|ipaddress> traps|informs version 2c <community name>

Use this command to create a trap sink or an inform sink for SNMP version 2c. Enter the host name or IP address, whether to create a trap or an inform, and the community name. See [Table 5—Examples for Creating Traps/Informs Sinks on page 137](#).

snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> [auth MD5|SHA <password> [priv DES <password>]]

Use this command to create a trap sink or an inform sink for SNMP version 3. Specify the host name or IP address, whether to create a trap or an inform, and enter the user name. Optionally, you can specify the authentication type, password, and the DES56 encryption password. The authentication password is used if the optional DES password is not entered. See [Table 5—Examples for Creating Traps/Informs Sinks on page 137](#).

Table 5—Examples for Creating Traps/Informs Sinks

Setting	Command
Creates an SNMPv1 trap sink.	snmp-server host 10.0.0.1 traps version 1 private
Creates an SNMPv2c trap sink.	snmp-server host 10.0.0.1 traps version 2c private
Creates an SNMPv2c inform sink.	snmp-server host 10.0.0.1 informs version 2c private
Creates an SNMPv3 trap sink with user “lrs”.	snmp-server host 10.0.0.1 traps version 3 user lrs
Creates an SNMPv3 inform sink with user “lrs”.	snmp-server host 10.0.0.1 informs version 3 user lrs
Creates an SNMPv3 inform with user “lrs” using authentication and encryption.	snmp-server host 10.0.0.1 informs version 3 user lrs auth MD5 12345678 priv DES 23456789

snmp-server location <text>

Enter the SNMP system location, such as “inside the krell lab”.

snmp-server name <text>

Enter the SNMP system name, such as “WISP 1”.

snmp-server user <username> [auth MD5|SHA <password> [priv DES [<password>]]]

To create an SNMPv3 user, enter the user name, authentication method and password, and DES56 encryption password to enable authentication and encryption for SNMP. The privacy password is optional. If it is not entered, the authentication password is also used for the privacy password.

The following examples illustrate how this command is used:

Table 6—Examples for Configuring an SNMPv3 User

Setting	Command
Create a user named “lrs” with no authentication and no privacy.	snmp-server user lrs
Create a user named “lrs” that only uses authentication.	snmp-server user lrs auth MD5 12345678

Table 6—Examples for Configuring an SNMPv3 User

Setting	Command
Create a user named “lrs” with authentication and encryption using the authentication password.	snmp-server user lrs auth MD5 12345678 priv DES
Create a user named “lrs” with authentication and with encryption that uses it's own password	snmp-server user lrs auth MD5 12345678 priv DES 23456789

Configure No SNMP-Server Commands

The following commands disable various aspects of simple network management protocol (SNMP) operation. See also [Configure SNMP-Server Commands](#).

no snmp-server

Disables the SNMP daemon.

no snmp-server community <community name>

Enter the name of the SNMP community to be deleted. See also [snmp-server community <community name> RO|RW \[<source ip address>\]](#).

no snmp-server contact

Deletes the SNMP contact information.

no snmp-server engineID

Removes the SNMP engine identifier. An engine ID can only be removed if there are no SNMPv3 users. Use the 'no snmp-server user' command to remove all users if you have any defined.

no snmp-server host <hostname|ipaddress> traps|informs version <1|2c|3>

Enter this command to disable the corresponding trap or inform. See [snmp-server host <hostname|ipaddress> traps|informs version 3 user <username> \[auth MD5|SHA <password> \[priv DES <password>\]\]](#).

no snmp-server location

Deletes the SNMP location information.

no snmp-server name

Deletes the SNMP name information

no snmp-server user <username> [auth MD5|SHA <password> [priv DES <password>]]

Enter this command to remove the specified SNMPv3 user (see **snmp-server user <username> [auth MD5|SHA <password> [priv DES <password>]]**).

Configure Username Admin (Read Level) Secret

The read level secret is used to access the Wi-Fi AP/Bridge through a secure shell or the configuration webpages; it is not used when a terminal program and an RS-232 connection are used. By default, the user name is “admin” and the password is “vivato”.

username admin secret [<password type (0|5)> <password text>

This command sets the read level password. When the “<password type (0|5)>” option is not used, it is assumed that the password you enter is unencrypted (clear text). The password type options allow you to specify that the password being entered is unencrypted, by specifying “0” for the password type, or is encrypted, by specifying “5” for the password type.

Use the **enable secret [<password type (0|5)>] <password text>** command to change the enable level secret.

Configure WDS (Wireless Distribution System)

A wireless distribution system uses a Vivato AP/Bridge and Vivato Wi-Fi Base Station to provide a wireless data link that can span large distances to provide a network connection to a remote Wi-Fi Base Station or to connect two network segments together. The remote Base Station can use the WDS link to a local AP/Bridge as a substitute for its own wired backhaul connection, requiring only mains power to provide 802.11b service to clients.

The link is created by first enabling WDS operation on a wireless interface on the Wi-Fi Base Station and on the AP/Bridge, and then specifying the MAC address of the WDS-enabled wireless interface on the opposing device as the “peer address”.

A WDS connection is created at the wireless interface configuration level using the **wds <port (1-6)>** command. The command prompt then changes to indicate that you are configuring that WDS connection (as shown below).

The WDS connection acts as a separate logical interface, even though it is configured on a wireless interface. Functioning as an interface, an IP address can be assigned to the WDS interface using a static address or by DHCP client operation.

Important



The WDS connection must be added to the default bridge before it can pass traffic to other interfaces on the AP/Bridge. Use the **add interface wireless <0-1> wds <1-6>** command to add the WDS connection to the bridge.

Important 	To help secure the WDS traffic, enable WEP on the wireless interfaces at both ends of the WDS link.
--	---

Use the **show wds** command to view a WDS configuration on a wireless interface.

The following WDS commands are available to configure the specific WDS connection indicated at the command prompt. See "**WDS Configuration Example**" on page 142 to see how some of these commands are used.

exit

Exit the WDS configuration and return to the configuration prompt level. To return to the WDS command prompt after exiting, you need to first prefix to the specific wireless interface (using the **interface wireless <0-1|all>** command), and then enter the **wds <port (1-6)>** command for the specific WDS connection.

ip address <ip address> <subnet mask> [secondary]

Specify an IP address and subnet mask for this WDS connection. The IP address and netmask bits can also be entered using the format in this example: 10.0.3.34/24. The optional "secondary" entry is used to create a secondary IP address for this WDS connection.

When a WDS connection is removed, any primary and secondary IP addresses assigned to that connection are also removed.

no ip address <ip address> <subnet mask> [secondary]

Enter the previously assigned IP address to remove it from this WDS interface. Use the "secondary" option to remove a secondary IP address.

ip address dhcp

Enter this command to enable dynamic host configuration protocol (DHCP) *for this interface to assign it an IP address*. If a DHCP server is accessible through this interface, the IP address of this interface is automatically assigned by that server.

no ip address dhcp

Enter this command to disable dynamic host configuration protocol (DHCP) *for this interface*. Use this command if you are going to assign a static IP address to this interface.

ip address dhcp renew

Enter this command to send a request to the DHCP server to renew the IP address for this interface.

ip address dhcp release

Enter this command to send a request to the DHCP server to release the IP address used by this interface and allow it to be reassigned.

ip broadcast-address <ip address> [secondary]

Enter the broadcast IP address for this WDS connection. The optional “secondary” entry is used to create a secondary broadcast IP address for this WDS connection.

no ip broadcast-address <ip address> [secondary]

Enter the previously assigned broadcast IP address to remove it from this WDS interface. Use the “secondary” option to remove a secondary broadcast IP address.

peer-address <mac address>

Enter the MAC address of the wireless interface on the Wi-Fi Base Station that is being used for a WDS link to the AP/Bridge (in the format 00:0B:33:31:85:A3).

A peer MAC address can only be used with one WDS connection on any wireless interface.

shutdown

Enter this command to disable this WDS connection.

no shutdown

Enable this WDS connection.

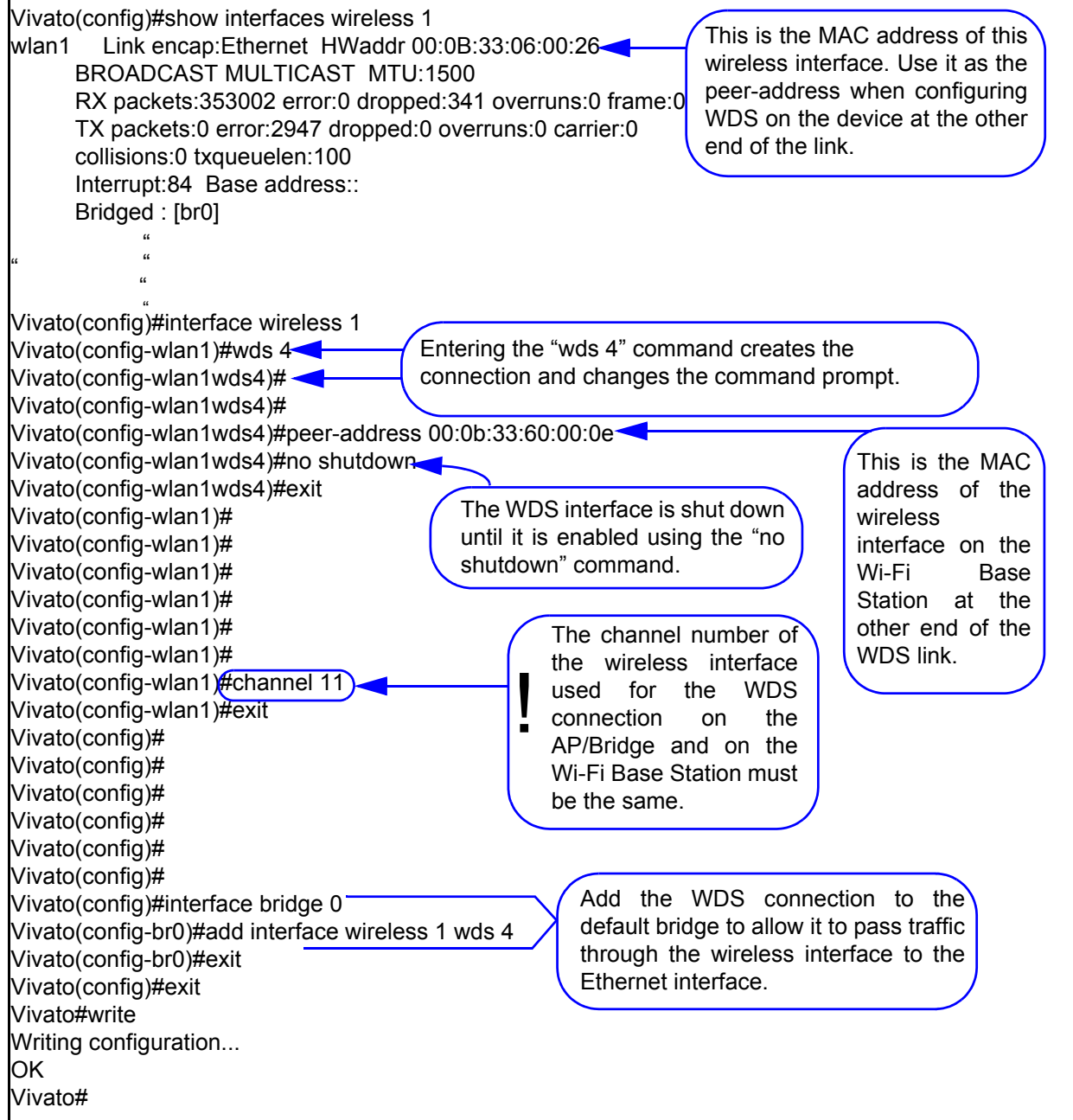


Figure 34—WDS Configuration Example

disable

Enter this command to leave the enable level and return to the read level.

edit flash:

After entering this command, you are prompted to enter the name of a configuration file in the Wi-Fi AP/Bridge to edit. The CLI then launches a vi editor to allow the configuration file to be modified and saved. CLI operation returns after exiting the vi editor.

To exit the editor without saving your changes, type `:q!`. To save your changes and exit, type `ZZ` or `:wq`.

exit

After using the **configure [terminal]** command to configure the Wi-Fi AP/Bridge, the CLI stays in the configuration mode until you enter the **exit** command. If you exit the configuration mode and enter the **exit** command again, the current CLI session is closed.

no <configuration command>

Override parameters you have entered. This operation is used extensively in the enable level commands to disable previously enabled operations or settings (as shown in this command list).

reboot

Issuing this command causes the Wi-Fi AP/Bridge to be reset, and powers on using the last saved configuration. See **write network flash:** or "**write [memory]**" on page 118 for commands to save the current configuration.

Caution



Any changes made to the configuration that have not been saved are lost when this command is issued.

support

This command causes an archive of the current configuration and system messages to be created and saved in a file called "VSupport_Vivato_<date>.tar". This file can then be copied to a local host computer using the **copy flash: tftp:** command, and sent to Vivato Customer Support for assistance.

Enable Level Command Descriptions
Configuration Using The Command Line Interface

Network Monitoring

Three methods can be used to monitor Vivato Wi-Fi AP/Bridge operations and network traffic:

- The built-in web page user interface. To use the monitoring functions of the web interface, see "[Monitoring Clients and System Operations](#)" on page 79.
- Command line interface (CLI). A explanation of using the CLI and a list of the available commands to configure and monitor AP/Bridge operations is provided in "[Configuration Using The Command Line Interface](#)" on page 95.
- Simple network management protocol (SNMP).

SNMP Operations

You can use third-party SNMP management software to monitor operations within the Vivato Wi-Fi AP/Bridge. These software packages are designed to use standard SNMP versions that have been defined to work with devices created by various manufacturers. The Wi-Fi AP/Bridge supports SNMP versions 1, 2c, and 3.

SNMP applications use management information bases (MIBs) - databases of objects that are used to monitor and configure a device.

Operating Considerations

Not all MIB objects are supported in this version of the Vivato Wi-Fi AP/Bridge. The following information describes which MIBs are provided and which objects are and are not supported in this firmware release:

- SNMP walk performance issues - Performing an `snmpwalk` or `snmpbulkwalk` may time-out when trying to walk the entire MIB tree. Use the `-t` option to set the timer value higher than the default: `snmpwalk -c public -v 2c -t 15 10.0.0.2 .1` will allow a full 15 seconds from start to finish.
- SNMP Sets - In general, sets are not supported in this release.
- SNMPv2 Support Only - Currently SNMPv2c is the only supported version, though version 3 will be supported in the near future. Some, but not all, SNMPv3 options are supported in this release (v3 traps for example, ARE supported).

Supported MIB

The following MIB is included on the Vivato Wi-Fi AP/Bridge CD. Operating limitations are relevant for this firmware release, but may not be present in future firmware releases.

RFC1213-MIB.txt

The following limitations exist for this MIB in this firmware release:

The following are not supported:

- ipRouteTable
- egp
- transmission

A not-writable error will be returned during the set operation if the CLI or Web UI has been used to set the following:

- sysContact
- sysName
- sysLocation

Enabling SNMP Operation

To use SNMP in the Wi-Fi AP/Bridge, you need to enter some information and enable SNMP. This can be done using the web interface or by using the CLI. Refer to "[Configure SNMP-Server Commands](#)" on page 136 for a listing of the CLI commands used for setting up and enabling SNMP.

Several web configuration menus are used to configure SNMP operation after selecting **Networks>SNMP**.

The **Base SNMP Options** screen is used to enable SNMP operation and provide information used for all version of SNMP.

SNMP Configuration Information	
[Base SNMP Options]	[Community Options] [V3 Options] [V2 Options] [V1 Options]
These menus are used for configuring all versions of SNMP.	These menus are used to configure specific versions of SNMP.
Status:	DISABLED ▾
System Name:	Unknown System Name
System Location:	Unknown Location
System Contact:	Unknown System Contact
Current SNMP Community Settings: (select for removal)	public RO private RW
Current Trap Sinks: (select for removal)	
Make Base SNMP Changes	

Figure 35—SNMP Base Settings For All Version of SNMP

The **Community Options** menu is used to specify read-only or read-write privileges. Enter the name of an SNMP community to create and whether it allows read only (RO) or read-write (RW) operation. If the IP address is entered, only SNMP requests from the source IP address are honored.

Create SNMP Community:	
Community Name:	
Type:	RO ▾
IP Address (Optional):	
Create New Community	

Figure 36—Creating an SNMP Community

The remaining three menus are used for configuring specific SNMP versions.

SNMP v1 Options:	
Hostname/IP Address:	
Traps:	
Community Name:	
Create Trap Sink	

SNMP v2 Options:	
Hostname/IP Address:	
Trap Sink Type:	traps v
Community Name:	
Create Trap Sink	

SNMP v3 Options:	
Create v3 Trap Sink	Create v3 User
Hostname/IP Address:	Username:
Trap Sink Type: traps v	Optional Settings
Username:	Authentication Type: MD5 v
Optional Settings	Password:
Authentication Type: v	Privacy Type: DES v
Password:	Password:
Privacy Type: v	Create SNMP User
Password:	
Create Trap Sink	

Figure 37—Specifying Settings for SNMP Versions 1, 2c, and 3

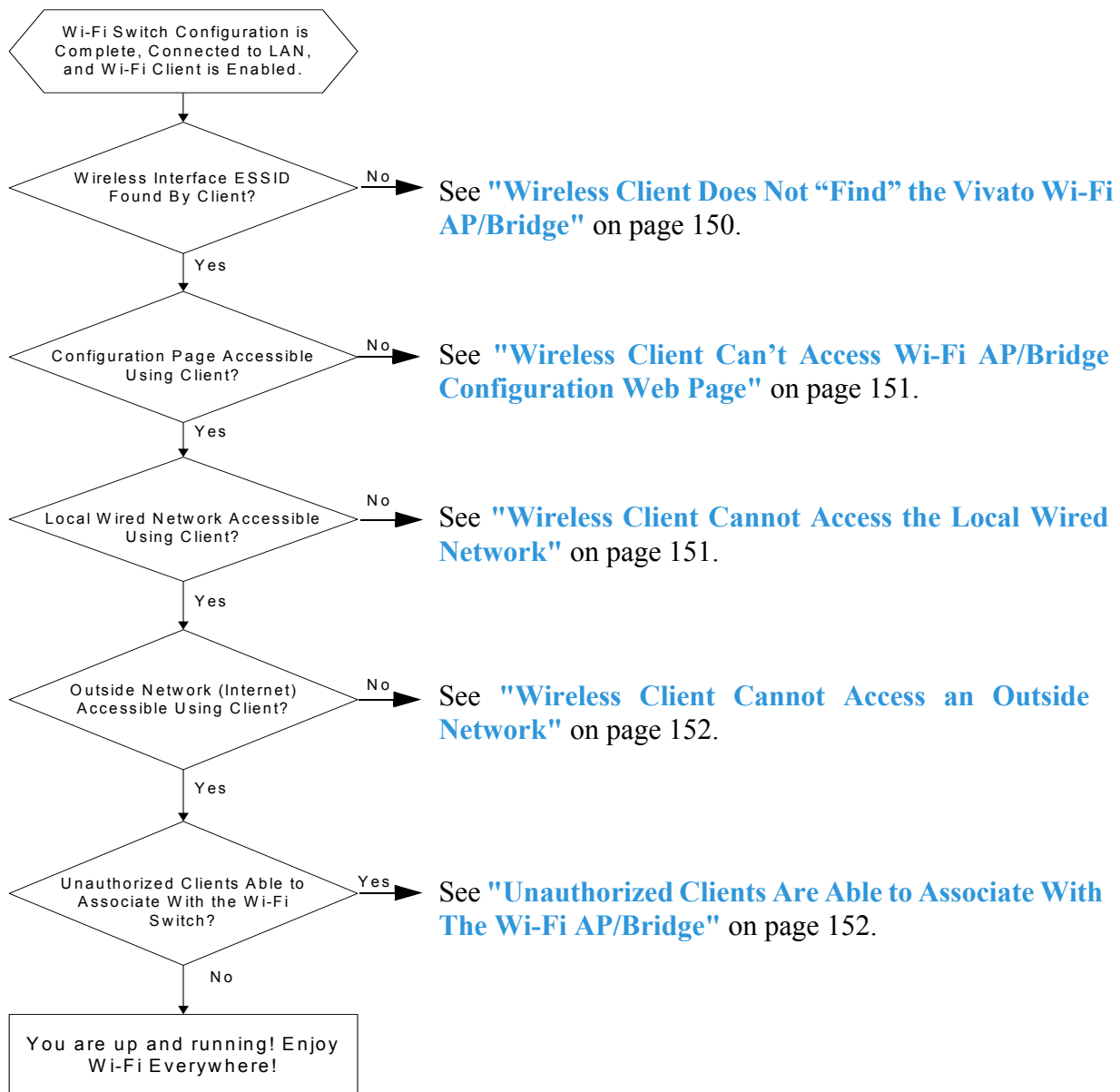
Verifying Wi-Fi Operation

After installing and configuring the Vivato Wi-Fi AP/Bridge, it is important to verify that it operates as intended. The information in this section is intended to help you verify Wi-Fi AP/Bridge operation and provides ideas to troubleshoot any configuration problems that you may have.

Use your Wi-Fi client's documentation to understand its configuration settings.

Verification Process

Use the following flowchart to verify Wi-Fi AP/Bridge operation and to identify some of the possible causes of problems you may encounter:



Wireless Client Does Not “Find” the Vivato Wi-Fi AP/Bridge

Part of configuring the Wi-Fi AP/Bridge involves entering the extended service set identifier (ESSID) for each wireless interface. This is the name that is displayed on your client’s list of available Wi-Fi networks. The following conditions must be present for the ESSID to be displayed on your client’s network list.

- The Wi-Fi AP/Bridge’s power LED must indicate that the AP/Bridge is operating. See ["Connectors and Indicators"](#) on page 23.
- At least one of the Wi-Fi AP/Bridge’s wireless interfaces must be enabled and the ESSID specified. See ["Network>Wireless Interfaces"](#) on page 66.
- Your Wi-Fi client is configured and working correctly. Refer to your client’s documentation.

Variations in Client Performance Due to Physical Orientation

The physical orientation of the client can have a direct effect on Wi-Fi operation, due to the variance in the antenna designs of clients. Studies have shown that rotating the client can significantly change the level of received signal in some cases.

If you are in an area that is partially blocked from the Wi-Fi AP/Bridge’s antenna pattern, try rotating the client 90 degrees (horizontally) to see if your reception is improved. You can also bend the AP/Bridge’s antennas up to 90 degrees to see what angle works best with the most clients.

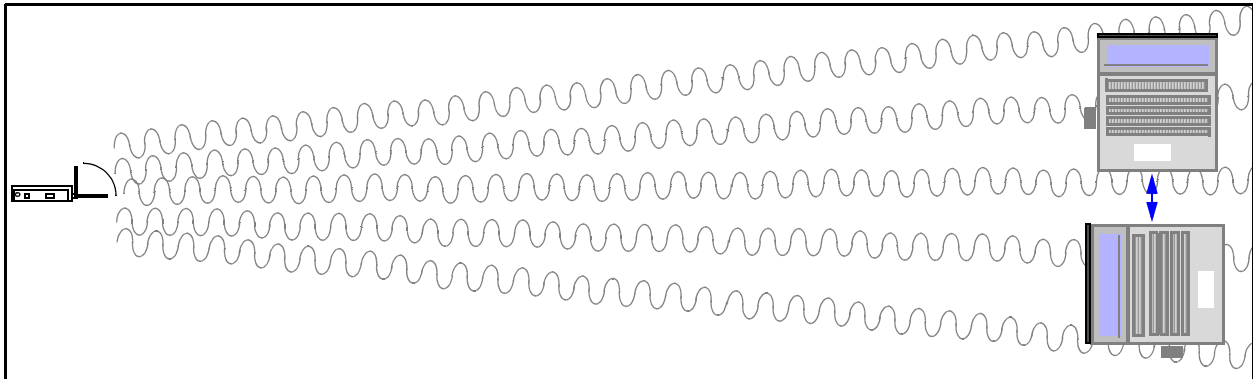


Figure 38—Rotating the Client to Improve Performance

Wireless Client Can't Access Wi-Fi AP/Bridge Configuration Web Page

For your client to associate with the Vivato Wi-Fi AP/Bridge, the following conditions must exist:

- The IP address of your wireless client must be within the same subnet range of the Wi-Fi AP/Bridge. The default IP address of the Wi-Fi AP/Bridge is 169.254.20.1. In some cases you can have your client automatically set its IP address within this range using automatic private IP addressing (see ["Using APIPA to Assign a Usable IP Address For Your Client"](#) on page 37).

You can also configure the Wi-Fi AP/Bridge to be a dynamic host configuration protocol (DHCP) server that assigns an IP address to your client when the client associates. See ["Network>DHCP"](#) on page 63.

You can also manually set the IP address of your client to use a static IP address by editing the **Internet Protocol (TCP/IP)** properties of your client, disabling automatic IP address assignment, and manually entering the address.

- The correct Address/Location must be specified in your web browser. See ["Configuration Connections"](#) on page 36.
- The security settings for your client and the Wi-Fi AP/Bridge must match. If you previously enabled security (such as WEP) in the Wi-Fi AP/Bridge, and your client's security settings are not providing access to the Wi-Fi AP/Bridge, you must use a wired connection to the Wi-Fi AP/Bridge to access the configuration web page and match the security settings between the AP/Bridge and your client. See ["Configuration Connections"](#) on page 36.
- The level of interfering signals must not be so great that the lowest allowed data rate (1 Mbps) cannot be used. Verify that Wi-Fi access points using the same channel assignments as the Wi-Fi AP/Bridge are not in close proximity. Also make sure that one or more microwave ovens are not operating within the Wi-Fi AP/Bridge's coverage area. See ["Network>Wireless Interfaces"](#) on page 66 and ["Interfering Signal Sources"](#) on page 30.

Wireless Client Cannot Access the Local Wired Network

If you are able to access the Vivato Wi-Fi AP/Bridge's configuration web page using your wireless client, but you are unable to access the wired network connected to one of the AP/Bridge's Ethernet ports, verify that the following conditions are present:

- The default bridge (br0) connecting the wireless interfaces to the Ethernet ports is enabled. See ["Network Settings"](#) on page 55.
- Your wired network is connected to the Wi-Fi AP/Bridge's Ethernet port.
- The Ethernet port you are connected to is enabled. The Vivato Wi-Fi AP/Bridge is pre configured with the Ethernet ports enabled. See ["Network>Ethernet Interface"](#) on page 65.
- The Vivato Wi-Fi AP/Bridge has been entered in the list of permissions for your local area

network (LAN) server. If your server uses an access list to allow access to the network, make sure that the Wi-Fi AP/Bridge has been added to that list.

- When authenticating through a RADIUS service, the RADIUS configuration information must be correctly entered. See "[Security>802.1x](#)" on page 72.
- The correct default gateway is specified. See "[Basic Network Setup](#)" on page 46.

Wireless Client Cannot Access an Outside Network

If you are able to connect to your local network through the Vivato Wi-Fi AP/Bridge, but you cannot access the Internet or another remote server, verify that the following conditions are present:

- The local network must have access to an Internet server; either its own server or through an internet service provider (ISP).
- If a modem (DSL or cable) is used to provide the internet connection through an ISP, the modem must be authenticated with the remote server. Refer to your modem's documentation or call your service provider for assistance.
- When authenticating through a RADIUS service, the RADIUS configuration information must be correctly entered. See "[Security>802.1x](#)" on page 72.
- The correct default gateway must be specified. See "[Basic Network Setup](#)" on page 46.

Unauthorized Clients Are Able to Associate With The Wi-Fi AP/Bridge

Security is disabled in the Wi-Fi AP/Bridge when delivered. If the security settings have not been configured and enabled, anyone with an IEEE 802.11b client can associate with the Wi-Fi AP/Bridge. To prevent this situation, enable the highest levels of security in the Wi-Fi AP/Bridge and your clients.

Connecting Through a WDS Connection

When using a WDS link between the AP/Bridge and a Vivato Wi-Fi Base Station, make sure the following configuration has been set ON BOTH DEVICES:

- A WDS interface was created AND ENABLED.
- The wireless interface MAC address used for the WDS connection of the opposing device has been set as the "peer address".
- The channel number of the wireless interface used for the WDS connection is the same.
- The wireless interface used for the WDS connection has been enabled.
- The WDS connection has been added to the bridge connecting the wireless interface to the Ethernet port (typically bridge 0).

Dynamic Assignment of Client IP Addresses

In order to communicate with the AP/Bridge, servers, and other devices on a network, clients must be configured to have an IP address within the same address range that is used by those devices. This is similar to a telephone connection, where only certain phone number prefixes are used within an area code to allow callers to talk to each other without being routed through long distance lines.

Client IP address assignment can be accomplished using statically configured IP addresses on each client or by using dynamic host control protocol (DHCP) operation to automatically set IP addresses.

Assigning static IP addresses requires each client to be manually configured by a user after being told what IP address to use by a system administrator. This is a slow and cumbersome operation when a large number of clients are used. It is also an inefficient use of IP addresses when some clients are not accessing the network.

How Does DHCP Work?

If clients are configured to use DHCP, IP addresses are automatically assigned to clients whenever they associate. If a DHCP server exists on your wired network, clients that associate with the AP/Bridge can request and receive an IP address from a pool of addresses configured on that server. Using this form of DHCP, all clients are assigned IP addresses that are on the same subnet as the AP/Bridge and its connected wired network (as shown below). This has the effect of using IP addresses from the same pool of addresses that are used by the wired network, reducing the number of devices that can exist on the network. This also allows wireless users to see the base IP address of your wired network by looking at their client settings.

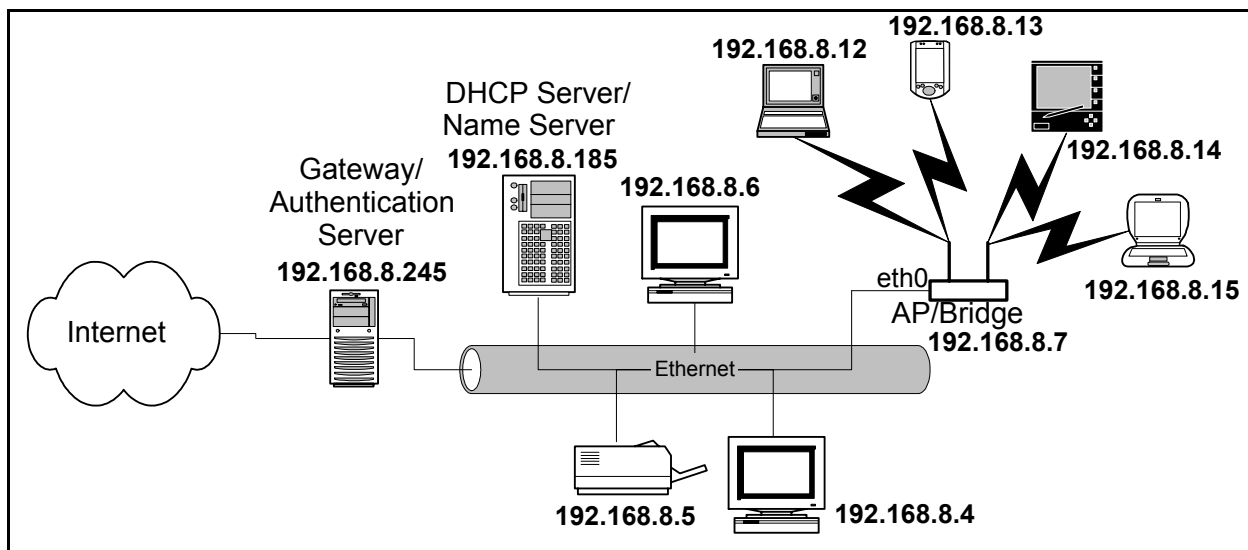


Figure 1—Wireless Client IP Address Assignment Using Your Network's DHCP Server¹

1. Network drawings shown in this document are for illustration purposes only.

What is Network Address Translation?

Dynamic Assignment of Client IP Addresses

The Vivato Wi-Fi AP/Bridge can be configured as a DHCP server. In conjunction with network address translation (NAT), this allows a totally different range of IP addresses to be used by your wireless clients than are used by your wired network. This results in only one IP address being used for all traffic to/from the AP/Bridge's connection to the wired network. In the network illustrated below, the AP/Bridge's Ethernet 0 (eth0) port is connected to the wired network using IP address 192.168.8.7. DHCP server operation is configured to issue IP addresses to wireless clients from a pool of addresses starting at 10.0.4.1. Even though they are on different subnets, the wireless clients are able to exchange packets with the wired network by using NAT.

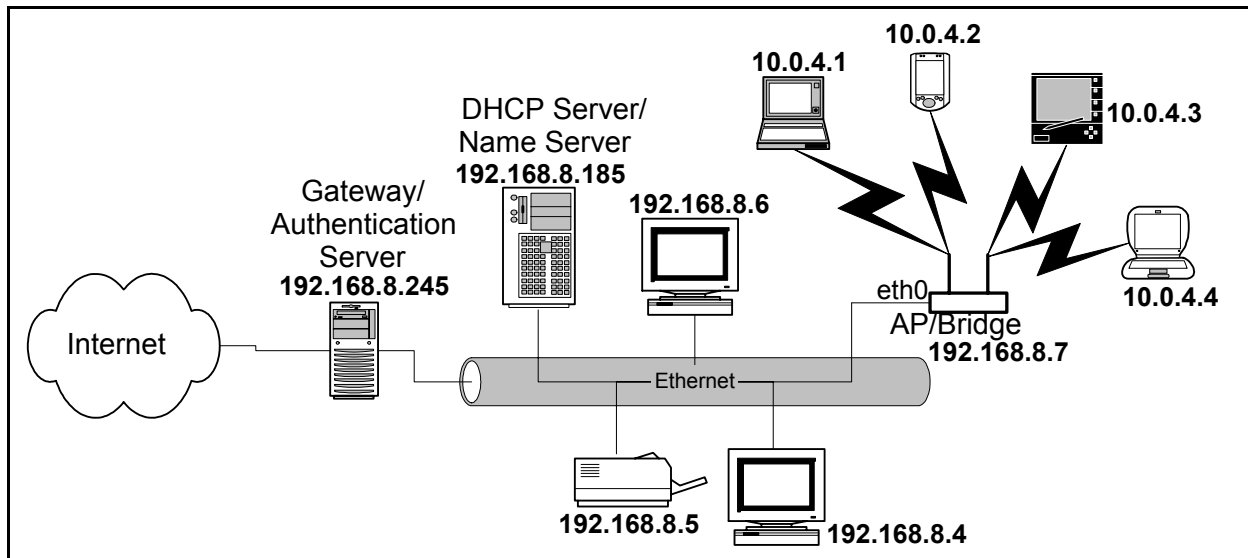


Figure 2—Using the AP/Bridge's DHCP Server and NAT to Assign Client IP Addresses

What is Network Address Translation?

NAT translates the source IP address for packets to/from different subnets to allow communication between them. In the figure above, the AP/Bridge replaces the source IP address on packets from wireless clients (10.0.4.x) with the IP address assigned to the eth0 port (192.168.8.7). Since the eth0 port's IP address is within the subnet used by the wired network, the packets are routed just as any other packet on the wired network. When a packet intended for a wireless client is received on the eth0 port, the AP/Bridge translates the IP address from the source 192.168.8.x address to the intended 10.0.4.x address.

“Breaking the Bridge”

As shown below, the AP/Bridge’s default configuration connects the Ethernet port (eth0) to both wireless interfaces (wlan0 & wlan1) using a bridge called “br0”.

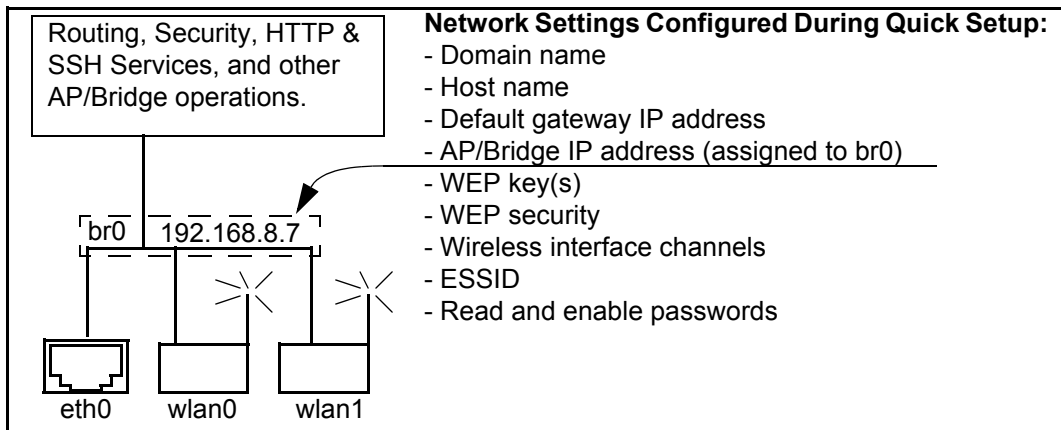


Figure 3—Default Configuration After Using the Quick Setup Web Pages

This is not a problem when using a network DHCP server to assign client IP addresses (as shown in [Figure 1— Wireless Client IP Address Assignment Using Your Network’s DHCP Server](#)).

However, to use the AP/Bridge as a DHCP server for your wireless clients, the Ethernet port must be removed from the bridge, otherwise the AP/Bridge will also respond to DHCP requests from devices connected to the Ethernet port. If a DHCP server already exists on your wired network, this could cause conflicts.

To isolate the Ethernet port from the default bridge, it must be removed using either the command line interface (CLI) or the Web interface. An IP address must then be assigned to the Ethernet port to enable access to the AP/Bridge from the wired network. After removing the Ethernet port from the bridge, IP routing must be enabled to route packets between the Ethernet port and the wireless interfaces. Going back to the telephone analogy, this is like routing a long distance call between different area codes.

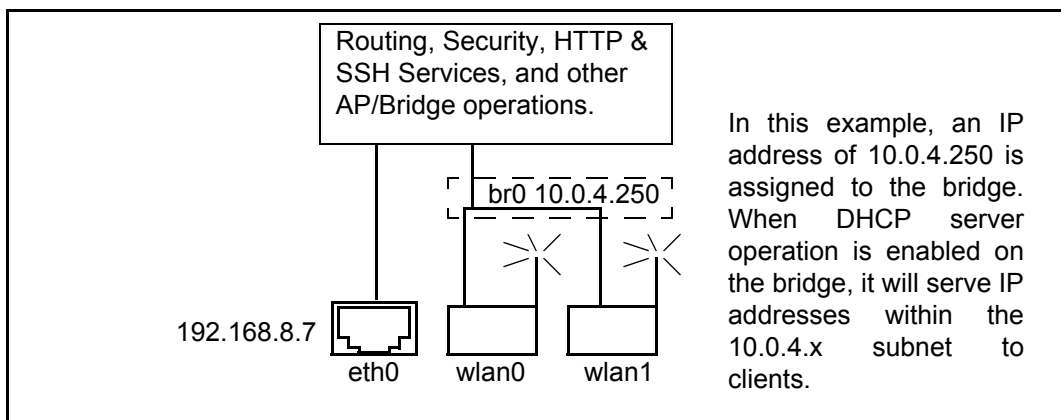


Figure 4—Removing Eth0 From the Default Bridge (br0) For DHCP Operation

Configuring DHCP Server Operation on the AP/Bridge

The following steps are used to configure DHCP server operation to provide client IP addresses. Entries marked optional indicate setting that are not absolutely necessary to have DHCP server operation working, but may be needed to access some wired network features.

These steps assume that the AP/Bridge was initially configured using the Quick Setup pages, and therefore the default bridge configuration exists:

- ☐ Remove eth0 from the default bridge (br0).
- ☐ Assign an IP address to br0 that is within the same subnet as the addresses to be assigned to wireless clients.
- ☐ Assign an IP address to the Ethernet interface (eth0) that is within the range of addresses used by your wired network.
- ☐ Set the DHCP broadcast address. This is the address used to send broadcast messages to all wireless clients.
- ☐ Set the DHCP domain name (optional). This is the name that refers to the bridge and the wireless clients associating with the AP/Bridge.
- ☐ Set the DHCP gateway IP address. This is the path (gateway) that the DHCP server uses to access the router function of the AP/Bridge. This is normally the IP address of the bridge.
- ☐ Enter the starting and ending IP addresses and net mask that define the pool of IP addresses that are served to wireless clients. Make sure that the IP address of the bridge is NOT inside this pool of addresses.
- ☐ Enter the DHCP lease time (optional). This value determines how long a client can continuously use an assigned IP address before it must ask to either renew this address or lose the IP connection.
- ☐ Enter the name server IP address. This is the name server on your wired network used to translate host names into IP addresses.
- ☐ Enter the network time protocol (ntp) server IP address (optional). This is used to sync the clock settings of your wireless client to your wired network.
- ☐ Enter the Windows internet naming service (WINS) server IP address (if used).
- ☐ Enable NAT for the bridge, specifying the Ethernet interface (eth0) as the source. This tells the DHCP server to use eth0's IP address as the source address for packets through the bridge.
- ☐ Enable the DHCP server for the bridge. The DHCP server is off by default, and must be enabled after it is configured.
- ☐ Enter a default route to your wired network's gateway. This tells the AP/Bridge where to send packets destined for an address outside of the local network.
- ☐ Enable global IP routing. This allows packets to be routed between the ethernet and bridge interfaces. Since the bridge no longer contains eth0, IP routing must be used to move packets between the Ethernet and wireless interfaces.

DHCP Server Configuration Example

The following CLI configuration example shows how the AP/Bridge can be configured to act as a DHCP server for clients connecting to the network shown below.

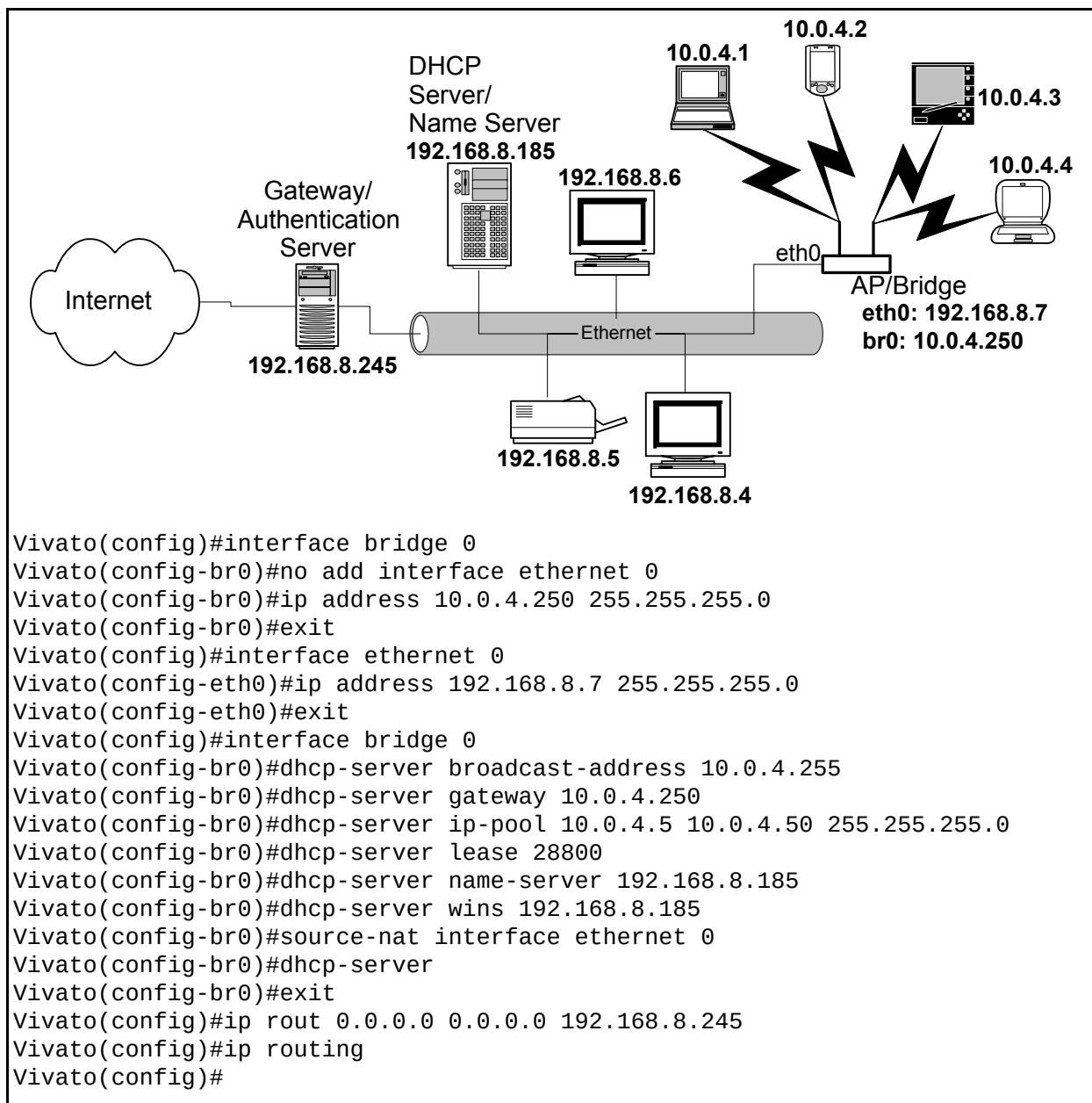


Figure 5—Configuring the AP/Bridge for DHCP Server Operation

Updating AP/Bridge Firmware

All of the AP/Bridge's features are contained in its firmware. As new features are created, new firmware downloads are made available on the Vivato Customer Support website to allow your AP/Bridge to be updated to provide those features.

Be sure to visit the Vivato Customer Support website and apply for a user password. After receiving the password by e-mail, go to www.vivato.net/access_cs.html, and enter your e-mail address and password to access the support page. Click on the Firmware Downloads tab and check to see if a later version of the firmware is available to download, along with the associated release notes and User Guide.

Using a Previously Saved Configuration With New Firmware

Due to changes in features, a saved configuration file from an older version of firmware may improperly configure the AP/Bridge after updating the firmware. Before loading and using new firmware, copy the "startup-config" file on the AP/Bridge to a computer that can display this text file for later use. After rebooting the AP/Bridge with the new firmware, use the saved configuration file as a guide to reconfiguring the AP/Bridge. Be sure to save the new configuration to preserve the changes.

A copy of the configuration can be saved to another computer using the **copy flash: scp:** or **copy flash: tftp:** CLI commands.

Updating Firmware Using the Command Line Interface (CLI)

Note: Updating firmware using the VivatoVision web interface is not available on this version of firmware.

Use these steps to update the software in your AP/Bridge:

- Step 1.** Using a web browser, download the new software image file from the Vivato support website onto a local computer on your network. Go to <http://www.vivato.net>, select the *Customer Support* link, and enter your e-mail address and password.
- Step 2.** Click on the **Firmware Downloads** link, set the **Product** field to "**AP/Bridge**", and then search the knowledge base for "**firmware**". A link is displayed to a page with the firmware file attached. Click on that file to download it.
- Step 3.** Use either the **copy scp: firmware:** command (if you are using a secured server) or the **copy tftp: firmware:** command (if you are using a TFTP server) to copy the software image file to the AP/Bridge.
- Step 4.** Reboot the AP/Bridge by disconnecting power for about 5 seconds and then reconnecting power.

Example TFTP Server Operation Using PumpKIN

Several free TFTP server programs are available via the Internet. One example is called “PumpKIN²”, and can be downloaded from www.klever.net/kin/pumpkin.html and installed in your computer. This is a freely-distributed program, and can be used to download a binary firmware image (.bin) file into the Vivato Wi-Fi Base Station or the Vivato AP/Bridge from a local PC.

This program is not associated with, and is not endorsed by, Vivato, Inc., and no guarantees concerning its continued availability or operation are intended or implied.

NOTE: Be sure to download the new AP/Bridge firmware from the Vivato Customer Support website, and save it in your computer, before running PumpKIN.

Configuring PumpKIN to “Put” a Firmware Image

Start PumpKIN on your computer. Select **Options**, and specify the directory path to the firmware binary file.

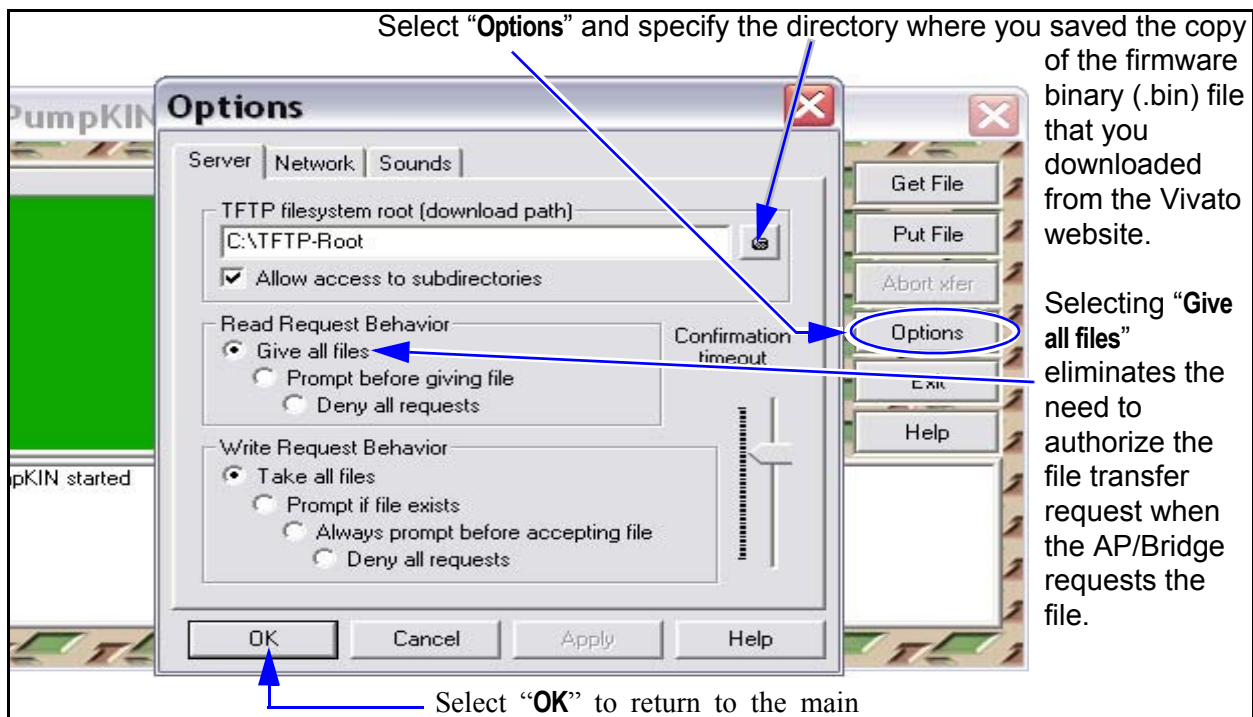


Figure 6— Telling PumpKIN to “Give all Files” When Requested by the AP/Bridge

2. Developed by: Klever Group, Inc. (<http://www.klever.net/>). Author: Michael Krelin (hacker@klever.net). Copyright 1997,1998 Klever Group, Inc.. Fan mail send to gefilte@klever.net

Select **Put File**. Select the firmware binary file to put to the AP/Bridge, and enter the IP address of the AP/Bridge.

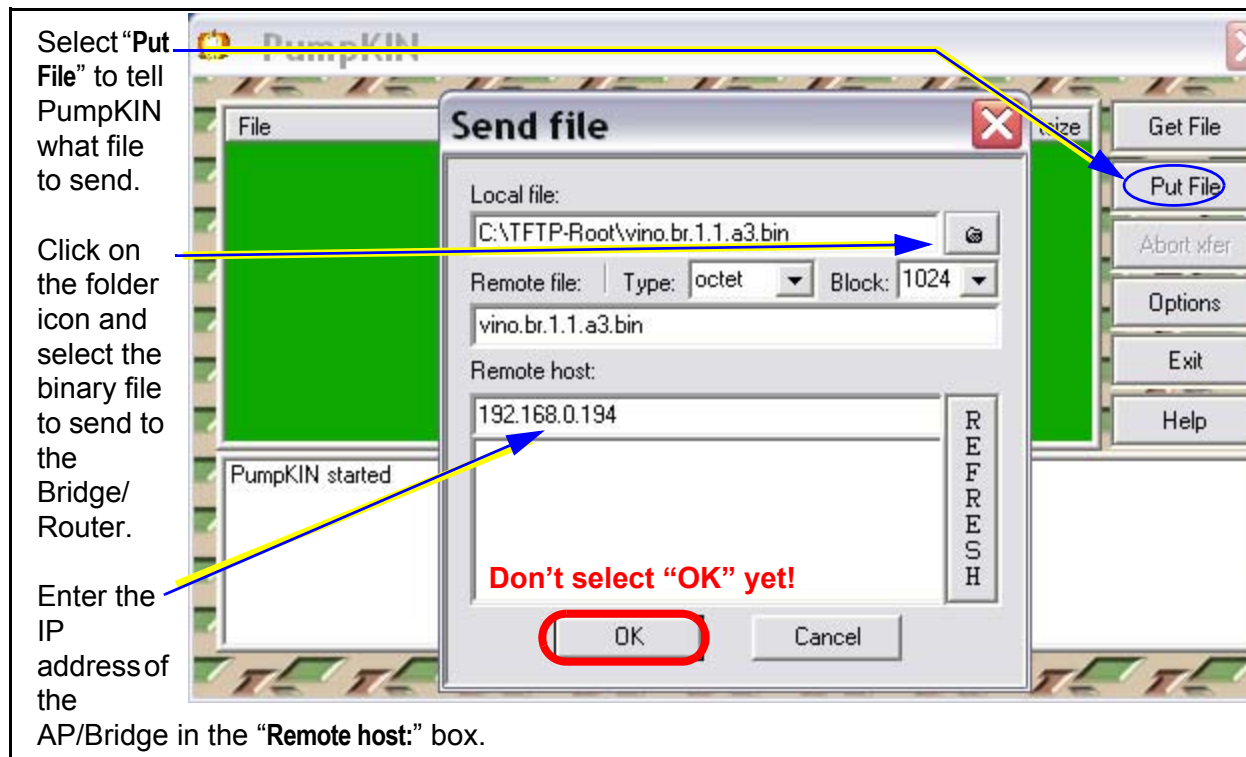


Figure 7— Specifying the File to Send and the IP Address of the AP/Bridge

Starting the TFTP File Transfer

Connect a CAT-5 *crossover* cable between the AP/Bridge and the PC's network interface card (NIC). If you are connecting the AP/Bridge to the PC through a hub, switch, or router, use standard CAT-5 patch cables.

With PumpKIN configured to send the file to the AP/Bridge, use the CLI to start transferring the file (as discussed earlier in this section). PumpKIN indicates the amount of data transferred and when the transfer has successfully completed.

Important 	If PumpKIN does not receive the TFTP request within its default time-out period (~30 seconds), it will refuse to send the file to the AP/Bridge. When both the AP/Bridge and PumpKIN have been configured, select OK on PumpKIN to allow it to send the file, then enter the final CLI TFTP command on the AP/Bridge to send the file request to PumpKIN and start the file transfer.
--	--

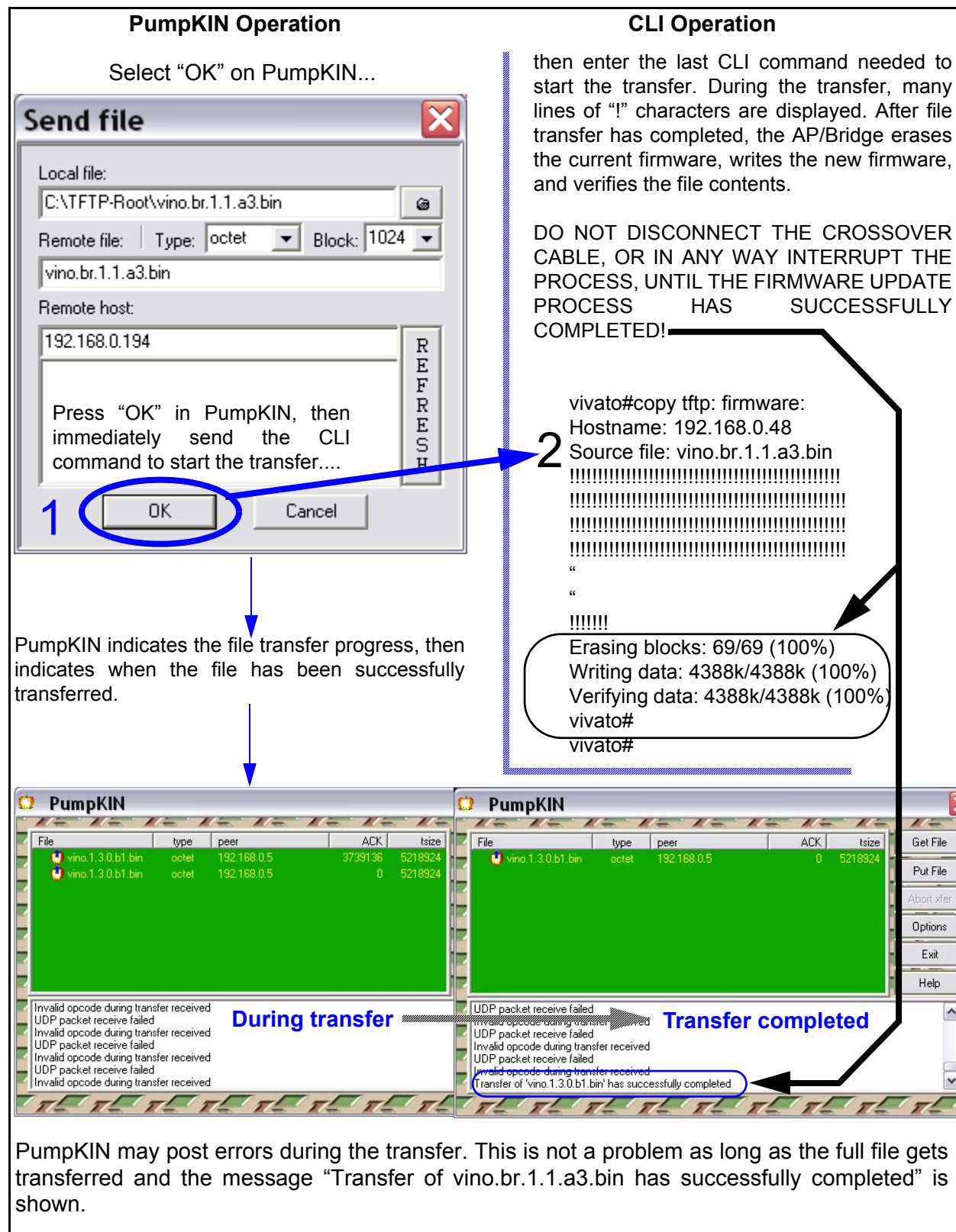


Figure 8— Starting the File Transfer From the Computer to the AP/Bridge

Index

Symbols

"Pumpkin" TFTP server 160

Numerics

802.1x Configuration (web) 72

A

antenna polarization 29

Associated Clients (web) 83

B

Bridge Devices (web) 60

bridge, default 36

C

channel number, assigning (web) 66

channel numbers (web) 66

channel, quick setup (web) 48

CLI (command line interface) 95

CLI commands

bridge interface 120

configure interfaces 119

configure network flash 114

configure terminal 114

copy flash

tftp

115

copy flash flash 115

copy flash scp 115

copy scp

firmware

116

copy scp flash 116

copy tftp

firmware

117

flash

117

crypto 118

delete 117

DHCP server 120

eap 128

edit flash 143

enable 102

enable secret 119

ethernet interface 126

exit 103

http server 119

iccf 122, 130

IP configuration 134

ip domainname 134

ip hostname 134

ip name-server 134

ip rout 134

ip routing 134

ip ssh bind interface 135

ip ssh genkey 135

ip ssh server 135

log 135

ping 103

rate limiting 135

reboot 143

rename flash

118

show (user level) 104

show interfaces 109

SNMP 136

support 143

traceroute 113

username secret 139

WDS 139

wireless interface 127

write network flash 118

write network scp 118

write terminal 118

CLI, connections 96

client IP address (web) 37

client IP addresses (web) 63

client security configuration 73

client-to-client blocking (ICCF) 122, 130

command line interface (CLI) 95

configuration 56, 65

wired connection 39

wireless connection (web) 41

wireless interfaces (web) 65

configuration (CLI), example 99

configuration (CLI), saving 118

configuration connections (web) 36

configuration file, edit (CLI) 143

configuration file, saving/retrieving (web) 88

configuration steps (web) 35

configuration, default 36

configuring the AP/Bridge (web) 35

customer support 13

D

default configuration 36
default configuration, restore 36
default ESSID 36
default gateway, quick setup (web) 46
default IP address 36
DHCP client control (CLI) 123
DHCP Operation (tutorial) 153
DHCP server configuration (CLI) 119
DHCP Server Configuration (web) 63
Diagnostics web page 93
documentation feedback 13
domain (specifying), quick setup (web) 46
domain name, quick setup (web) 46
domain name, specifying (CLI) 134

E

edit configuration file (CLI) 143
enable level password (CLI) 119
Enable Mode 45
enable password, changing (web) 88
enable password, quick setup (web) 45
ESSID beacons, disable (CLI) 128
ESSID, default 36
ESSID, quick setup (web) 48
ESSID, specifying (web) 66
ethernet interfaces (web) 65
ethernet interfaces, configuring (web) 56, 65

F

feedback, documentation 13
file, configuration (web) 88
firmware update command (CLI) 116, 117
firmware updates (web) 90
firmware version, reading (web) 85

G

gateway, quick setup (web) 46
gateway, specifying default 134

H

Help, web page help 94
Home configuration screen 52
host name, quick setup (web) 46
host name, specifying (CLI) 134
hostname, specifying (web) 46

HTTP, enabling 86

I

installation 29
inter-client communication filtering (ICCF) 122, 130
interference, signal 30
IP address, default 36, 60
IP address, quick setup (web) 46
IP address, specifying (web) 46
IP addresses, client 153
IP addresses, client (web) 63

L

logging support file 143

M

MAC address
 show version (CLI) 112
manual feedback 13
CLI commands
 write 118
MIB (mngmnt info base) 145
Monitoring web page 79
monitoring, network (SNMP) 145

N

name server, specifying (CLI) 134
net mask, quick setup (web) 46
Netmask, specifying (web) 46
Network

 Interfaces (web) 65
 Summary page 56
 web page settings 55
 wireless interfaces (web) 66

Network configuration screen 55
Network Interfaces (web) 55

O

obstructions, indoor 31, 32

P

password
 enable level (CLI) 119
 read level (CLI) 139
password, Enable Mode (web) 45
password, read level (web) 44
Passwords, changing (web) 88

PEAP (802.1x), client configuration 76
Ping (web) 93

Q

Quick Setup (web) 43

R

rate limiting (broadcast/multicast) (CLI) 135
read level password (CLI) 139
Read level password (web) 44
read password, changing (web) 88
read password, quick setup (web) 44
reboot, quick setup (web) 49
reboot, through web interface 86
register your Wi-Fi AP/Bridge 29
RESET button 36
restore default configuration 36
route, creating (CLI) 134
Routes, existing and creating (web) 57
RS-232, CLI access 96

S

saving CLI configuration (write file) 118
security, initial quick setup (web) 47
security, web page settings 71
serial number, displaying (CLI) 112
shipping contents 27
SNMP (Network Monitoring) 145
ssh enable/keys, generating (web) 87
SSH, enabling 86
SSID (ESSID) beacons, disable (CLI) 128
SSID blocking (disable beacon-ssid CLI) 128
status

- ethernet interfaces (web) 56, 65**
- wireless interfaces (web) 56, 65**

summary page, network 56
support, customer 13
support, generating system log (CLI) 143
System

- web page settings 85**

System messages (web) 79
System Services web page 86

T

TFTP Server operation 160
Traceroute (web) 94
troubleshooting operation 149

U

**update firmware (copy tftp
firmware)(CLI) 117**
update, firmware (web) 90
user name, specifying (CLI) 139

V

verifying operation 149

W

Warranty and End User License 3
WDS configuration (web) 68
WDS Configuration Example (CLI) 142
WDS, display configuration 109
web page, configuration 35
WEP configuration (web) 71
WEP, CLI configuration 132
WEP, client configuration 75
WEP, initial quick setup (web) 48
Win 2K IAS configuration for EAP 129
wireless distribution system (WDS) (CLI) 139
wireless interface

- channel numbers (web) 66**
- configuring (web) 66**
- enable/disable (web) 66**
- IP address (web) 66**
- netmask (web) 66**
- statistics (web) 66**

wireless interfaces (web) 56
wireless interfaces, configuring (web) 65

