

Latitude
Longitude
Height

General page - PTP 450i BHS

The General page of PTP 450i BHS is explained in [Table 116](#). The General page of PTP 450 BHS looks same as PTP 450i BHS.

Table 116 General page attributes – PTP 450i BHS

Device Type		
Timing Mode :	☐ Timing Master ☒ Timing Slave	
Link Speeds		
Link Speed :	Auto 1000F/100F/100H/10F/10H ▼	
PoE		
802.3at Type 2 PoE Status :	Not Present (Ignored)	
PoE Classification :	☐ Enabled ☒ Disabled	
Region Settings		
Region :	Other - Regulatory ▼	
Country :	Other ▼	
Web Page Configuration		
Webpage Auto Update :	1	Seconds (0 = Disable Auto Update)
Bridge Configuration		
Bridge Entry Timeout :	25	Minutes (Range : 25—1440 Minutes)
Bridging Functionality :	☐ Disable ☒ Enable	
Frame Timing		
Frame Timing Pulse Gated :	☒ Enable (If SM out of sync then do not propagate the frame timing pulse) ☐ Disable (Always propagate the frame timing pulse)	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	☐ Broadcast ☒ LLDP Multicast	
Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

Attribute	Meaning		
Timing Mode	Allows the user to choose the mode between Timing Master and Timing Slave.		
Link Speed	From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all BHM and BHSs in the operator network.		
802.3at Type 2 PoE Status and PoE Classification	When the PoE Classification functionality is enabled and if Type 2 power is not present, the PAs do not power up and draw too much power. By default, the PoE Classification feature is disabled and the PAs will power up regardless of the classification presented by the power source. This is supported only on 450i Series ODUs. PoE Classification configuration status also can be check under home > General > Device Information tab: <table> <tr> <td>802.3at Type 2 PoE Status :</td><td>Not Present (Ignored)</td></tr> </table>	802.3at Type 2 PoE Status :	Not Present (Ignored)
802.3at Type 2 PoE Status :	Not Present (Ignored)		
Region	This parameter allows you to set the region in which the radio will operate. The BHS radio automatically inherits the Region type of the master. This behavior ignores the value of the Region parameter in the BHS, even when the value is None. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter must be always set to the value that corresponds to the local region.		
Country	This parameter allows you to set the country in which the radio will operate. The BHS radio automatically inherits the Country Code type of the master. This behavior ignores the value of the Country parameter in the BHS, even when the value is None. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter must be always set to the value that corresponds to the local region. PMP/PTP 450i Series ODU shipped to the United States is locked to a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.		
Webpage Auto Update	See Table 113 General page attributes – PMP 450i AP on page 7-70		
Bridge Entry Timeout	Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the BHM encounters no activity with the BHS (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout must be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.		

 Caution This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 (minutes). An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.	
Bridging Functionality	See Table 113 General page attributes – PMP 450i AP on page 7-70
Frame Timing Pulse Gated	If this BHS extends the sync pulse to a BH master or an BHM, select either Enable—If this BHS loses sync from the BHM, then <i>do not</i> propagate a sync pulse to the BH timing master or other BHM. This setting prevents interference in the event that the BHS loses sync. Disable—If this BHS loses sync from the BHM, then propagate the sync pulse to the BH timing master or other BHM.
Multicast Destination Address	See Table 113 General page attributes – PMP 450i AP on page 7-70
Latitude Longitude Height	See Table 113 General page attributes – PMP 450i AP on page 7-70

PMP/PTP 450 Series



Note
Refer [Table 113](#) and [Table 114](#) for PMP 450 AP/SM General page parameters details.

General page - PMP 450 AP

Figure 119 General page attributes - PMP 450 AP

Device Type		
Device Setting :	☒ AP ☐ SM	
Link Speeds		
Link Speed :	Auto 100F/100H/10F/10H ▼	
Bandwidth Configuration Source		
Configuration Source :	SM ▼	
Sync Setting		
Sync Input :	AutoSync ▼	
AP Type :	☒ Standard AP ☐ Remote AP	
Region Settings		
Region :	Other - Regulatory ▼	
Country :	Other - FCC ▼	
Web Page Configuration		
Webpage Auto Update :	5 Seconds (0 = Disable Auto Update)	
Bridge Configuration		
Bridge Entry Timeout :	25 Minutes (Range : 25—1440 Minutes)	
Translation Bridging :	☐ Enabled ☒ Disabled	
Send Untranslated ARP :	☐ Enabled ☒ Disabled	
SM Isolation :	Disable SM Isolation ▼	
Packet Flooding :	☐ Bridge Flooding Enabled - Forward unknown unicast packets to all SMs. ☒ Bridge Flooding Disabled - Only forward learned unicast packets.	
Update Application Information		
Update Application Address :	0.0.0.0	
TCP Settings		
Prioritize TCP ACK :	☒ Enabled ☐ Disabled	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	☐ Broadcast ☒ LLDP Multicast	
DHCP Relay Agent		
DHCP Relay Agent :	Disable ▼	
DHCP Server (Name or IP Address) :	☐ Append DNS Domain Name ☒ Disable DNS Domain Name 255.255.255.255	
Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

General page - PMP 450 SM

Figure 120 General page attributes - PMP 450 SM

Link Speeds		
Link Speed :	Auto 100F/100H/10F/10H	
Ethernet Link Enable/Disable :	☒ Enabled ☐ Disabled	

Regional Settings		
Region :	Other - Regulatory	
Country :	Other	

Web Page Configuration		
Webpage Auto Update :	1	Seconds (0 = Disable Auto Update)

Bridge Configuration		
Bridge Entry Timeout :	25	Minutes (Range : 25—1440 Minutes)

Frame Timing		
Frame Timing Pulse Gated :	☒ Enable (If SM out of sync then do not propagate the frame timing pulse) ☐ Disable (Always propagate the frame timing pulse)	

Layer 2 Discovery Destination Address		
Multicast Destination Address :	☐ Broadcast ☒ LLDP Multicast	

Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

General page – PTP 450 BHM

Figure 121 General page attributes - PTP 450 BHM

Device Type		
Timing Mode :	☒ Timing Master ☐ Timing Slave	
Link Speeds		
Link Speed :	Auto 100F/100H/10F/10H ▼	
Sync Setting		
Sync Input :	Generate Sync ▼	
Regional Settings		
Region :	North America ▼	
Country :	United States ▼	
Web Page Configuration		
Webpage Auto Update :	1	Seconds (0 = Disable Auto Update)
Bridge Configuration		
Bridge Entry Timeout :	25	Minutes (Range : 25—1440 Minutes)
Bridging Functionality :	☐ Disable ☒ Enable	
Update Application Information		
Update Application Address :	0.0.0.0	
TCP Settings		
Prioritize TCP ACK :	☒ Enabled ☐ Disabled	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	☐ Broadcast ☒ LLDP Multicast	
Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

General page – PTP 450 BHS

Figure 122 General page attributes - PTP 450 BHS

Device Type		
Timing Mode :	☐ Timing Master ☒ Timing Slave	

Link Speeds		
Link Speed :	Auto 100F/100H/10F/10H ▼	

Regional Settings		
Region :	North America ▼	
Country :	United States ▼	

Web Page Configuration		
Webpage Auto Update :	0	Seconds (0 = Disable Auto Update)

Bridge Configuration		
Bridge Entry Timeout :	25	Minutes (Range : 25—1440 Minutes)
Bridging Functionality :	☐ Disable ☒ Enable	

Frame Timing		
Frame Timing Pulse Gated :	☒ Enable (If SM out of sync then do not propagate the frame timing pulse) ☐ Disable (Always propagate the frame timing pulse)	

Layer 2 Discovery Destination Address		
Multicast Destination Address :	☐ Broadcast ☒ LLDP Multicast	

Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

Configuring Unit Settings page

Applicable products	PMP : ☒ AP	☒ SM	PTP: ☒ BHM	☒ BMS
----------------------------	---	--	---	---

The **Unit Settings** page of the 450 Platform Family contains following options:

- Unit-Wide Changes
- Download Configuration File
- Upload and Apply Configuration File (for AP and BHM)
- LED Panel Settings (for SM and BHS)



Note

LED Panel setting is applicable for SM and BHS only.

Upload and Apply Configuration File attributes are not supported for SM and BHS.

The 450 Platform Family also supports import and export of configuration from the AP/BHM/SM/BHS as a text file. The configuration file is in JSON format. The logged in user must be an ADMINISTRATOR in order to export or import the configuration file.

The exported configuration file contains the complete configuration including all the default values. To keep a backup of the current configuration, the file can be saved as-is and imported later.

The configuration file supports encrypted password. The exported configuration file will contain encrypted password. The import of configuration can have either encrypted or plain text password in Configuration file. A new tab Encrypt the Password is added under Encrypted Password tab to generate encrypted password for a given password.

The Import and Export procedure of configuration file is described in [Import and Export of config file](#) on page 7-209.

LED Panel Mode has options select Revised mode and Legacy mode. The Legacy mode configures the radio to operate with standard LED behavior.

Unit Settings page of 450 Platform Family - AP/BHM

The Unit Setting page of AP/BHM is explained in [Table 117](#).

Table 117 Unit Settings attributes – 450 Platform Family AP/BHM

Default Plug Mode

Set To Factory Defaults Upon Default ☐ Enabled
Plug Mode Detection : ☒ Disabled

Unit-Wide Changes

Undo Unit-Wide Saved Changes Set to Factory Defaults

Encrypt the Password

Password :
Encrypted Password :
Encrypt the password

Download Configuration File

Configuration File : [0a003ea13575.cfg](#)

Upload and Apply Configuration File

File: Choose File No file chosen
Upload
Apply Configuration File

Status of Configuration File

Attribute	Meaning
Set to Factory Defaults Upon Default Mode Detection	If Enabled is checked, then the default mode functions is enabled. When the module is rebooted with Default mode enabled, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override <i>cannot</i> see or learn the settings that were previously configured in it. If Disabled is checked, then the default mode functions is disabled. See Radio recovery mode on page 1-24
	 Caution When Set to Factory Defaults Upon Default Mode is set to Enable, the radio does not select all of the frequencies for Radio Frequency Scan Selection List. It needs to be selected manually.
Undo Unit-Wide Saved Changes	When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults	When you click this button, <i>all configurable parameters on all tabs</i> are reset to the factory settings. Note This can be reverted by selecting "Undo Unit-Wide Saved Changes", <i>before</i> rebooting the radio, though this is not recommended.
Password	This allows to provide encrypted password for a given password. On click of 'Encrypt the password' button, the Encrypted Password field will display encrypted value of entered plain text password in 'Password' field.
Configuration File	This allows to download the configuration file of the radio. This configuration file contains the complete configuration including all the default values. The configuration file is highlighted as downloadable link and the naming convention is "<mac address of AP>.cfg".
Apply Configuration File	This allows to import and apply configuration to the AP. Chose File: Select the file to upload the configuration. The configuration file is named as "<file name>.cfg". Upload: Import the configuration to the AP. Apply Configuration File: Apply the imported configuration file to the AP. The imported configuration file may either contain a full device configuration or a partial device configuration. If a partial configuration file is imported, only the items contained in the file will be updated, the rest of the device configuration parameters will remain the same. Operators may also include a special flag in the configure file to instruct the device to first revert to factory defaults then to apply the imported configuration.
Status of Configuration file	This section shows the results of the upload.

Unit Settings page of PMP/PTP 450i SM/BHS

The Unit Settings page of PMP/PTP 450i SM/BHS is explained in [Table 118](#).

Table 118 SM Unit Settings attributes

Default Plug Mode

Set To Factory Defaults Upon Default Plug Mode Detection :

Enabled

Disabled

LED Panel Settings

LED Panel Mode :

Revised Mode (Optimized For Indoor SM)

Legacy Mode

Unit-Wide Changes

Undo Unit-Wide Saved Changes

Set to Factory Defaults

Encrypt the Password

Password :

Encrypted Password :

Encrypt the password

Download Configuration File

Configuration File :

[0a003ea0a066.cfg](#)

Upload and Apply Configuration File

Configuration file import is currently unsupported over the web proxy.

Status of Configuration File

Attribute	Meaning
Set to Factory Defaults Upon Default Plug Detection	See Table 117 Unit Settings attributes – 450 Platform Family AP/BHM on page 7-90
LED Panel Settings	Legacy Mode configures the radio to operate with standard LED behavior.
Undo Unit-Wide Saved Changes	
Password	
Set to Factory Defaults	See Table 117 Unit Settings attributes – 450 Platform Family AP/BHM on page 7-90
Configuration File	
Status of Configuration file	

Setting up time and date

Time page of 450 Platform Family - AP/BHM

Applicable products

PMP: ☒ APPTP: ☒ BHM

The Time page of 450 Platform Family AP/BHM is explained in [Table 119](#).

Table 119 450 Platform Family - AP/BHM Time attributes

NTP Server Configuration

NTP Server (Name or IP Address) : ☐ Append DNS Domain Name
☒ Disable DNS Domain Name

NTP Server 1 (Name or IP Address) :

NTP Server 2 (Name or IP Address) :

NTP Server 3 (Name or IP Address) :

NTP Server(s) In Use : pool.ntp.org (108.61.73.244)

Current System Time

Time Zone :

System Time : 20:33:13 06/26/2013 UTC

Last NTP Time Update : 20:32:07 06/26/2013 UTC

Time and Date

Time : : : UTC

Date : / /

NTP Update Log

06/26/2013 : 20:32:07 UTC : Clock Updated, Server 1

Attribute	Meaning
NTP Server (Name or IP Address)	The management DNS domain name may be toggled such that the name of the NTP server only needs to be specified and the DNS domain name is automatically appended to that name.
NTP Server 1 (Name or IP Address)	To have each log in the AP/BHM correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP/BHM or must set the time and date whenever a power cycle of the AP/BHM has occurred. A network element passes time and date in any of the following scenarios:
NTP Server 2 (Name or IP Address)	
NTP Server 3 (Name or IP Address)	
	- A connected CMM4 passes time and date (GPS time and date, if received). - A connected CMM4 passes the time and date (GPS time and date, if received), but only if both the CMMr is operating on CMMr Release 2.1 or later release. (These releases include NTP server functionality.)

-
- A separate NTP server (including APs/BHMs receiving NTP data) is addressable from the AP/BHM.

If the AP/BHM needs to obtain time and date from a CMM4, or a separate NTP server, enter the IP address or DNS name of the CMM4 or NTP server on this tab. To force the AP/BHM to obtain time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time via NTP**.

The polling of the NTP servers is done in a sequential fashion, and the polling status of each server is displayed in the NTP Update Log section of the Time Configuration page. An entry of 0.0.0.0 in any of the NTP Server fields indicates an unused server configuration.

NTP Server(s) in Use	Lists the IP addresses of servers used for NTP retrieval.
Time Zone	The Time Zone option may be used to offset the received NTP time to match the operator's local time zone. When set on the AP/BHM, the offset is set for the entire sector SMs (or BHS) are notified of the current Time Zone upon initial registration). If a Time Zone change is applied, the SMs(or BHS) is notified of the change in a best effort fashion, meaning some SMs//BHSs may not pick up the change until the next re-registration. Time Zone changes are noted in the Event Log of the AP/BHM and SM/BHS.
System Time	The current time used by the system.
Last NTP Time Update	The last time that the system time was set via NTP.
Time	This field may be used to manually set the system time of the radio.
Date	This field may be used to manually set the system date of the radio.
NTP Update Log	This field shows NTP clock update log. It includes NTP clock update Date and Time stamp along with server name.

Configuring synchronization

Applicable products

PMP : ☒ AP

PTP: ☒ BHM

This section describe synchronization options for PMP and PTP configuration.

This **Sync Input** parameter can be configured under Sync Setting tab of **Configure > General** page (see [General configuration](#) on page 7-70).

PMP/PTP 450i Series has following synchronization options:

- AutoSync
- AutoSync + Free Run
- Generate Sync
- Free Run Before GPS Sync

Figure 123 Sync Setting configuration

AutoSync

For PTP, the BHM automatically receives sync from one of the following sources:

- GPS Sync over Timing Port (UGPS, co-located AP GPS sync output, or “Remote ” Device feed from a registered SM’s GPS sync output)
- GPS Sync over Power Port (CMM4)

Upon AP/BM power on, the AP/BHM does not transmit until a valid synchronization pulse is received from one of the sources above. If there is a loss of GPS synchronization pulse, within two seconds the AP/BHM automatically attempts to source GPS signaling from another source.

In case of PMP, when there are synchronization sources on both the timing port and the power port, the power port GPS source is chosen first.

If no valid GPS signal is received, the AP/BHM ceases transmission and SM/BHS registration is lost until a valid GPS signal is received again on the AP or BHM.



Note

After an AP reboot, the sync acquisition takes a little longer than it had on 450i (anywhere from 40 seconds to 120 seconds difference).

AutoSync + Free Run

This mode operates similarly to mode “AutoSync”, but if a previously received synchronization signal is lost and no GPS signaling alternative is achieved, the AP/BHM automatically changes to synchronization mode “Generate Sync”. While SM registration ins maintained, in this mode there is no synchronization of APs/BHMs that can “hear” each other; the AP/BHM will only generate a sync signal for the local AP/BHM and its associated SMs/BHS. Once a valid GPS signal is obtained again, the AP/BHM automatically switches to receiving synchronization via the GPS source and SM/BHS registration is maintained.

When the Sync Input field is set to Autosync or Autosync + Free Run, other options become available to be set e.g. UGPS Power and other fields. This is true on APs and BHMs.



Note

In mode AutoSync + Free Run, if a GPS signal is never achieved initially, the system will not switch to “Free Run” mode, and SMs/BHS will not register to the AP/BHM. A valid GPS signal must be present initially for the AP to switch into “Free Run” mode (and to begin self-generating a synchronization pulse).

Also, When an AP/BHM is operating in “Free Run” mode, over a short time it will no longer be synchronized with co-located or nearby APs/BHMs (within radio range). Due to this lack of transmit and receive synchronization across APs/BHMs or across systems, performance while in “Free Run” mode may be degraded until the APs/BHMs operating in “Free Run” mode regain a external GPS synchronization source. Careful attention is required to ensure that all systems are properly receiving an external GPS synchronization pulse, and please consider “Free Run” mode as an emergency option.

Generate Sync (factory default)

This option may be used when the AP/BHM is not receiving GPS synchronization pulses from either a CMM4 or UGPS module, and there are no other APs/BHMs active within the link range. Using this option will not synchronize transmission of APs/BHMs that can “hear” each other; it will only generate a sync signal for the local AP/BHM and its associated SMs/BHS.



Note

When an AP/BHM has its “Regional Code” set to “None”, The radio will not provide valid Sync Pulse Information.

There is a RED warning that the radio will not transmit, but the user might expect to see a valid sync if the radio is connected to a working CMM4 or UGPS.

Configuring security

Perform this task to configure the 450 Platform system in accordance with the network operator's security policy. Choose from the following procedures:

- [Managing module access by password](#) on page 7-98: to configure the unit access password and access level
- [Isolating from the internet](#) on page 7-101: to ensure that APs are properly secured from external networks
- [Encrypting radio transmissions](#) on page 7-101: to configure the unit to operate with AES or DES wireless link security
- [Requiring SM Authentication](#) on page 7-102: to set up the AP to require SMs to authenticate via the AP, WM, or RADIUS server
- [Filtering protocols and ports](#) on page 7-103: to filter (block) specified protocols and ports from leaving the system
- [Encrypting downlink broadcasts](#) on page 7-106: to encrypt downlink broadcast transmissions
- [Isolating SMs](#) on page 7-106: to prevent SMs in the same sector from directly communicating with each other
- [Filtering management through Ethernet](#) on page 7-107: to prevent management access to the SM via the radio's Ethernet port
- [Allowing management only from specified IP addresses](#) on page 7-107: to only allow radio management interface access from specified IP addresses
- [Restricting radio Telnet access over the RF interface](#) on page 7-107: to restrict Telnet access to the AP
- [Configuring SNMP Access](#) on page 7-110
- [Configuring Security](#) on page 7-112

Managing module access by password

Applicable products PMP : ☒ AP ☒ SM PTP: ☒ BHM ☒ BMS

See [Managing module access by passwords](#) on page 3-39.

Adding a User for Access to a module

The **Account > Add User** page allows to create a new user for accessing 450 Platform Family - AP/SM/BHM/BHS. The Add User page is explained in [Table 120](#).

Table 120 Add User page of account page - AP/ SM/BH

Attribute	Meaning
User Name	User Account name.
Level	Select appropriate level for new account. It can be INSTALLER, ADMINISTRATOR or TECHNICIAN. See Managing module access by passwords on page 3-39.
New Password	Assign the password for new user account
Confirm Password	This new password must be confirmed in the “ Confirm Password ” field.
User Mode	User Mode is used to create an account which are mainly used for viewing the configurations. The local and remote Read-Only user account can be created by “Admin”, “Installer” or “Tech” logins. To create a Read-Only user, the “read-only” check box needs to be checked.



Note

The Read-Only user cannot perform any service impacting operations like creating read-only accounts, editing and viewing read-only user accounts, changes in login page, read-only user login, Telnet access, SNMP, RADIUS and upgrade/downgrade.

Deleting a User from Access to a module

The **Account > Delete User** page provides a drop down list of configured users from which to select the user you want to delete. The Delete User page is explained in [Table 121](#).

Table 121 Delete User page - 450 Platform Family - AP/ SM/BH

Delete User User : admin Delete Account Status	
Attribute	Meaning
User	Select a user from drop down list which has to be deleted and click Delete button. Accounts that cannot be deleted are - the current user's own account. - the last remaining account of ADMINISTRATOR level.

Changing a User Setting

The **Account > Change User Setting** page allows to update password, mode update and general status permission for a user.

From the factory default state, configure passwords for both the root and admin account at the ADMINISTRATOR permission level, using **Update Password** tab of Change Users Setting page. The Change User Setting page is explained in [Table 122](#).

Table 122 Change User Setting page - 450 Platform Family AP/ SM/BH

Update Password User : admin New Password : Confirm Password : Change Password Update Mode User : test User Mode : read-only Change Mode General Status Permission General Status Page Viewable to Guest Users : Enabled Disabled Change Permission Account Status	
--	--

Attribute	Meaning
Update Password tab	This tab provides a drop down list of configured users from which a user is selected to change password.
Update Mode tab	This tab facilitates to convert a configured user to a Read-Only user.
General Status Permission tab	This tab enables and disables visibility of General Status Page for all Guest user. To display of Radio data on SMs/BHS main Login page for Guest login, it can be enabled or disabled in Security tab of Configuration page.

Figure 124 AP Evaluation Configuration parameter of Security tab for PMP

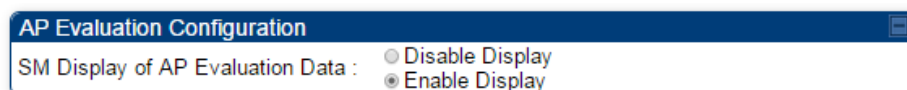
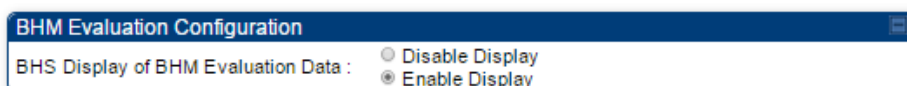


Figure 125 BHM Evaluation Configuration parameter of Security tab for PTP



Users account

The **Account > Users** page allows to view all configured users account for accessing the module. The Users page is explained in [Table 123](#).

Table 123 User page –450 Platform Family AP/SM/BH

Username	Permission	Mode
admin	ADMINISTRATOR	Read-Write
root	ADMINISTRATOR	Read-Write
ins	INSTALLER	Read-Write

Attribute	Meaning
Username	User access account name
Permission	Permission of configured user – INSTALLER, ADMINISTRATOR or TECHNICIAN
Mode	This field indicate access mode of user – Read-Write or Read-Only.

Overriding Forgotten IP Addresses or Passwords on AP and SM

See [Radio recovery mode](#) on page 1-24

Isolating from the internet – APs/BHMs

Applicable products	PMP: ☒ AP	PTP: ☒ BHM
---------------------	---	--

See [Isolating AP/BHM from the Internet](#) on page 3-37.

Encrypting radio transmissions

Applicable products	PMP: ☒ AP ☒ SM	PTP: ☒ BHM ☒ BMS
---------------------	--	--

See [Encrypting radio transmissions](#) on page 3-37.

Requiring SM Authentication

Applicable products	PMP : ☒ AP ☒ SM
---------------------	---

Through the use of a shared AP key, or an external RADIUS (Remote Authentication Dial In User Service) server, it enhances network security by requiring SMs to authenticate when they register. For descriptions of each of the configurable security parameters on the AP, see [Configuring Security](#) on page 7-112. For descriptions of each of the configurable security parameters on the SM, see [Security](#) on page 7-117.

Operators may use the AP's **Authentication Mode** field to select from among the following authentication modes:

- **Disabled**—the AP requires no SMs to authenticate (factory default setting).
- **Authentication Server** —the AP requires any SM that attempts registration to be authenticated in Wireless Manager before registration
- **AP PreShared Key** - The AP acts as the authentication server to its SMs and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP and all SMs desired to register to that AP. There is also an option of leaving the AP and SMs at their default setting of using the "Default Key". Due to the nature of the authentication operation, if you want to set a specific authentication key, then you **MUST** configure the key on all of the SMs and reboot them **BEFORE** enabling the key and option on the AP. Otherwise, if you configure the AP first, none of the SMs is able to register.
- **RADIUS AAA** - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.

For more information on configuring the PMP 450 Platform network to utilize a RADIUS server, see [Configuring a RADIUS server](#) on page 7-217.

Filtering protocols and ports

Applicable products PMP : ☒ AP ☒ SM PTP: ☒ BHM ☒ BMS

The filtering protocols and ports allows to configure filters for specified protocols and ports from leaving the AP/SM/BHM/BHS and entering the network. See [Filtering protocols and ports](#) on page 3-40.

Protocol filtering page of 450 Platform Family AP/BHM

The Protocol Filtering page of 450 Platform Family - AP/BHM is explained in [Table 124](#).

Table 124 AP/BHM Protocol Filtering attributes

Packet Filter Configuration

Packet Filter Types :

☒ PPPoE

☐ All IPv4

☐ SMB (Network Neighborhood)

☐ SNMP

☐ Bootp Client

☐ Bootp Server

☐ IPv4 Multicast

☐ User Defined Port 1 (See Below)

☐ User Defined Port 2 (See Below)

☐ User Defined Port 3 (See Below)

☐ All other IPv4

☐ All IPv6

☐ SMB (Network Neighborhood)

☐ SNMP

☐ Bootp Client

☐ Bootp Server

☐ IPv6 Multicast

☐ All other IPv6

☐ ARP

☐ All others

Filter Direction :

☐ Upstream

☐ Downstream

User Defined Port Filtering Configuration

Port #1 :

0

(Decimal Value)

TCP :

☐ Enabled

☒ Disabled

UDP :

☐ Enabled

☒ Disabled

Port #2 :

0

(Decimal Value)

TCP :

☐ Enabled

☒ Disabled

UDP :

☐ Enabled

☒ Disabled

Port #3 :

0

(Decimal Value)

TCP :

☐ Enabled

☒ Disabled

UDP :

☐ Enabled

☒ Disabled

AP Specialty Filters

RF Telnet Access :

☒ Enabled

☐ Disabled

PPPoE PADI Downlink Forwarding :

☒ Enabled

☐ Disabled

Page 7-103

Attribute	Meaning
Packet Filter Types	For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. To filter packets in any of the user-defined ports, must do all of the following: Check the box for User Defined Port <i>n</i> (See Below) in the Packet Filter Types section of this tab. In the User Defined Port Filtering Configuration section of this tab: • provide a port number at Port #<i>n</i>. • enable TCP and/or UDP by clicking the associated radio button
Filter Direction	Operators may choose to filter upstream (uplink) RF packets or downstream (downlink) RF packets.
User Defined Port Filtering Configuration	You can specify ports for which to block subscriber access, regardless of whether NAT is enabled.
RF Telnet Access	RF Telnet Access restricts Telnet access to the AP/BHM from a device situated below a network SM/BHS (downstream from the AP/BHM). This is a security enhancement to restrict RF-interface sourced AP access specifically to the LAN1 IP address and LAN2 IP address (Radio Private Address, typically 192.168.101.[LUID]). This restriction disallows unauthorized users from running Telnet commands on the AP/BHM that can change AP/BHM configuration or modifying network-critical components such as routing and ARP tables.
PPPoE PADI Downlink Forwarding	Enabled: the AP/BHM allows downstream and upstream transmission of PPPoE PADI packets. By default, PPPoE PADI Downlink Forwarding is set to “Enabled”. Disabled: the AP/BHM disallows PPPoE PADI packets from entering the Ethernet interface and exiting the RF interface (downstream to the SM/BHS). PPPoE PADI packets are still allowed to enter the AP’s RF interface and exit the AP’s /BHM’s Ethernet interface (upstream).

Protocol filtering page of SM/BHS

The Protocol Filtering page of SM/BHS is explained in [Table 125](#).

Table 125 SM/BHS Protocol Filtering attributes

Packet Filter Configuration

Packet Filter Types :

☐ PPPoE

☐ All IPv4

☐ SMB (Network Neighborhood)

☐ SNMP

☐ Bootp Client

☐ Bootp Server

☐ IPv4 Multicast

☐ User Defined Port 1 (See Below)

☐ User Defined Port 2 (See Below)

☐ User Defined Port 3 (See Below)

☐ All other IPv4

☐ All IPv6

☐ SMB (Network Neighborhood)

☐ SNMP

☐ Bootp Client

☐ Bootp Server

☐ IPv6 Multicast

☐ All other IPv6

☐ ARP

☐ All others

Filter Direction :

☐ Upstream

☐ Downstream

User Defined Port Filtering Configuration

Port#1 :

0

(Decimal Value)

TCP :

☐ Enabled

☒ Disabled

UDP :

☐ Enabled

☒ Disabled

Port#2 :

0

(Decimal Value)

TCP :

☐ Enabled

☒ Disabled

UDP :

☐ Enabled

☒ Disabled

Port#3 :

0

(Decimal Value)

TCP :

☐ Enabled

☒ Disabled

UDP :

☐ Enabled

☒ Disabled

Attribute	Meaning
Packet Filter Configuration tab	See Table 124 AP/BHM Protocol Filtering attributes on page 7-103
User Defined Port Filtering Configuration tab	See Table 124 AP/BHM Protocol Filtering attributes on page 7-103

Page 7-105

Port configuration

450 Platform Family ODUs support access to various communication protocols and only the ports required for these protocols are available for access by external entities. Operators may change the port numbers for these protocols via the radio GUI or SNMP.

The **Port Configuration** page of the AP/SM/BHM/BHS is explained in [Table 126](#).

Table 126 Port Configuration attributes – AP/SM/BHM/BMS

Port Configuration		
FTP Port :	21	Default port number is 21
HTTP Port :	80	Default port number is 80
HTTPs Port :	443	Default port number is 443
Radius Port :	1812	Default port number is 1812
Radius Accounting Port :	1813	Default port number is 1813
SNMP Port :	161	Default port number is 161
SNMP Trap Port :	162	Default port number is 162
Syslog Server Port :	514	Default port number is 514

Attribute	Meaning
FTP Port	The listen port on the device used for FTP communication.
HTTP Port	The listen port on the device used for HTTP communication.
HTTPS Port	The listen port on the device used for HTTPS communication.
Radius Port	The destination port used by the device for RADIUS communication.
Radius Accounting Port	The destination port used by the device for RADIUS accounting communication.
SNMP Port	The listen port on the device used for SNMP communication.
SNMP Trap Port	The destination port used by the device to which SNMP traps are sent.
Syslog Server Port	The destination port used by the device to which Syslog messaging is sent.

Encrypting downlink broadcasts

See [Encrypting downlink broadcasts](#) on page 3-44.

Isolating SMs

See [Isolating SMs in PMP](#) on page 3-44.

Filtering management through Ethernet

See [Filtering management through Ethernet](#) on page 3-44.

Allowing management only from specified IP addresses

See [Allowing management from only specified IP addresses](#) on page 3-45.

Restricting radio Telnet access over the RF interface

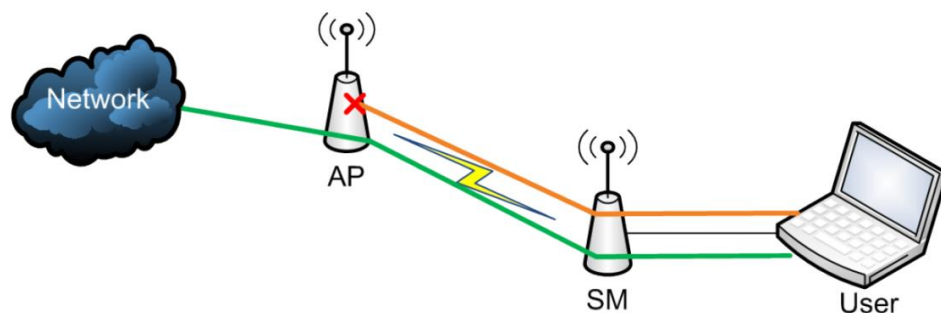
RF Telnet Access restricts Telnet access to the AP from a device situated below a network SM (downstream from the AP). This is a security enhancement to restrict RF-interface sourced AP access specifically to the LAN1 IP address and LAN2 IP address (Radio Private Address, typically 192.168.101. [LUID]). This restriction disallows unauthorized users from running Telnet commands on the AP that can change AP configuration or modifying network-critical components such as routing and ARP tables.

The RF Telnet Access may be configured via the AP GUI or via SNMP commands, and RF Telnet Access is set to “Enabled” by default. Once RF Telnet Access is set to “Disabled”, if there is a Telnet session attempt to the AP originating from a device situated below the SM (or any downstream device), the attempt is dropped. This also includes Telnet session attempts originated from the SM’s management interface (if a user has initiated a Telnet session to a SM and attempts to Telnet from the SM to the AP). In addition, if there are any active Telnet connections to the AP originating from a device situated below the SM (or any downstream device), the connection is dropped. This behavior must be considered if system administrators use Telnet downstream from an AP (from a registered SM) to modify system parameters.

Setting RF Telnet Access to “Disabled” does not affect devices situated above the AP from accessing the AP via Telnet, including servers running the CNUT (Canopy Network Updater tool) application. Also, setting RF Telnet Access to “Disabled” does not affect any Telnet access into upstream devices (situated above or adjacent to the AP) through the AP (see [Figure 126](#)).

The figure below depicts a user attempting two telnet sessions. One is targeted for the AP (orange) and one is targeted for the network upstream from the AP (green). If RF Telnet Access is set to “Disabled” (factory default setting), the Telnet attempt from the user to the AP is blocked, but the attempt from the user to Network is allowed to pass through the Cambium network.

Figure 126 RF Telnet Access Restrictions (orange) and Flow through (green)



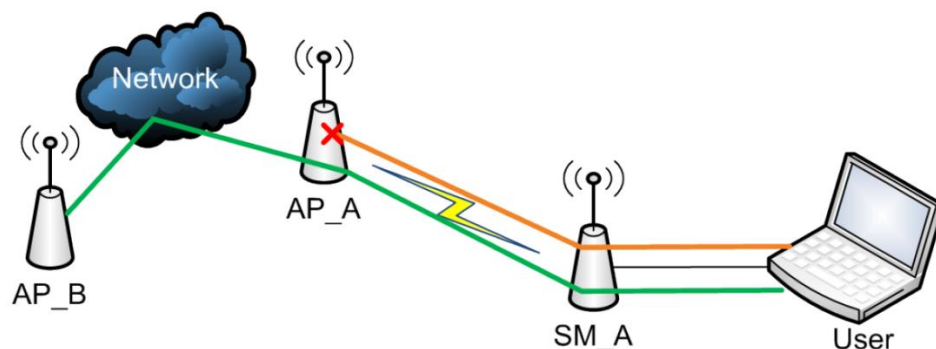
Key Security Considerations when using the RF Telnet Access Feature

To ensure that the network is fully protected from unauthorized AP Telnet sessions, the following topics must be considered:

Securing AP Clusters

When working with a cluster of AP units, to eliminate potential security holes allowing Telnet access, ensure that the RF Telnet Access parameter is set to “Disabled” for every AP in the cluster. In addition, since users situated below the AP are able to pass Telnet sessions up through the SM and AP to the upstream network (while AP RF Telnet Access is set to “Disabled”), ensure that all CMM4 or other networking equipment is secured with strong passwords. Otherwise, users may Telnet to the CMM4 or other networking equipment, and subsequently access network APs (see [Figure 127](#)) via their Ethernet interfaces (since RF Telnet Access only prevents Telnet sessions originating from the AP’s wireless interface).

Figure 127 RF Telnet Access Restriction (orange) and Potential Security Hole (green)



As a common practice, AP administrator usernames and passwords must be secured with strong, non-default passwords.

Restricting AP RF Telnet Access

AP Telnet access via the RF interface may be configured in two ways – the AP GUI and SNMP.

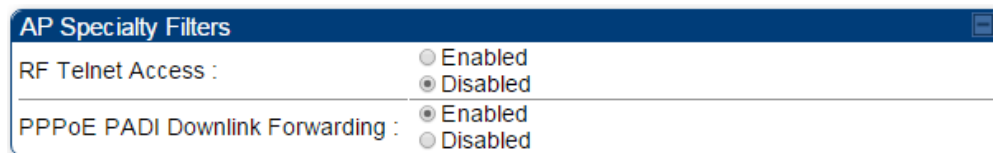
Controlling RF Telnet Access via the AP GUI

To restrict all Telnet access to the AP via the RF interface from downstream devices, follow these instructions using the AP GUI:

Procedure 20 Restricting RF Telnet access

- 1 Log into the AP GUI using administrator credentials
- 2 On the AP GUI, navigate to **Configuration > Protocol Filtering**

- 3 Under GUI heading “Telnet Access over RF Interface”, set **RF Telnet Access** to **Disabled**



AP Specialty Filters	
RF Telnet Access :	☐ Enabled ☒ Disabled
PPPoE PADI Downlink Forwarding :	☒ Enabled ☐ Disabled

- 4 Click the **Save** button
- 5 Once the **Save** button is clicked, all RF Telnet Access to the AP from devices situated below the AP is blocked.

**Note**

The factory default setting for RF Telnet Access is disabled and PPPoE PADI Downlink Forwarding is enabled.

Configuring SNMP Access

The SNMPv3 interface provides a more secure method to perform SNMP operations. This standard provides services for authentication, data integrity and message encryption over SNMP. Refer to [Planning for SNMPv3 operation](#) on page 3-38 for details.



Note

The factory default setting for SNMP is “SNMPv2c Only”.

Procedure 21 Configuring SNMPv3

- 1 Log into the AP GUI using administrator credentials
- 2 On the AP/SM GUI, navigate to **Configuration > Security Page**
- 3 Under GUI heading “Security Mode”, set **SNMP** to **SNMPv3 Only**

SNMP :	SNMPv2c Only ▼
Telnet :	SNMPv2c Only
	SNMPv3 Only
	SNMPv2c and SNMPv3

- 4 Click the **Save Changes** button
- 5 Go to **Configuration > SNMP Page**
- 6 Under GUI heading “SNMPv3 setting”, set **Engine ID**, **SNMPv3 Security Level**, **SNMPv3 Authentication Protocol**, **SNMPv3 Privacy Protocol**, **SNMPv3 Read-Only User**, **SNMPv3 Read/Write User**, **SNMPv3 Trap Configuration** parameters:

SNMPv3 Settings	
Engine ID :	800000a1030a003e47d1bc Use Default Engine ID
SNMPv3 Security Level :	noAuth,noPriv ▼
SNMPv3 Authentication Protocol :	md5 ▼
SNMPv3 Privacy Protocol :	cbc-des ▼
SNMPv3 Read-Only User :	Username Canopyro Authorization Key Privacy Key
SNMPv3 Read/Write User :	☐ Enable R/W User ☒ Disable R/W User Username Canopy Authorization Key Privacy Key
SNMPv3 Trap Configuration :	Disabled ▼

Engine ID :

Each radio (AP/SM/BHM/BHS) has a distinct SNMP authoritative engine identified by a unique Engine ID. While the Engine ID is configurable to the operator it is expected that the operator follow the guidelines of the SNMPEngineID defined in the SNMP-FRAMEWORK-MIB (RFC 3411). The default Engine ID is the MAC address of the device.

SNMPv3 security level, Authentication and Privacy Protocol

The authentication allows authentication of SNMPv3 user and privacy allows for encryption of SNMPv3 message. 450 Platform Family supports MD5 authentication and CBC-DES privacy protocols.

SNMPv3 Read-Only and Read/Write User

The user can be defined by configurable attributes. The attributes and default values are:

- Read-only user
 - Username = Canopyro
 - Authentication Password = authCanopyro
 - Privacy Password = privacyCanopyro
- Read-write user (by default read-write user is disabled)
 - Username = Canopy
 - Authentication Password = authCanopy
 - Privacy Password = privacyCanopy

SNMPv3 Trap Configuration

The traps may be sent from radios in SNMPv3 format based on parameter settings. It can be configured for Disabled, Enabled for Read-Only User, Enable for Read/Write User.

Configuring Security

Applicable products PMP : ☒ AP ☒ SM PTP: ☒ BHM ☒ BMS

Security page – 450 Platform Family AP/BHM

The security page of AP/BHM is explained in [Table 127](#).

Table 127 Security attributes –450 Platform Family AP

Authentication Server Settings	
Authentication Mode :	Disabled
Authentication Server DNS Usage :	☐ Append DNS Domain Name ☒ Disable DNS Domain Name
Authentication Server 1 :	Shared Secret 0.0.0.0
Authentication Server 2 :	Shared Secret 0.0.0.0
Authentication Server 3 :	Shared Secret 0.0.0.0
Authentication Server 4 (BAM ONLY) :	0.0.0.0
Authentication Server 5 (BAM ONLY) :	0.0.0.0
Radius Port :	1812 <i>Default port number is 1812</i>
Authentication Key :	(Using All 0xFF's Key)
Select Key :	☐ Use Key above ☒ Use Default Key
Dynamic Authorization Extensions for RADIUS :	☐ Enable CoA and Disconnect Message ☒ Disable CoA and Disconnect Message
Bypass Authentication for ICC SMS :	☐ Enabled ☒ Disabled

Airlink Security	
Encryption Setting :	None

AP Evaluation Configuration	
SM Display of AP Evaluation Data :	☐ Disable Display ☒ Enable Display

Session Timeout	
Web, Telnet, FTP Session Timeout :	600 Seconds

IP Access Filtering	
IP Access Control :	☐ IP Access Filtering Enabled - Only allow access from IP addresses specified below ☒ IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)

Security Mode	
Web Access :	HTTP Only
SNMP :	SNMPv2c Only
Telnet :	☒ Enabled ☐ Disabled
FTP :	☒ Enabled ☐ Disabled
TFTP :	☒ Enabled ☐ Disabled

Site Information	
Site Information Viewable to Guest Users :	☐ Enabled ☒ Disabled
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Security Banner	
Enable Security Banner during Login :	☐ Enabled ☒ Disabled
Security Banner Notice :	This is a sample of the text that can be put in this banner
User must accept security banner before login :	☒ Enabled ☐ Disabled

Attribute	Meaning
Authentication Mode	Operators may use this field to select from among the following authentication modes: Disabled—the AP/BHM requires no SMs/BHS to authenticate. (Factory default). Authentication Server —the AP/BHM requires any SM/BHS that attempts registration to be authenticated in Wireless Manager before registration. AP PreShared Key - The AP/BHM acts as the authentication server to its SMs/BHS and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP/BHM and all SMs/BHS desired to register to that AP/BHM. There is also an option of leaving the AP/BHM and SMs/BHS at their default setting of using the “Default Key”. Due to the nature of the authentication operation, if you want to set a specific authentication key, then you MUST configure the key on all of the SMs/BHS and reboot them BEFORE enabling the key and option on the AP/BHM. Otherwise, if you configure the AP/BHM first, none of the SMs/BHS is able to register. RADIUS AAA - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.

**Note**

This parameter is applicable to BHM.

Authentication Server DNS Usage	The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.  Note This parameter is applicable to BHM.
Authentication Server 1 to 5	Enter the IP address or server name of the authentication server (RADIUS or WM) and the Shared Secret configured in the authentication server. When Authentication Mode RADIUS AAA is selected, the default value of Shared Secret is “CanopySharedSecret”. The Shared Secret may consist of up to 32 ASCII characters.  Note This parameter is applicable to BHM.
Radius Port	This field allows the operator to configure a custom port for RADIUS server communication. The default value is <i>1812</i>.  Note This parameter is applicable to BHM.
Authentication Key	The authentication key is a 32-character hexadecimal string used when Authentication Mode is set to AP PreShared Key. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.  Note This parameter is applicable to BHM.
Select Key	This option allows operators to choose which authentication key is used: Use Key above means that the key specified in Authentication Key is used for authentication Use Default Key means that a default key (based off of the SM’s MAC address) is used for authentication  Note This parameter is applicable to BHM.
Dynamic Authorization Extensions for RADIUS	Enable CoA and Disconnect Message: Allows to control configuration parameters of SM using RADIUS CoA and Disconnect Message feature. Disable CoA and Disconnect Message: Disables RADIUS CoA and Disconnect Message feature. To enable CoA and Disconnect feature, the Authentication Mode should be set to RADIUS AAA.
Bypass Authentication for ICC SMs	Enabled: SM authentication is disabled when SM connects via ICC (Installation Color Code). Disabled: SM authentication is enabled.
Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs.

None provides no encryption on the air link.

DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system.

AES (Advanced Encryption Standard): An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.



Note

This parameter is applicable to BHM.

SM Display of AP
Evaluation Data
Or
BHS Display of BHM
Evaluation Data

Allows operators to suppress the display of data about this AP/BHM on the AP/BHM Evaluation tab of the Tools page in all SMs/BHS that register. The factory default setting for SM Display of AP Evaluation Data or BHS Display of BHM Evaluation Data is enabled display.

PMP 450/450i Series – SM display of AP Evaluation Data parameter

PTP 450/450i Series – BHS display of BHM Evaluation Data parameter

Web, Telnet, FTP
Session Timeout

Enter the expiry in seconds for remote management sessions via **HTTP**, **telnet**, or **ftp** access to the AP/BHM.

IP Access Control

You can permit access to the AP/BHM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address

Allowed Source IP 1
to 3

If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three.

If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • HTTP Only – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • HTTPS Only – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • HTTP and HTTPS – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • SNMPv2c Only – Enables SNMP v2 community protocol. • SNMPv3 Only – Enables SNMP v3 protocol. It is a secured communication protocol. • SNMPv2c and SNMPv3 – It enables both the protocols.
Telnet	This option allows to Enable and Disable Telnet access to the Radio.
FTP	This option allows to Enable and Disable FTP access to the Radio.
TFTP	This option allows to Enable and Disable TFTP access to the Radio.

Security page - 450 Platform Family SM

The security page of 450 Platform Family SM is explained in [Table 128](#).

Table 128 Security attributes –450 Platform Family SM

Authentication Key Settings Authentication Key : (Using All 0xFF's Key) Select Key : ☐ Use Key above ☒ Use Default Key
AAA Authentication Settings Enforce Authentication : Disable Phase 1 : eap/tls Phase 2 : MSCHAPv2 Identity/Realm : ☐ Enable Realm ☒ Disable Realm Identity anonymous @ Realm canopy.net Username : 0a-00-3e-a0-00-79 Use Default Username Password : ***** Confirm Password :
RADIUS Certificate Settings Upload Certificate File File: Choose File No file chosen Import Certificate Use Default Certificates <i>This will delete all current certificates</i>
Certificate 1 C =US S =Illinois O = Solutions, Inc. OU =Canopy Wireless Broadband CN =Canopy AAA Server Demo CA E =technical-support@canopywireless.com Valid From: 01/01/2001 00:00:00 Valid To: 12/31/2049 23:59:59 Delete
Certificate 2 C =US S =Illinois O = Inc. OU =Canopy Wireless Broadband CN =PMP320 Demo CA Valid From: 07/01/2009 06:00:00 Valid To: 12/31/2049 23:59:59 Delete

Airlink Security	
Encryption Setting :	DES ▼
Session Timeout	
Web, Telnet, FTP Session Timeout :	800000 Seconds
SM Management Interface Access via Ethernet Port	
Ethernet Access :	☒ Enabled ☐ Disabled
IP Access Filtering	
IP Access Control :	☐ IP Access Filtering Enabled - Only allow access from IP addresses specified below ☒ IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Security Mode	
Web Access :	HTTP Only ▼
SNMP :	SNMPv2c Only ▼
Telnet :	☒ Enabled ☐ Disabled
FTP :	☒ Enabled ☐ Disabled
TFTP :	☒ Enabled ☐ Disabled

Attribute	Meaning
Authentication Key	Only if the AP to which this SM will register requires authentication, specify the key that the SM will use when authenticating. For alpha characters in this hex key, use only upper case.
Select Key	The Use Default Key selection specifies the predetermined key for authentication in Wireless Manager The Use Key above selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the WM
Enforce Authentication	The SM may enforce authentication types of AAA and AP Pre-sharedKey . The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM locks out the AP for 15 minutes).
Phase 1	The protocols supported for the Phase 1 (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

Phase 2	Select the desired Phase 2 (Inside Identity) authentication protocol from the Phase 2 options of PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), and MSCHAP (Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.
Identity/Realm	If Realms are being used, select Enable Realm and configure an outer identity in the Identity field and a Realm in the Realm field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default Identity is "anonymous". The Identity can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default Realm is "canopy.net". The Realm can also be up to 128 non-special alphanumeric characters. Configure an outer Identity in the Username field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity Username is "anonymous". The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Username	Enter a Username for the SM. This must match the username configured for the SM on the RADIUS server. The default Username is the SM's MAC address. The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password	Enter the desired password for the SM in the Password and Confirm Password fields. The Password must match the password configured for the SM on the RADIUS server. The default Password is "password". The Password can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Upload Certificate File	To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a Delete button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on Choose File, browse to the location of the certificate, and click the Import Certificate button, and then reboot the radio to use the new certificate. When a certificate is in use, after the SM successfully registers to an AP, an indication of In Use will appear in the description block of the certificate being used. The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system. Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the Delete button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the Use Default Certificates button in the RADIUS Certificate Settings parameter block and reboot the radio.

Encryption Setting	Specify the type of airlink security to apply to this SM. The encryption setting must match the encryption setting of the AP. None provides no encryption on the air link. DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. AES (Advanced Encryption Standard): An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet, or FTP access to the SM.
Ethernet Access	If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select Ethernet Access Disabled. This selection disables access through this port to via HTTP (the GUI), SNMP, telnet, FTP, and TFTP. With this selection, management access is available through only the RF interface via either an IP address (if Network Accessibility is set to Public on the SM) or the Session Status or Remote Subscribers tab of the AP. Note This setting does not prevent a device connected to the Ethernet port from accessing the management interface of other SMs in the network. To prevent this, use the IP Access Filtering Enabled selection in the IP Access Control parameter of the SMs in the network. See IP Access Control below. If you want to allow management access through the Ethernet port, select Ethernet Access Enabled. This is the factory default setting for this parameter.
IP Access Control	You can permit access to the SM from any IP address (IP Access Filtering Disabled) or limit it to access from only one, two, or three IP addresses that you specify (IP Access Filtering Enabled). If you select IP Access Filtering Enabled, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted from any IP address
Allowed Source IP 1 to 3	If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the SM from any IP address. You may populate as many as all three.

	If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • HTTP Only – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • HTTPS Only – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • HTTP and HTTPS – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • SNMPv2c Only – Enables SNMP v2 community protocol. • SNMPv3 Only – Enables SNMP v3 protocol. It is secured communication protocol. • SNMPv2c and SNMPv3 – It enables both the protocols.
Telnet	This option allows to Enable and Disable Telnet access to the Radio.
FTP	This option allows to Enable and Disable FTP access to the Radio.
TFTP	This option allows to Enable and Disable TFTP access to the Radio.
Site Name	Specify a string to associate with the physical module.
Site Contact	Enter contact information for the module administrator.
Site Location	Enter information about the physical location of the module.
Enable Security Banner during Login	Enable: The Security Banner Notice will be displayed before login. Disable: The Security Banner Notice will not be displayed before login.
Security Banner Notice	User can enter ASCII (0-9a-zA-Z newline, line-feed are allowed) text up-to 1300 characters.
User must accept security banner before login	Enable: login area (username and password) will be disabled unless user accepts the security banner. Disable: User can't login to radio without accepting security banner.

Security page –450 Platform Family BHS

The Security page of 450 Platform Family BHS is explained in [Table 129](#).

Table 129 Security attributes - 450 Platform Family BHS

Authentication Key Settings			
Authentication Key :	(Using All 0xFF's Key)		
Airlink Security			
Encryption Setting :	DES ▼		
Session Timeout			
Web, Telnet, FTP Session Timeout :	600	Seconds	
IP Access Filtering			
IP Access Control :	☐ IP Access Filtering Enabled - Only allow access from IP addresses specified below ☒ IP Access Filtering Disabled - Allow access from all IP addresses		
Allowed Source IP 1 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Security Mode			
Web Access :	HTTP Only ▼		
SNMP :	SNMPv2c Only ▼		
Telnet :	☒ Enabled ☐ Disabled		
FTP :	☒ Enabled ☐ Disabled		
TFTP :	☒ Enabled ☐ Disabled		

Attribute	Meaning
Authentication Key	Only if the BHM to which this BHS registers requires an authentication, specify the key that the BHS will use when authenticating. For alpha characters in this hex key, use only upper case.
Encryption Setting	Specify the type of airlink security to apply to this BHS. The encryption setting must match the encryption setting of the BHM. None provides no encryption on the air link. DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. It is factory default setting. AES (Advanced Encryption Standard): An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.

Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet, or FTP access to the BHS.
IP Access Control	You can permit access to the BHS from any IP address (IP Access Filtering Disabled) or limit it to access from only one, two, or three IP addresses that you specify (IP Access Filtering Enabled). If you select IP Access Filtering Enabled , then you must populate at least one of the three Allowed Source IP parameters or have no access permitted from any IP address
Allowed Source IP 1 to 3	If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the BHS from any IP address. You may populate as many as all three. If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • HTTP Only – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • HTTPS Only – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • HTTP and HTTPS – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • SNMPv2c Only – Enables SNMP v2 community protocol. • SNMPv3 Only – Enables SNMP v3 protocol. It is secured communication protocol. • SNMPv2c and SNMPv3 – It enables both the protocols.
Telnet	This option allows to Enable and Disable Telnet access to the Radio.
FTP	This option allows to Enable and Disable FTP access to the Radio.
TFTP	This option allows to Enable and Disable TFTP access to the Radio.

Configuring radio parameters

- [PMP 450m Series – Configuring radio on page 7-125](#)
- [PMP/PTP 450i Series – configuring radio on page 7-125](#)
- [PMP/PTP 450 Series – configuring radio on page 7-147](#)
- [Custom Frequencies page on page 7-164](#)
- [DFS for 5 GHz Radios on page 7-167](#)
- [MIMO-A mode of operation on page 7-169](#)
- [Improved PPS performance of 450 Platform Family on page 7-171](#)

PMP 450m Series – Configuring radio

Radio page - PMP 450m AP 5 GHz

The **Radio** tab of the PMP 450m AP contains some of the configurable parameters that define how an AP operates.



Note

Only the frequencies available for your region and the selected Channel bandwidth are displayed.

Table 130 PMP 450m AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5520.0 ▾
Channel Bandwidth :	20 MHz ▾
Cyclic Prefix :	One Sixteenth
Color Code :	250 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	85 % (Range: 15 — 85 %)
Contention Slots :	2 (Range: 1 — 15)

Power Control	
EIRP :	22 dBm (Range: +22 — +37 dBm)
SM Receive Target Level :	-60 dBm (Range : -77 — -37 dBm) combined power

Advanced	
Receive Quality Debug :	☐ Enabled ☒ Disabled
Near Field Operation :	☐ Enabled ☒ Disabled

Attribute	Meaning
Frequency Band	Select the desired operating frequency band.
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is None . For a list of channels in the band, see the drop-down list on the radio GUI.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM. The supported Channel Bandwidth is 20 MHz.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multipathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Color Code	Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP <i>must</i> match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (<i>not</i> all 255 color codes).
Subscriber Color Code Rescan (When not on a Primary Color Code)	This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code. The time (in minutes) for a subscriber to rescan (if this AP is not configured with the SM's primary color code). This timer will only fire once – if the Subscriber Color Code Wait Period for Idle timer is configured with a nonzero value and the Subscriber Color Code Rescan expires, the Subscriber Color Code Wait Period for Idle is started. If the Subscriber Color Code Wait Period for Idle timer is configured with a zero value and the Subscriber Color Code Rescan timer expires, the SM will immediately go into rescan mode
Subscriber Color Code Wait Period for Idle	The time (in minutes) for a subscriber to rescan while idle (if this AP is not configured with the SM's primary color code). This timer will fire periodic events. The fired event determines if any RF unicast traffic (either inbound or outbound) has occurred since the last event. If the results of the event determine that no RF unicast traffic has occurred (SM is idle), then the subscriber will rescan.

Installation Color Code	With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. When using the Installation Color Code feature, ensure that the SM is configured with the factory default Color Code configuration (Color Code 1 is "0", Color Code 2-10 set to "0" and "Disable"). The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message "SM is registered via ICC – Bridging Disabled!" is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If a SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using Rescan APs functionality on the AP Eval page).
Max Range	Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which a SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance • does not increase the power of transmission from the AP. • can reduce aggregate throughput. <u>For example, with a 20 MHz channel and 2.5 ms frame, every additional 2.24 miles reduces the data air time by one symbol (around 1% of the frame).</u> Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. <u>The parameters have to be selected so that there is no overlap between one AP transmitting and another AP receiving. A co-location tool is provided to help with selecting sets of parameters that allow co-location.</u> If the AP is in cluster, then you must set this parameter on all other APs in the cluster exactly the same, except as described in the Downlink Data NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).
Downlink Data	Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 90 Mb, then 75% specified for this parameter allocates 67.5 Mb for the downlink and 22.5 Mb for the uplink. The default for this parameter is 75%. This parameter must be set in the range of 15% - 85%, otherwise the invalid input will not be accepted and the previously-entered valid setting is used.

	 Note In order to prevent self-interference, the frame configuration needs to align which includes Downlink Data, Max Range and Contention slots. For North America Region, the maximum Downlink % for a 5.4 GHz radio is 75% only.
Contention Slots (a.k.a. Control Slots)	This field indicates the number of (reserved) Contention slots configured by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page 7-168.
EIRP	This field indicates the combined power level at which the AP will transmit, based on the Country Code. It also includes the antenna gain and array gain.
SM Receive Target Level	Each SM's Transmitter Output Power is automatically set by the AP. The AP monitors the received power from each SM, and adjusts each SM's Transmitter Output Power so that the received power at the AP from that SM is not greater what is set in this field. This value represents the transmitted and received power (combined power) perceived on the SM.
Receive Quality Debug	To aid in link performance monitoring, the AP and SM now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM and 256-QAM) and per channel (polarization).
	 Note Due to CPU load, this will slightly degrade packet per second processing.
Near Field Operation	This parameter is enabled by the Near Field Operation control. This is only available when the EIRP is set to 22 dBm or below. When Near Field Operation is enabled, the Near Field Range is used to apply compensation to the unit's calibration to support operation in the near field.

PMP/PTP 450i Series – configuring radio

Radio page - PMP 450i AP 3 GHz

The **Radio** tab of the PMP 450i AP 3 GHz is shown in Figure 128.

Figure 128 PMP 450i AP Radio attributes - 3 GHz

Radio Configuration	
Frequency Band :	3.5 GHz ▾
Frequency Carrier :	3505.000 ▾
Channel Bandwidth :	10 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Color Code :	43 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Frame Configuration	
Max Range :	40 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	15 dBm (Range: -30 — +25 dBm) (12 dBm B / 12 dBm A)
External Gain :	0 dBi (Range: 0 — +70 dBi)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power
Adjacent Channel Support :	☐ Enabled ☒ Disabled

Multicast Data Control	
Multicast VC :	Disable ▾
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 6093 kbps)

Advanced																
MIMO Rate Adapt Algorithm :	MIMO-A/B ▾															
Control Messages :	☐ SISO ☒ MIMO-A															
Receive Quality Debug :	☐ Enabled ☒ Disabled															
	OFF ▾															
Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:																
Frame Alignment Legacy Mode :	<table border="1"> <thead> <tr> <th>Sync Src.\ SW Rev.</th> <th>13.4.1 or higher</th> <th>12.0 to 13.4 (DFS on)</th> <th>12.0 to 13.4 (DFS off)</th> <th>below 12.0</th> </tr> </thead> <tbody> <tr> <td>Timing Port</td> <td>OFF</td> <td>OFF</td> <td>OFF</td> <td>OFF</td> </tr> <tr> <td>Power Port</td> <td>OFF</td> <td>OFF</td> <td>ON (Mode 1)</td> <td>OFF</td> </tr> </tbody> </table>	Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0	Timing Port	OFF	OFF	OFF	OFF	Power Port	OFF	OFF	ON (Mode 1)	OFF
Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0												
Timing Port	OFF	OFF	OFF	OFF												
Power Port	OFF	OFF	ON (Mode 1)	OFF												

**Note**

Refer Table 132 PMP 450i SM Radio attributes – 5 GHz [on page 7-136](#) [for parameter details](#)

Radio page - PMP 450i AP 5 GHz

The **Radio** tab of the PMP 450i AP contains some of the configurable parameters that define how an AP operates.

**Note**

Only the frequencies available for your region and the selected Channel bandwidth are displayed.

Table 131 PMP 450i AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5480.0 ▾
Channel Bandwidth :	10 MHz ▾
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Cyclic Prefix :	One Sixteenth
Color Code :	0 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	0 dBm (Range: -30 — +27 dBm) (-3 dBm V / -3 dBm H)
External Gain :	11 dBi (Range: 0 — +40 dBi)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power

Multicast Data Control	
Multicast VC :	Disable ▾
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 6093 kbps)

Advanced

SM Registration :

☒ All (450i/450/430)
☐ 450i Only

PMP 430 SM Registration :

☒ Allow
☐ Deny

PMP 450/430 Legacy Mode :

☐ Enabled
☒ Disabled

Control Messages :

☐ SISO
☒ MIMO-A

PMP 430 Interop Mode :

☐ SISO
☒ MIMO-A

Receive Quality Debug :

☐ Enabled
☒ Disabled

OFF

Frame Alignment Legacy Mode :

Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0
Timing Port	OFF	OFF	OFF	OFF
Power Port	OFF	OFF	ON (Mode 1)	OFF

Attribute	Meaning
Frequency Band	See Table 130 PMP 450m AP Radio attributes - 5 GHz on page 7-125
Frequency Carrier	
Alternate Frequency Carrier 1 and 2	These parameters are displayed based on Regional Settings. Refer Country on page 7-73
Channel Bandwidth	
Cyclic Prefix	
Frame Period	
Color Code	
Subscriber Color Code Rescan (When not on a Primary Color Code)	See Table 130 PMP 450m AP Radio attributes - 5 GHz on page 7-125
Subscriber Color Code Wait Period for Idle	
Installation Color Code	
Max Range	
Downlink Data	See Table 130 PMP 450m AP Radio attributes - 5 GHz on page 7-125

Contention Slots (a.k.a. Control Slots)	This field indicates the number of (reserved) Contention slots configured by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page 7-168.
Broadcast Repeat Count	The default is 2 repeats (in addition to the original broadcast packet, for a total of 3 packets sent for every one needed), and is settable to 1 or 0 repeats (2 or 1 packets for every broadcast). ARQ (Automatic Repeat reQuest) is not present in downlink broadcast packets, since it can cause unnecessary uplink traffic from every SM for each broadcast packet. For successful transport without ARQ, the AP repeats downlink broadcast packets. The SMs filter out all repeated broadcast packets and, thus, do not transport further. The default of 2 repeats is optimum for typical uses of the network as an internet access system. In applications with heavy download broadcast such as video distribution, overall throughput is significantly improved by setting the repeat count to 1 or 0. This avoids flooding the downlink with repeat broadcast packets.
Transmitter Output Power	This value represents the combined power of the AP's two transmitters. Nations and regions may regulate transmitter output power. For example 900 MHz, 5.4 GHz and 5.8 GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. The professional installer of the equipment has the responsibility to - maintain awareness of applicable regulations. - calculate the permissible transmitter output power for the module. - confirm that the initial power setting is compliant with national or regional regulations. - confirm that the power setting is compliant following any reset of the module to factory defaults.
External Gain	This value needs to correspond to the published gain of the antenna used to ensure the radio will meet regulatory requirements.
SM Receive Target Level	See Table 130 PMP 450m AP Radio attributes - 5 GHz on page 7-125
Multicast VC Data Rate	This pull down menu of the Multicast Data Control screen helps in configuring multicast packets to be transmitted over a dedicated channel at a configurable rate of 1X, 2X, 4X or 6X. The default value is "Disable". If set to the default value, all multicast packets are transmitted over the Broadcast VC data path. This feature is available only for the PMP 450 Series and is not backward compatible with PMP 430 series of radios.

Multicast Repeat Count	This value is the number of packets that are repeated for every multicast VC packet received on the AP (located under Radio tab of Configuration). Multicast (like Broadcast) packets go over a VC that is shared by all SMs, so there is no guaranteed delivery. The repeat count is an attempt to improve the odds of the packets getting over the link. If the user has issues with packets getting dropped, they can use this parameter to improve the performance at the cost of the overall throughput possible on that channel. The default value is 0.
Multicast Downlink CIR	This value is the committed information rate for the multicast downlink VC (located under the Radio tab of Configuration). The default value is 0 kbps. The range of this parameter is based on the number of repeat counts. The higher the repeat count, the lower the range for the multicast downlink CIR.
SM Registration All	This field allows to control registration of all type 450 Platform Family SM including 430 Series SM(450i/450/430) or 450i Series SM only.
PMP 430 SM Registration	This field allows to control of PMP 430 SMs whether PMP 430 SMs are allowed to register to PMP 450i APs. By default, it is enabled and PMP 430 SM registrations are accepted. When this field is set to disabled, PMP 430 SM's registrations fail with reject reason 8. This will cause SMs to lock out the AP for 15 minutes.  Note This option is not displayed if the Frame Period is set to 5 ms. This option applies only to PMP 450/450i Series APs - 5 GHz.
Control Message	Controls whether the control messages are sent in MIMO-B or MIMO-A mode. MIMO-A is recommended. However, if an AP on 13.2 is attempting to connect to an SM on 13.1.3 or before, changing to MIMO-B may aid in getting the SM registered.
PMP 450/430 Legacy mode	Disabled: It is factory default setting. It allows to operate in 450i Series capabilities. Enabled: It allows to operate radio in Legacy mode PMP 450 or 430.
PMP 430 Interop Mode	For n-1 compatibility, In SISO mode this forces the AP to only send Control and Beacons over one of the RF paths.
Receive Quality Debug	To aid in link performance monitoring, the AP and SM now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM) and per channel (polarization).
	 Note Due to CPU load, this will slightly degrade packet per second processing.

Frame Alignment
Legacy Mode

Mode	Behavior (non-900 MHz radios)	Behavior (FSK 900 MHz radios)
OFF	By default frame start is aligned with devices with Timing Port synchronization If the synchronization source changes (due to Autosync or otherwise) the radio will dynamically adjust its frame start to maintain alignment with the default frame start timing	By default frame start is aligned with FSK 900 MHz devices with Timing Port synchronization If the synchronization source changes (due to Autosync or otherwise) the radio will dynamically adjust its frame start to maintain alignment with the default frame start timing
ON (Mode 1)	The radio will align with devices running software versions from 12.0 to 13.4.	The radio will align with FSK 900 MHz devices running software versions from 12.0 to 13.4.
ON (Mode 2)	N/A	The radio will align with FSK 900 MHz devices with software versions 11.2 or older.

Radio page - PMP 450i SM 3 GHz

The **Radio** tab of the PMP 450i SM 3 GHz is shown in Figure 129.

Figure 129 PMP 450i SM Radio attributes - 3 GHz

Radio Configuration

3.5/3.6 GHz

☒ 3302.500
 ☒ 3303.500
 ☐ 3305.000
 ☐ 3315.000
 ☐ 3325.000
 ☐ 3335.000
 ☐ 3345.000
 ☐ 3355.000
 ☐ 3365.000
 ☐ 3375.000
 ☐ 3385.000
 ☐ 3395.000
 ☐ 3405.000
 ☐ 3415.000
 ☐ 3425.000
 ☐ 3435.000
 ☐ 3445.000
 ☐ 3455.000
 ☐ 3465.000
 ☐ 3475.000
 ☐ 3485.000
 ☐ 3495.000
 ☐ 3500.000
 ☒ 3505.000
 ☐ 3515.000
 ☐ 3525.000
 ☐ 3535.000
 ☐ 3545.000
 ☐ 3552.500
 ☐ 3555.000
 ☐ 3565.000
 ☐ 3575.000
 ☐ 3585.000
 ☐ 3595.000
 ☐ 3600.000
 ☐ 3652.500
 ☐ 3675.000
 ☐ 3690.000
 ☐ 3847.500

5 MHz only

<=7 MHz

<= 10 MHz

<=15 MHz

<=20 MHz

Not available in this region

Select All

Clear All

Restore

Custom Radio Frequency Scan Selection List :

Channel Bandwidth Scan :

☐ 5 MHz
 ☐ 7 MHz
 ☒ 10 MHz
 ☐ 15 MHz
 ☐ 20 MHz
 ☐ 30 MHz

Cyclic Prefix Scan :

☒ One Sixteenth

AP Selection Method :

☐ Power Level
 ☒ Optimize for Throughput

Color Code 1 :

43

(0—254) / Priority

Primary

Installation Color Code :

☐ Enabled
 ☒ Disabled

Large VC data Q :

☐ Enabled
 ☒ Disabled

Additional Color Codes

Color Code :

0

(0—254) / Priority

Primary

Add/Modify Color Code

Remove Color Code

Additional Color Codes Table

No additional color codes configured

Power Control

External Gain :

17

dBi (Range: 0 — +70 dBi)

Advanced

Receive Quality Debug :

☐ Enabled
 ☒ Disabled



Note

Refer Table 132 PMP 450i SM Radio attributes – 5 GHz on page 7-136 for parameter details

Radio page – PMP 450i SM 5 GHz

The Radio page of PMP 450i SM is explained in [Table 132](#).

Table 132 PMP 450i SM Radio attributes – 5 GHz

Radio Configuration

4.9 GHz

No custom frequencies present.

5.1 GHz

☐ 5150.0
☐ 5152.5 ☐ 5155.0 ☐ 5157.5 ☐ 5160.0 ☐ 5162.5 ☐ 5165.0 ☐ 5167.5 ☐ 5170.0
☐ 5172.5 ☐ 5175.0 ☐ 5177.5 ☐ 5180.0 ☐ 5182.5 ☐ 5185.0 ☐ 5187.5 ☐ 5190.0
☐ 5192.5 ☐ 5195.0 ☐ 5197.5 ☐ 5200.0 ☐ 5202.5 ☐ 5205.0 ☐ 5207.5 ☐ 5210.0
☐ 5212.5 ☐ 5215.0 ☐ 5217.5 ☐ 5220.0 ☐ 5222.5 ☐ 5225.0 ☐ 5227.5 ☐ 5230.0
☐ 5232.5 ☐ 5235.0 ☐ 5237.5 ☐ 5240.0 ☐ 5242.5 ☐ 5245.0 ☐ 5247.5
☐ 5250.0

5.2 GHz

☐ 5250.0
☐ 5252.5 ☐ 5255.0 ☐ 5257.5 ☐ 5260.0 ☐ 5262.5 ☐ 5265.0 ☐ 5267.5 ☐ 5270.0
☐ 5272.5 ☐ 5275.0 ☐ 5277.5 ☐ 5280.0 ☐ 5282.5 ☐ 5285.0 ☐ 5287.5 ☐ 5290.0
☐ 5292.5 ☐ 5295.0 ☐ 5297.5 ☐ 5300.0 ☐ 5302.5 ☐ 5305.0 ☐ 5307.5 ☐ 5310.0
☐ 5312.5 ☐ 5315.0 ☐ 5317.5 ☐ 5320.0 ☐ 5322.5 ☐ 5325.0 ☐ 5327.5 ☐ 5330.0
☐ 5332.5 ☐ 5335.0 ☐ 5337.5 ☐ 5340.0 ☐ 5342.5 ☐ 5345.0 ☐ 5347.5
☐ 5350.0

5.4/5.7 GHz

☐ 5470.00
☐ 5472.50 ☐ 5475.00 ☐ 5477.50 ☐ 5480.00 ☐ 5482.50 ☐ 5485.00 ☐ 5487.50
☐ 5490.00 ☐ 5492.50 ☐ 5495.00 ☐ 5497.50 ☐ 5500.00 ☐ 5502.50 ☐ 5505.00
☐ 5507.50 ☐ 5510.00 ☐ 5512.50 ☐ 5515.00 ☐ 5517.50 ☐ 5520.00 ☐ 5522.50
☐ 5525.00 ☐ 5527.50 ☐ 5530.00 ☐ 5532.50 ☐ 5535.00 ☐ 5537.50 ☐ 5540.00
☐ 5542.50 ☐ 5545.00 ☐ 5547.50 ☐ 5550.00 ☐ 5552.50 ☐ 5555.00 ☐ 5557.50
☐ 5560.00 ☐ 5562.50 ☐ 5565.00 ☐ 5567.50 ☐ 5570.00 ☐ 5572.50 ☐ 5575.00
☐ 5577.50 ☐ 5580.00 ☐ 5582.50 ☐ 5585.00 ☐ 5587.50 ☐ 5590.00 ☐ 5592.50
☐ 5595.00 ☐ 5597.50 ☐ 5600.00 ☐ 5602.50 ☐ 5605.00 ☐ 5607.50 ☐ 5610.00
☐ 5612.50 ☐ 5615.00 ☐ 5617.50 ☐ 5620.00 ☐ 5622.50 ☐ 5625.00 ☐ 5627.50
☐ 5630.00 ☐ 5632.50 ☐ 5635.00 ☐ 5637.50 ☐ 5640.00 ☐ 5642.50 ☐ 5645.00
☐ 5647.50 ☐ 5650.00 ☐ 5652.50 ☐ 5655.00 ☐ 5657.50 ☐ 5660.00 ☐ 5662.50
☐ 5665.00 ☐ 5667.50 ☐ 5670.00 ☐ 5672.50 ☐ 5675.00 ☐ 5677.50 ☐ 5680.00
☐ 5682.50 ☐ 5685.00 ☐ 5687.50 ☐ 5690.00 ☐ 5692.50 ☐ 5695.00 ☐ 5697.50
☐ 5700.00 ☐ 5702.50 ☐ 5705.00 ☐ 5707.50 ☐ 5710.00 ☐ 5712.50 ☐ 5715.00
☐ 5717.50 ☐ 5720.00 ☐ 5722.50
☐ 5725.0
☐ 5725.0
☐ 5727.5 ☐ 5730.0 ☐ 5732.5 ☐ 5735.0 ☐ 5737.5 ☐ 5740.0 ☐ 5742.5 ☐ 5745.0
☐ 5747.5 ☐ 5750.0 ☐ 5752.5 ☐ 5755.0 ☐ 5757.5 ☐ 5760.0 ☐ 5762.5 ☐ 5765.0
☐ 5767.5 ☐ 5770.0 ☐ 5772.5 ☐ 5775.0 ☐ 5777.5 ☐ 5780.0 ☐ 5782.5 ☐ 5785.0
☐ 5787.5 ☐ 5790.0 ☐ 5792.5 ☐ 5795.0 ☐ 5797.5 ☐ 5800.0 ☐ 5802.5 ☐ 5805.0
☐ 5807.5 ☐ 5810.0 ☐ 5812.5 ☐ 5815.0 ☐ 5817.5 ☐ 5820.0 ☐ 5822.5 ☐ 5825.0
☐ 5827.5 ☐ 5830.0 ☐ 5832.5 ☐ 5835.0 ☐ 5837.5 ☐ 5840.0 ☐ 5842.5 ☐ 5845.0
☐ 5847.5 ☒ 5850.0 ☐ 5852.5 ☐ 5855.0 ☐ 5857.5 ☐ 5860.0 ☐ 5862.5 ☐ 5865.0
☐ 5867.5 ☐ 5870.0 ☐ 5872.5 ☐ 5875.0 ☐ 5877.5 ☐ 5880.0 ☐ 5882.5 ☐ 5885.0
☐ 5887.5 ☐ 5890.0 ☐ 5892.5 ☐ 5895.0 ☐ 5897.5 ☐ 5900.0 ☐ 5902.5 ☐ 5905.0
☐ 5907.5 ☐ 5910.0 ☐ 5912.5 ☐ 5915.0 ☐ 5917.5 ☐ 5920.0 ☐ 5922.5
☐ 5925.0

5 MHz only
☒ 7 MHz
☐ 10 MHz
☐ 15 MHz
☐ 20 MHz
☐ 30 MHz
 Not available in this region
 Bold only available with Engineering Key

Channel Bandwidth Scan :	☐ 5 MHz ☐ 7 MHz ☐ 10 MHz ☐ 15 MHz ☒ 20 MHz ☐ 30 MHz
Cyclic Prefix Scan :	☒ One Sixteenth
AP Selection Method :	☐ Power Level ☒ Optimize for Throughput
Color Code 1 :	14 (0—254) / Priority Primary
Installation Color Code :	☐ Enabled ☒ Disabled
Large VC data Q :	☐ Enabled ☒ Disabled

Additional Color Codes	
Color Code :	0 (0—254) / Priority Primary
Add/Modify Color Code Remove Color Code	

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-161.
Channel Bandwidth Scan	The channel size used by the radio for RF transmission.  Note Selecting multiple channel bandwidths will increase registration and re-registration times.
Cyclic Prefix Scan	The cyclic prefix for which AP scanning is executed.
AP Selection Method	Operators may configure the method by which a scanning SM selects an AP. By default, AP Selection Method is set to “Optimize for Throughput”, which has been the mode of operation in releases prior to 12.0.3.1. Power Level: AP selection based solely on power level <i>or</i> Optimize for Throughput: AP selection based on throughput optimization – the selection decision is based on power level (which affects the modulation state), channel bandwidth (which affects throughput) and number of SM registrations to the AP (which affects system contention performance).
Color Code 1	Color code allows you to force the SM to register to only a specific AP, even where the SM can communicate with multiple APs. For registration to occur, the color code of the SM and the AP <i>must</i> match. Specify a value from 0 to 254. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. The default setting for the color code value is 0. This value matches only the color code of 0 (<i>not</i> all 255 color codes).

	SMs may be configured with up to 20 color codes. These color codes can be tagged as Primary, Secondary, or Tertiary, or Disable. When the SM is scanning for APs, it will first attempt to register to an AP that matches one of the SM's primary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM's secondary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM's tertiary color codes. This is all done in the scanning mode of the SM and will repeat until a registration has occurred. Color codes in the same priority group are treated equally. For example, all APs matching one of the SM's primary color codes are analyzed equally. Likewise, this evaluation is done for the secondary and tertiary groups in order. The analysis for selecting an AP within a priority group is based on various inputs, including signal strength and number of SMs already registered to each AP. The first color code in the configuration is the pre-Release 9.5 color code. Thus, it is always a primary color code for legacy reasons. The color codes can be disabled, with the exception of the first color code.
Installation Color Code	With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. When using the Installation Color Code feature, ensure that the SM is configured with the factory default Color Code configuration (Color Code 1 is "0", Color Code 2-10 set to "0" and "Disable"). The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message "SM is registered via ICC – Bridging Disabled!" is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM.
External Gain	This value represents the antenna gain. For ODUs with integrated antenna, this is set at the correct value in the factory. For Connectorized ODUs with external antenna, the user must set this value to the overall antenna gain, including any RF cable loss between the ODU and the antenna.
Large VC data Queue	AP and BH have a configurable option used to prevent packet loss in the uplink due to bursting IP traffic. This is designed for IP burst traffic particular to video surveillance applications.
Receive Quality Debug	To aid in link performance monitoring, the AP and SM now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM) and per channel (polarization).

**Note**

Due to CPU load, this will slightly degrade packet per second processing.

**Note**

The frequencies that a user can select are controlled by the country or a region and the Channel Bandwidth selected. There can be a case where a user adds a custom frequency (from the [Custom Frequencies page](#) on page 7-164) and cannot see it in the pull down menu.

Radio page - PMP 450i AP 900 MHz

The Radio tab of the PMP 450i AP 900 MHz is described in below table [Table 133](#).

Table 133 PMP 450i AP Radio attributes - 900 MHz

Radio Configuration	
Frequency Carrier :	917.00 ▼
Channel Bandwidth :	10 MHz ▼
Cyclic Prefix :	One Sixteenth ▼
Frame Period :	☒ 5.0 ms ☐ 2.5 ms
Color Code :	85 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 120 miles)
Downlink Data :	50 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	25 dBm (Range: -30 — +25 dBm) (22 dBm B / 22 dBm A)
External Gain :	0 dB (Range: 0 — +40 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power

Multicast Data Control	
Multicast VC Data Rate :	Disable ▼
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 0 kbps)

Advanced													
Control Messages :	☐ SISO ☒ MIMO-A												
Receive Quality Debug :	☐ Enabled ☒ Disabled												
Pager Reject Filter :	☐ Enabled ☒ Disabled (NOTE: Frequencies 920 MHz and above will not work when enabled.)												
	OFF ▼												
Frame Alignment Legacy Mode :	Choose Legacy Mode setting from the table below based on colocated 900 MHz FSK's software revision and sync source: <table border="1"> <thead> <tr> <th>Sync Src.\ SW Rev.</th> <th>13.4.1 or higher</th> <th>12.0 to 13.4</th> <th>below 12.0</th> </tr> </thead> <tbody> <tr> <td>Timing Port</td> <td>OFF</td> <td>OFF</td> <td>OFF</td> </tr> <tr> <td>Power Port</td> <td>OFF</td> <td>ON (Mode 1)</td> <td>ON (Mode 2)</td> </tr> </tbody> </table>	Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4	below 12.0	Timing Port	OFF	OFF	OFF	Power Port	OFF	ON (Mode 1)	ON (Mode 2)
Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4	below 12.0										
Timing Port	OFF	OFF	OFF										
Power Port	OFF	ON (Mode 1)	ON (Mode 2)										

Attribute	Meaning
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is None . For a list of channels in the band, see the drop-down list on the radio GUI.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM. The supported Channel Bandwidths are 5, 7, 10 and 20 MHz.
Cyclic Prefix	See Table 130 PMP 450m AP Radio attributes - 5 GHz on page 7-125.
Frame Period	
Color Code	
Subscriber Color Code Rescan (When not on a Primary Color Code)	
Subscriber Color Code Wait Period for Idle	
Installation Color Code	
Max Range	
Downlink Data	
Contention Slots (a.k.a. Control Slots)	
Broadcast Repeat Count	
Transmitter Output Power	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
External Gain	See Table 130 PMP 450m AP Radio attributes - 5 GHz on page 7-125
SM Receive Target Level	
Multicast VC Data Rate	
Multicast Repeat Count	
Multicast Downlink CIR	
Control Message	
Receive Quality Debug	In 900 MHz, Pager Reject filter is placed on the AP to block Pager signals which could cause interference to the whole band. The Pager signals typically operate in the 928-930 frequency range. When the filter is enabled, the signals of 920 MHz and above are attenuated which enables better reception of signals in the rest of the band. Note that the AP/SM should not be configured on the frequencies of 920 MHz and above when this filter is enabled.
Pager Reject Filter	

Frame Alignment Legacy Mode	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
-----------------------------	---

Radio page - PTP 450i BHM 5 GHz

The **Radio** page of PTP 450i BHM is explained in [Table 134](#).

Table 134 PTP 450i BHM Radio page attributes – 5 GHz

Radio Configuration

Frequency Band :

5.4 GHz ▾

Frequency Carrier :

5490.0 ▾

Channel Bandwidth :

20 MHz ▾

Cyclic Prefix :

One Sixteenth ▾

Frame Period :

☐ 5.0 ms

☒ 2.5 ms

Color Code :

254 (0—254)

Large VC data Q :

☐ Enabled

☒ Disabled

Frame Configuration

Downlink Data :

75 % (Range: 15 — 85 %)

Power Control

Transmit Power :

-10 dBm (Range: -30 — +27 dBm) (-13 dBm V / -13 dBm H)

External Gain :

0 dB (Range: 0 — +40 dB)

Advanced

Receive Quality Debug :

☐ Enabled

☒ Disabled

OFF ▾

Frame Alignment Legacy Mode :

Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0
Timing Port	OFF	OFF	OFF	OFF
Power Port	OFF	OFF	ON (Mode 1)	OFF

Attribute	Meaning
Frequency Band	Select the operating frequency band of the radio. The supported bands are 4.9 GHz, 5.4 GHz and 5.7 GHz.
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is None . For a list of channels in the band, see the drop-down list on the radio GUI.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the BHM and the BHS.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Frame Period	Select the Frame Period of the radio. The support Frame Periods are : 5 ms and 2.5 ms.
Color Code	Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each link a different color code. Color code allows you to force a BHS to register to only a specific BHM. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes).
Large VC data Q	Enable Large VC Q for applications that burst data high rates. Large Qs may decrease effective throughput for TCP application. Disable Large VC Q if application need not handle bursts of data. Large Qs may decrease effective throughput for TCP application.
Downlink Data	Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the BHM to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the BHM is 132 Mbps, then 75% specified for this parameter allocates 99 Mbps for the downlink and 33 Mbps for the uplink. The default for this parameter is 50%. This parameter must be set in the range of 15% - 85%, otherwise the invalid input will not be accepted and the previously-entered valid setting is used.  Note In order to prevent self-interference, the frame configuration needs to align. This includes Downlink Data, Max Range and Contention slots.
Transmit Power	This value represents the combined power of the BHM's two transmitters. Nations and regions may regulate transmit power. For example

	• PTP 450i Series modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. The professional installer of the equipment has the responsibility to: • Maintain awareness of applicable regulations. • Calculate the permissible transmitter output power for the module. • Confirm that the initial power setting is compliant with national or regional regulations. Confirm that the power setting is compliant following any reset of the module to factory defaults.
External Gain	This value needs to correspond to the published gain of the antenna used to ensure the radio will meet regulatory requirements.
Receive Quality Debug	To aid in link performance monitoring, the BHM and BHS now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM and 256-QAM) and per channel (polarization).
	Note Due to CPU load, this slightly degrades the packet during per second processing.
Frame Alignment Legacy Mode	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130 .

Radio page – PTP 450i BHS 5 GHz

The Radio page of PTP 450i BHS is explained in [Table 135](#).

Table 135 PTP 450i BHS Radio attributes – 5 GHz

Radio Configuration

4.9 GHz

☒ 4909.000
 ☒ 4945.000
 ☒ 4950.000

5.1 GHz

☒ 5150.0
☐ 5152.5 ☐ 5155.0 ☐ 5157.5 ☐ 5160.0 ☐ 5162.5 ☐ 5165.0 ☐ 5167.5 ☐ 5170.0 ☐ 5172.5
☐ 5175.0 ☐ 5177.5 ☐ 5180.0 ☐ 5182.5 ☐ 5185.0 ☐ 5187.5 ☐ 5190.0 ☐ 5192.5 ☐ 5195.0
☐ 5197.5 ☐ 5200.0 ☐ 5202.5 ☐ 5205.0 ☐ 5207.5 ☐ 5210.0 ☐ 5212.5 ☐ 5215.0 ☐ 5217.5
☐ 5220.0 ☐ 5222.5 ☐ 5225.0 ☐ 5227.5 ☐ 5230.0 ☐ 5232.5 ☐ 5235.0 ☐ 5237.5 ☐ 5240.0
☐ 5242.5 ☐ 5245.0 ☐ 5247.5
☒ 5250.0

5.2 GHz

☒ 5250.0
☐ 5252.5 ☐ 5255.0 ☐ 5257.5 ☐ 5260.0 ☐ 5262.5 ☐ 5265.0 ☐ 5267.5 ☐ 5270.0 ☐ 5272.5
☐ 5275.0 ☐ 5277.5 ☐ 5280.0 ☐ 5282.5 ☐ 5285.0 ☐ 5287.5 ☐ 5290.0 ☐ 5292.5 ☐ 5295.0
☐ 5297.5 ☐ 5300.0 ☐ 5302.5 ☐ 5305.0 ☐ 5307.5 ☐ 5310.0 ☐ 5312.5 ☐ 5315.0 ☐ 5317.5
☐ 5320.0 ☐ 5322.5 ☐ 5325.0 ☐ 5327.5 ☐ 5330.0 ☐ 5332.5 ☐ 5335.0 ☐ 5337.5 ☐ 5340.0
☐ 5342.5 ☐ 5345.0 ☐ 5347.5
☒ 5350.0

5.4/5.7 GHz

☒ 5470.00
☐ 5472.50 ☐ 5475.00 ☐ 5477.50 ☐ 5480.00 ☐ 5482.50 ☐ 5485.00 ☐ 5487.50 ☐ 5490.00
☐ 5492.50 ☐ 5495.00 ☐ 5497.50 ☐ 5500.00 ☐ 5502.50 ☐ 5505.00 ☐ 5507.50 ☐ 5510.00
☐ 5512.50 ☐ 5515.00 ☐ 5517.50 ☐ 5520.00 ☐ 5522.50 ☐ 5525.00 ☐ 5527.50 ☐ 5530.00
☐ 5532.50 ☐ 5535.00 ☐ 5537.50 ☐ 5540.00 ☐ 5542.50 ☐ 5545.00 ☐ 5547.50 ☐ 5550.00
☐ 5552.50 ☐ 5555.00 ☐ 5557.50 ☐ 5560.00 ☐ 5562.50 ☐ 5565.00 ☐ 5567.50 ☐ 5570.00
☐ 5572.50 ☐ 5575.00 ☐ 5577.50 ☐ 5580.00 ☐ 5582.50 ☐ 5585.00 ☐ 5587.50 ☒ 5590.00
☐ 5592.50 ☐ 5595.00 ☐ 5597.50 ☐ 5600.00 ☐ 5602.50 ☐ 5605.00 ☐ 5607.50 ☐ 5610.00
☐ 5612.50 ☐ 5615.00 ☐ 5617.50 ☐ 5620.00 ☐ 5622.50 ☐ 5625.00 ☐ 5627.50 ☐ 5630.00
☐ 5632.50 ☐ 5635.00 ☐ 5637.50 ☐ 5640.00 ☐ 5642.50 ☐ 5645.00 ☐ 5647.50 ☐ 5650.00
☐ 5652.50 ☐ 5655.00 ☐ 5657.50 ☐ 5660.00 ☐ 5662.50 ☐ 5665.00 ☐ 5667.50 ☐ 5670.00
☐ 5672.50 ☐ 5675.00 ☐ 5677.50 ☐ 5680.00 ☐ 5682.50 ☐ 5685.00 ☐ 5687.50 ☐ 5690.00
☐ 5692.50 ☐ 5695.00 ☐ 5697.50 ☐ 5700.00 ☐ 5702.50 ☐ 5705.00 ☐ 5707.50 ☐ 5710.00
☐ 5712.50 ☐ 5715.00 ☐ 5717.50 ☐ 5720.00 ☐ 5722.50
☒ 5725.0
☐ 5727.5 ☐ 5730.0 ☐ 5732.5 ☐ 5735.0 ☐ 5737.5 ☐ 5740.0 ☐ 5742.5 ☐ 5745.0 ☐ 5747.5
☐ 5750.0 ☐ 5752.5 ☐ 5755.0 ☐ 5757.5 ☐ 5760.0 ☐ 5762.5 ☐ 5765.0 ☐ 5767.5 ☐ 5770.0
☐ 5772.5 ☐ 5775.0 ☐ 5777.5 ☐ 5780.0 ☐ 5782.5 ☐ 5785.0 ☐ 5787.5 ☐ 5790.0 ☐ 5792.5
☐ 5795.0 ☐ 5797.5 ☐ 5800.0 ☐ 5802.5 ☐ 5805.0 ☐ 5807.5 ☐ 5810.0 ☐ 5812.5 ☐ 5815.0
☐ 5817.5 ☐ 5820.0 ☐ 5822.5 ☐ 5825.0 ☐ 5827.5 ☐ 5830.0 ☐ 5832.5 ☐ 5835.0 ☐ 5837.5
☐ 5840.0 ☐ 5842.5 ☐ 5845.0 ☐ 5847.5 ☐ 5850.0 ☐ 5852.5 ☐ 5855.0 ☐ 5857.5 ☐ 5860.0
☐ 5862.5 ☐ 5865.0 ☐ 5867.5 ☐ 5870.0 ☐ 5872.5 ☐ 5875.0 ☐ 5877.5 ☐ 5880.0 ☐ 5882.5
☐ 5885.0 ☐ 5887.5 ☐ 5890.0 ☐ 5892.5 ☐ 5895.0 ☐ 5897.5 ☐ 5900.0 ☐ 5902.5 ☐ 5905.0
☐ 5907.5 ☐ 5910.0 ☐ 5912.5 ☐ 5915.0 ☐ 5917.5 ☐ 5920.0 ☐ 5922.5
☒ 5925.0

5 MHz only

☒ 7 MHz
☐ 10 MHz
☐ 15 MHz
☐ 20 MHz
☐ 30 MHz

Not available in this region

Bold only available with Engineering Key

Custom Radio Frequency Scan Selection List :

Channel Bandwidth Scan :	☒ 5 MHz ☐ 7 MHz ☐ 10 MHz ☐ 15 MHz ☐ 20 MHz ☐ 30 MHz
Cyclic Prefix Scan :	☒ One Sixteenth
Color Code :	248 (0—254)
Large VC data Q :	☐ Enabled ☒ Disabled

Power Control	
Transmit Power :	4 dBm (Range: -30 — +27 dBm) (1 dBm V / 1 dBm H)
External Gain :	0 dBi (Range: 0 — +40 dBi)

Advanced	
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check any frequency that you want the BHS to scan for BHM transmissions. See Radio Frequency Scan Selection List on page 7-161.
Channel Bandwidth Scan	The channel size used by the radio for RF transmission.  Note Selecting multiple channel bandwidths will increase registration and re-registration times.
Cyclic Prefix Scan	The cyclic prefix for which BHM scanning is executed.
Color Code	Color code allows to force the BHS to register to only a specific BHM, even where the BHS can communicate with multiple BHMs. For registration to occur, the color code of the BHS and the BHM <i>must</i> match. Specify a value from 0 to 254. The color codes can be disabled, with the exception of the first color code.
Large VC data Q	BHM and BHS have a configurable option used to prevent packet loss in the uplink due to bursting IP traffic. This is designed for IP burst traffic particular to video surveillance applications.
Transmit Power	Refer Table 134 PTP 450i BHM Radio page attributes – 5 GHz on page 7-142
External Gain	
Receive Quality Debug	

PMP/PTP 450 Series – configuring radio

Radio page - PMP 450 AP 5 GHz

The **Radio** tab of the AP for 5 GHz is as shown in [Table 136](#).

Table 136 PMP 450 AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5480.0 ▾
Channel Bandwidth :	20 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Color Code :	5 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☒ Enabled ☐ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range: 0 — 2)

Power Control	
Transmit Power :	16 dBm (Range: -30 — +22 dBm) (13 dBm V / 13 dBm H)
External Gain :	0 dB (Range: 0 — +40 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power

Multicast Data Control	
Multicast VC Data Rate :	Disable ▾
Multicast Repeat Count :	0 (Range: 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 0 kbps)

Advanced																
PMP 430 SM Registration :	☒ Allow ☐ Deny															
Control Messages :	☐ SISO ☒ MIMO-A															
PMP 430 Interop Mode :	☐ SISO ☒ MIMO-A															
Receive Quality Debug :	☐ Enabled ☒ Disabled															
	OFF ▾															
Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:																
Frame Alignment Legacy Mode :	<table border="1"> <thead> <tr> <th>Sync Src.\ SW Rev.</th> <th>13.4.1 or higher</th> <th>12.0 to 13.4 (DFS on)</th> <th>12.0 to 13.4 (DFS off)</th> <th>below 12.0</th> </tr> </thead> <tbody> <tr> <td>Timing Port</td> <td>OFF</td> <td>OFF</td> <td>OFF</td> <td>OFF</td> </tr> <tr> <td>Power Port</td> <td>OFF</td> <td>OFF</td> <td>ON (Mode 1)</td> <td>OFF</td> </tr> </tbody> </table>	Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0	Timing Port	OFF	OFF	OFF	OFF	Power Port	OFF	OFF	ON (Mode 1)	OFF
Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0												
Timing Port	OFF	OFF	OFF	OFF												
Power Port	OFF	OFF	ON (Mode 1)	OFF												

Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
PMP 430 SM Registration	
PMP 450/430 Legacy Mode	
Control Messages	
PMP 430 Interop Mode	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
Receive Quality Debug	
Frame Alignment Legacy Mode	

Radio page - PMP 450 AP 3.65 GHz

Table 137 PMP 450 AP Radio attributes - 3.65 GHz

Radio Configuration	
Frequency Carrier :	3650.000 ▼
Channel Bandwidth :	20 MHz ▼
Cyclic Prefix :	One Sixteenth ▼
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Color Code :	5 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	25 dBm (Range: -30 — +25 dBm) (22 dBm A / 22 dBm B)
External Gain :	0 dB (Range: 0 — +70 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power
Adjacent Channel Support :	☐ Enabled ☒ Disabled

Multicast Data Control	
Multicast VC Data Rate :	Disable ▼
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 0 kbps)

Advanced	
Control Messages :	☐ SISO ☒ MIMO-A
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.

Radio page - PMP 450 AP 3.5 GHz

Table 138 PMP 450 AP Radio attributes - 3.5 GHz

Radio Configuration	
Frequency Carrier :	3590.001 ▼
Channel Bandwidth :	10 MHz ▼
Cyclic Prefix :	One Sixteenth ▼
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Color Code :	35 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	1 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	85 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	25 dBm (Range: -30 — +25 dBm) (22 dBm A / 22 dBm B)
External Gain :	0 dB (Range: 0 — +70 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power
Adjacent Channel Support :	☐ Enabled ☒ Disabled

Multicast Data Control	
Multicast VC Data Rate :	Disable ▼
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 0 kbps)

Advanced	
Control Messages :	☐ SISO ☒ MIMO-A
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute

Meaning

Radio Configuration,
 Frame Configuration,
 Power Control,
 Multicast Data Control
 and Advance tab

See [Table 131 PMP 450i AP Radio attributes - 5 GHz](#) on page 7-130.

Radio page - PMP 450 AP 2.4 GHz

Table 139 PMP 450 AP Radio attributes - 2.4 GHz

Radio Configuration	
Frequency Carrier :	2440.0 ▼
Channel Bandwidth :	20 MHz ▼
Cyclic Prefix :	One Sixteenth ▼
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Color Code :	24 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☒ Enabled ☐ Disabled

Frame Configuration	
Max Range :	30 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	22 dBm (Range: -30 — +22 dBm) (19 dBm A / 19 dBm B)
External Gain :	35 dB (Range: 0 — +35 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power

Multicast Data Control	
Multicast VC Data Rate :	Disable ▼
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 0 kbps)

Advanced	
Control Messages :	☐ SISO ☒ MIMO-A
Receive Quality Debug :	☒ Enabled ☐ Disabled

Attribute	Meaning
-----------	---------

Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
---	---

Radio page - PMP 450 SM 5 GHz

Table 140 PMP 450 SM Radio attributes – 5 GHz

Radio Configuration	
5.4 GHz	
☐ 5472.5 ☐ 5475.0 ☐ 5477.5 ☐ 5480.0 ☐ 5482.5 ☐ 5485.0 ☐ 5487.5 ☐ 5490.0 ☐ 5492.5 ☐ 5495.0 ☐ 5497.5 ☐ 5500.0 ☐ 5502.5 ☐ 5505.0 ☐ 5507.5 ☐ 5510.0 ☐ 5512.5 ☐ 5515.0 ☐ 5517.5 ☐ 5520.0 ☐ 5522.5 ☐ 5525.0 ☐ 5527.5 ☐ 5530.0 ☐ 5532.5 ☐ 5535.0 ☐ 5537.5 ☐ 5540.0 ☐ 5542.5 ☐ 5545.0 ☐ 5547.5 ☐ 5550.0 ☐ 5552.5 ☐ 5555.0 ☐ 5557.5 ☐ 5560.0 ☐ 5562.5 ☐ 5565.0 ☐ 5567.5 ☐ 5570.0 ☐ 5572.5 ☐ 5575.0 ☐ 5577.5 ☐ 5580.0 ☐ 5582.5 ☐ 5585.0 ☐ 5587.5 ☐ 5590.0 ☐ 5592.5 ☐ 5595.0 ☐ 5597.5 ☐ 5600.0 ☐ 5602.5 ☐ 5605.0 ☐ 5607.5 ☐ 5610.0 ☐ 5612.5 ☐ 5615.0 ☐ 5617.5 ☐ 5620.0 ☐ 5622.5 ☐ 5625.0 ☐ 5627.5 ☐ 5630.0 ☐ 5632.5 ☐ 5635.0 ☐ 5637.5 ☐ 5640.0 ☐ 5642.5 ☐ 5645.0 ☐ 5647.5 ☐ 5650.0 ☐ 5652.5 ☐ 5655.0 ☐ 5657.5 ☐ 5660.0 ☐ 5662.5 ☐ 5665.0 ☐ 5667.5 ☐ 5670.0 ☐ 5672.5 ☐ 5675.0 ☐ 5677.5 ☐ 5680.0 ☐ 5682.5 ☐ 5685.0 ☐ 5687.5 ☐ 5690.0 ☐ 5692.5 ☐ 5695.0 ☐ 5697.5 ☐ 5700.0 ☐ 5702.5 ☐ 5705.0 ☐ 5707.5 ☐ 5710.0 ☐ 5712.5 ☐ 5715.0 ☐ 5717.5 ☐ 5720.0 ☐ 5722.5	
Custom Radio Frequency Scan Selection List :	
5.7 GHz	
☐ 5727.5 ☐ 5730.0 ☐ 5732.5 ☐ 5735.0 ☐ 5737.5 ☐ 5740.0 ☐ 5742.5 ☐ 5745.0 ☐ 5747.5 ☐ 5750.0 ☐ 5752.5 ☐ 5755.0 ☐ 5757.5 ☒ 5760.0 ☐ 5762.5 ☐ 5765.0 ☐ 5767.5 ☐ 5770.0 ☐ 5772.5 ☐ 5775.0 ☐ 5777.5 ☐ 5780.0 ☐ 5782.5 ☐ 5785.0 ☐ 5787.5 ☐ 5790.0 ☐ 5792.5 ☐ 5795.0 ☐ 5797.5 ☐ 5800.0 ☐ 5802.5 ☐ 5805.0 ☐ 5807.5 ☐ 5810.0 ☐ 5812.5 ☐ 5815.0 ☐ 5817.5 ☐ 5820.0 ☐ 5822.5 ☐ 5825.0 ☐ 5827.5 ☐ 5830.0 ☐ 5832.5 ☐ 5835.0 ☐ 5837.5 ☐ 5840.0 ☐ 5842.5 ☐ 5845.0 ☐ 5847.5 ☐ 5850.0 ☐ 5852.5 ☐ 5855.0 ☐ 5857.5 ☐ 5860.0 ☐ 5862.5 ☐ 5865.0 ☐ 5867.5 ☐ 5870.0 ☐ 5872.5 ☐ 5875.0 ☐ 5877.5 ☐ 5880.0 ☐ 5882.5 ☐ 5885.0 ☐ 5887.5 ☐ 5890.0 ☐ 5892.5 ☐ 5895.0 ☐ 5897.5	
5 MHz only ☐ 10 MHz ☒ 15 MHz ☐ 20 MHz FCC TDWR Band Not available in this region	
Select All Select All 5.4 Select All 5.7 Clear All Restore	
Channel Bandwidth Scan :	☐ 5 MHz ☐ 10 MHz ☐ 15 MHz ☒ 20 MHz ☐ 30 MHz
Cyclic Prefix :	One Sixteenth
AP Selection Method :	☐ Power Level ☒ Optimize for Throughput
Color Code 1 :	87 (0—254) / Priority Primary
Installation Color Code :	☒ Enabled ☐ Disabled
Large VC data Q :	☐ Enabled ☒ Disabled
Additional Color Codes	
Color Code : 0 (0—254) / Priority Primary Add/Modify Color Code Remove Color Code	
Additional Color Codes Table	
Color Code	Priority
0	Primary
Power Control	
External Gain :	0 dBi (Range: 0 — +40 dBi)
Advanced	
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-161.
See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.	

Radio page - PMP 450 SM 3.65 GHz

Table 141 PMP 450 SM Radio attributes – 3.65 GHz

Radio Configuration		
Custom Radio Frequency Scan Selection List :	☐ 3502.500 ☐ 3503.500 ☐ 3505.000 ☐ 3507.500 ☐ 3510.000 ☐ 3515.000 ☐ 3552.500 ☐ 3553.500 ☐ 3555.000 ☐ 3557.500 ☐ 3560.000 ☐ 3565.000 ☒ 3600.000 ☒ 3602.500 ☒ 3603.500 ☒ 3605.000 ☒ 3607.500 ☒ 3610.000 ☒ 3615.000 ☒ 3640.000 ☒ 3642.500 ☒ 3645.000 ☒ 3646.500 ☒ 3647.500 ☒ 3650.000 ☒ 3650.010 ☒ 3652.500 ☒ 3653.000 ☒ 3653.500 ☒ 3655.000 ☒ 3657.000 ☒ 3657.500 ☒ 3660.000 ☒ 3675.000 ☒ 3690.000 ☒ 3692.000 ☐ 3692.500 ☐ 3695.000 ☐ 3696.000 ☐ 3696.500 ☐ 3697.000 ☐ 3697.500 ☐ 3700.000 ☐ 3735.000 ☐ 3740.000 ☐ 3742.500 ☐ 3745.000 ☐ 3746.500 ☐ 3747.500 ☐ 3750.000 ☒ 3785.000 ☒ 3790.000 ☒ 3792.500 ☒ 3795.000 ☒ 3796.500 ☒ 3797.500 ☐ 3800.000	
	5 MHz only <= 7 MHz <= 10 MHz <= 15 MHz <= 20 MHz Not available in this region Select All Clear All Restore	
	Channel Bandwidth Scan :	☒ 5 MHz ☐ 7 MHz ☐ 10 MHz ☐ 15 MHz ☐ 20 MHz ☐ 30 MHz
	Cyclic Prefix Scan :	☒ One Sixteenth
	AP Selection Method :	☐ Power Level ☒ Optimize for Throughput
	Color Code 1 :	0 (0—254) / Priority Primary ▼
	Installation Color Code :	☒ Enabled ☐ Disabled
	Large VC data Q :	☐ Enabled ☒ Disabled
	Additional Color Codes	
	Color Code :	0 (0—254) / Priority Primary ▼ Add/Modify Color Code Remove Color Code
	Additional Color Codes Table	
	No additional color codes configured	
	Power Control	
	External Gain :	0 dBi (Range: 0 — +70 dBi)
	Advanced	
	Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-161.

See [Table 131 PMP 450i AP Radio attributes - 5 GHz](#) on page 7-130.

Radio page - PMP 450 SM 3.5 GHz

Table 142 PMP 450 SM Radio attributes – 3.5 GHz

Radio Configuration	
	☐ 3302.500 ☒ 3303.500 ☒ 3352.000 ☐ 3352.500 ☐ 3397.500 ☐ 3403.500 ☐ 3450.000 ☐ 3500.000 ☐ 3502.500
Custom Radio Frequency Scan Selection List :	5 MHz only <=7 MHz <= 10 MHz <=15 MHz <=20 MHz <=30 MHz Not available in this region Bold only available with Engineering Key Select All Clear All Restore
Channel Bandwidth Scan :	☒ 5 MHz ☐ 7 MHz ☐ 10 MHz ☐ 15 MHz ☐ 20 MHz ☐ 30 MHz
Cyclic Prefix Scan :	☒ One Sixteenth
AP Selection Method :	☐ Power Level ☒ Optimize for Throughput
Color Code 1 :	0 (0—254) / Priority Primary
Installation Color Code :	☒ Enabled ☐ Disabled
Large VC data Q :	☐ Enabled ☒ Disabled

Additional Color Codes	
Color Code :	0 (0—254) / Priority Primary
Add/Modify Color Code Remove Color Code	

Additional Color Codes Table	
No additional color codes configured	

Power Control	
External Gain :	0 dBi (Range: 0 — +70 dBi)

Advanced	
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-161.

See [Table 131 PMP 450i AP Radio attributes - 5 GHz](#) on page 7-130.

Radio page - PMP 450 SM 2.4 GHz

Table 143 PMP 450 SM Radio attributes – 2.4 GHz

Radio Configuration	
Custom Radio Frequency Scan Selection List :	☐ 2400.0 ☐ 2402.5 ☐ 2405.0 ☐ 2407.5 ☐ 2410.0 ☐ 2412.5 ☐ 2415.0 ☐ 2417.5 ☒ 2420.0 ☐ 2422.5 ☐ 2425.0 ☐ 2427.5 ☐ 2430.0 ☐ 2432.5 ☐ 2435.0 ☐ 2437.5 ☐ 2440.0 ☐ 2442.5 ☐ 2445.0 ☐ 2447.5 ☐ 2450.0 ☐ 2452.5 ☐ 2455.0 ☐ 2457.5 ☐ 2460.0 ☐ 2462.5 ☐ 2465.0 ☐ 2467.5 ☐ 2470.0 ☐ 2472.5 ☐ 2475.0 ☐ 2477.5 ☐ 2480.0 ☐ 2482.5 ☐ 5 MHz only ☐ <= 7/10 MHz ☐ <= 15 MHz ☐ <= 20 MHz ☐ <= 30 MHz Not available in this region Bold only available with Engineering Key Select All Clear All Restore
Channel Bandwidth Scan :	☐ 5 MHz ☐ 7 MHz ☐ 10 MHz ☐ 15 MHz ☒ 20 MHz ☐ 30 MHz
Cyclic Prefix Scan :	One Sixteenth
AP Selection Method :	☐ Power Level ☒ Optimize for Throughput
Color Code 1 :	152 (0—254) / Priority Primary ▼
Installation Color Code :	☒ Enabled ☐ Disabled
Large VC data Q :	☐ Enabled ☒ Disabled
Additional Color Codes	
Color Code :	0 (0—254) / Priority Primary ▼ Add/Modify Color Code Remove Color Code
Additional Color Codes Table	
No additional color codes configured	
Power Control	
External Gain :	0 dBi (Range: 0 — +40 dBi)
Advanced	
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-161.

See [Table 131 PMP 450i AP Radio attributes - 5 GHz](#) on page 7-130.

Radio page - PMP 450 SM 900 MHz

Table 144 PMP 450 SM Radio attributes –900 MHz

Radio Configuration	
	☐ 904.50 ☐ 905.00 ☒ 905.50 ☒ 906.00 ☒ 906.50 ☐ 907.00 ☐ 907.50 ☐ 908.00 ☐ 908.50 ☐ 909.00 ☐ 909.50 ☐ 910.00 ☐ 910.50 ☐ 911.00 ☐ 911.50 ☐ 912.00 ☐ 912.50 ☐ 913.00 ☐ 913.50 ☐ 914.00 ☐ 914.50 ☐ 915.00 ☐ 915.50 ☐ 916.00 ☐ 916.50 ☒ 917.00 ☐ 917.50 ☐ 918.00 ☐ 918.50 ☐ 919.00 ☐ 919.50 ☐ 920.00 ☐ 920.50 ☐ 921.00 ☐ 921.50 ☐ 922.00 Custom Radio Frequency Scan Selection List : ☐ 922.50 ☐ 923.00 ☒ 923.50 ☒ 924.00 ☒ 924.50 ☐ 924.75 ☐ 925.00 ☐ 925.50 5 MHz only ☒ ≤7 MHz ☐ ≤10 MHz Not available in this region Select All Clear All Restore
Channel Bandwidth Scan :	☐ 5 MHz ☐ 7 MHz ☒ 10 MHz ☐ 20 MHz
Cyclic Prefix Scan :	☒ One Sixteenth
AP Selection Method :	☐ Power Level ☒ Optimize for Throughput
Color Code 1 :	65 (0—254) / Priority Primary ▼
Installation Color Code :	☐ Enabled ☒ Disabled
Large VC data Q :	☐ Enabled ☒ Disabled
Additional Color Codes	
Color Code :	5 (0—254) / Priority Tertiary ▼
	Add/Modify Color Code Remove Color Code
Additional Color Codes Table	
<u>Color Code</u>	<u>Priority</u>
0	Primary
1	Secondary
5	Tertiary
Power Control	
External Gain :	0 dB (Range: 0 — +40 dB)
Advanced	
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
Channel Bandwidth Scan	See Table 131 PMP 450i AP Radio attributes - 5 GHz on page 7-130.
Cyclic Prefix Scan	
AP Selection Method	

Color Code 1

**Installation Color
Code**

Large VC data Queue

Color Code

External Gain See [Table 131 PMP 450i AP Radio attributes - 5 GHz](#) on page [7-130](#)

**Receive Quality
Debug** See [Table 131 PMP 450i AP Radio attributes - 5 GHz](#) on page [7-130](#).

**Note**

The frequencies that a user can select are controlled by the country or a region and the Channel Bandwidth selected. There can be a case where a user adds a custom frequency (from the [Custom Frequencies page](#) on page [7-164](#)) and cannot see it in the pull down menu.

Radio page - PTP 450 BHM 5 GHz

Table 145 PTP 450 BHM Radio attributes –5 GHz

Radio Configuration

Frequency Band :

5.4 GHz ▾

Frequency Carrier :

5680.0 ▾

LBT Frequency Selected

Alternate Frequency Carrier 1 :

5492.5 ▾

Alternate Frequency Carrier 2 :

5485.0 ▾

Channel Bandwidth :

20 MHz ▾

Cyclic Prefix :

One Sixteenth ▾

Color Code :

5

(0—254)

Large VC data Q :

☐ Enabled

☒ Disabled

Frame Configuration

Downlink Data :

50

% (Range: 15 — 85 %)

Power Control

Transmit Power :

3

dBm (Range: -30 — +3 dBm) (0 dBm V / 0 dBm H)

External Gain :

17

dB (Range: 0 — +40 dB)

Advanced

Receive Quality Debug :

☐ Enabled

☒ Disabled

OFF ▾

Frame Alignment Legacy Mode :

Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0
Timing Port	OFF	OFF	OFF	OFF
Power Port	OFF	OFF	ON (Mode 1)	OFF

Attribute	Meaning
-----------	---------

Refer Table 134 PTP 450i BHM Radio page attributes – 5 GHz on page 7-142 for all parameters details.

Radio page - PTP 450 BHS 5 GHz

Table 146 PTP 450 BHM Radio attributes –5 GHz

Radio Configuration	
5.4/5.7 GHz	
☐ 5470.00 ☐ 5472.50 ☐ 5475.00 ☐ 5477.50 ☐ 5480.00 ☐ 5482.50 ☐ 5485.00 ☐ 5487.50 ☐ 5490.00 ☐ 5492.50 ☐ 5495.00 ☐ 5497.50 ☐ 5500.00 ☐ 5502.50 ☐ 5505.00 ☐ 5507.50 ☐ 5510.00 ☐ 5512.50 ☐ 5515.00 ☐ 5517.50 ☐ 5520.00 ☐ 5522.50 ☐ 5525.00 ☐ 5527.50 ☐ 5530.00 ☒ 5532.50 ☒ 5535.00 ☒ 5537.50 ☒ 5540.00 ☒ 5542.50 ☐ 5545.00 ☐ 5547.50 ☐ 5550.00 ☐ 5552.50 ☐ 5555.00 ☐ 5557.50 ☐ 5560.00 ☐ 5562.50 ☐ 5565.00 ☐ 5567.50 ☐ 5570.00 ☐ 5572.50 ☐ 5575.00 ☐ 5577.50 ☐ 5580.00 ☐ 5582.50 ☐ 5585.00 ☐ 5587.50 ☐ 5590.00 ☐ 5592.50 ☐ 5595.00 ☐ 5597.50 ☐ 5600.00 ☐ 5602.50 ☐ 5605.00 ☐ 5607.50 ☐ 5610.00 ☐ 5612.50 ☐ 5615.00 ☐ 5617.50 ☐ 5620.00 ☐ 5622.50 ☐ 5625.00 ☐ 5627.50 ☐ 5630.00 ☐ 5632.50 ☐ 5635.00 ☐ 5637.50 ☐ 5640.00 ☐ 5642.50 ☐ 5645.00 ☐ 5647.50 ☐ 5650.00 ☐ 5652.50 ☐ 5655.00 ☐ 5657.50 ☐ 5660.00 ☐ 5662.50 ☐ 5665.00 ☐ 5667.50 ☐ 5670.00 ☐ 5672.50 ☐ 5675.00 ☐ 5677.50 ☐ 5680.00 ☐ 5682.50 ☐ 5685.00 ☐ 5687.50 ☐ 5690.00 ☐ 5692.50 ☐ 5695.00 ☐ 5697.50 ☐ 5700.00 ☐ 5702.50 ☐ 5705.00 ☐ 5707.50 ☐ 5710.00 ☐ 5712.50 ☐ 5715.00 ☐ 5717.50 ☐ 5720.00 ☐ 5722.50 ☐ 5725.00 ☐ 5727.5 ☐ 5730.0 ☐ 5732.5 ☐ 5735.0 ☐ 5737.5 ☐ 5740.0 ☐ 5742.5 ☐ 5745.0 ☐ 5747.5 ☐ 5750.0 ☐ 5752.5 ☐ 5755.0 ☐ 5757.5 ☐ 5760.0 ☐ 5762.5 ☐ 5765.0 ☐ 5767.5 ☐ 5770.0 ☐ 5772.5 ☐ 5775.0 ☐ 5777.5 ☐ 5780.0 ☐ 5782.5 ☐ 5785.0 ☐ 5787.5 ☐ 5790.0 ☐ 5792.5 ☐ 5795.0 ☐ 5797.5 ☐ 5800.0 ☐ 5802.5 ☐ 5805.0 ☐ 5807.5 ☐ 5810.0 ☐ 5812.5 ☐ 5815.0 ☐ 5817.5 ☐ 5820.0 ☐ 5822.5 ☐ 5825.0 ☐ 5827.5 ☐ 5830.0 ☐ 5832.5 ☐ 5835.0 ☐ 5837.5 ☐ 5840.0 ☐ 5842.5 ☐ 5845.0 ☐ 5847.5 ☐ 5850.0 ☐ 5852.5 ☐ 5855.0 ☐ 5857.5 ☐ 5860.0 ☐ 5862.5 ☐ 5865.0 ☐ 5867.5 ☐ 5870.0 ☐ 5872.5 ☐ 5875.0 ☐ 5877.5 ☐ 5880.0 ☐ 5882.5 ☐ 5885.0 ☐ 5887.5 ☐ 5890.0 ☐ 5892.5 ☐ 5895.0 ☐ 5897.5 ☐ 5925.0 5 MHz only ☒ ≤ 7/10 MHz ☐ ≤ 15 MHz ☐ ≤ 20 MHz ☐ ≤ 30 MHz Not available in this region Bold only available with Engineering Key	
Custom Radio Frequency Scan Selection List : Select All Select All 5.4 Select All 5.7 Clear All Restore	
Channel Bandwidth Scan :	☐ 5 MHz ☐ 7 MHz ☐ 10 MHz ☐ 15 MHz ☒ 20 MHz
Cyclic Prefix Scan :	☒ One Sixteenth
Color Code :	244 (0—254)
Large VC data Q :	☐ Enabled ☒ Disabled
Power Control	
Transmit Power :	-10 dBm (Range: -30 — +22 dBm) (-13 dBm V / -13 dBm H)
External Gain :	0 dBi (Range: 0 — +40 dBi)
Advanced	
MIMO Rate Adapt Algorithm :	MIMO-A/B
Receive Quality Debug :	☐ Enabled ☒ Disabled

Attribute	Meaning
-----------	---------

Refer [Table 135 PTP 450i BHS Radio attributes – 5 GHz](#) on page 7-145 for all parameters details.

Radio Frequency Scan Selection List

The SM or BHS scans complete spectrum as per Full Spectrum Band Scan feature. SMs or BHS first boot into the smallest selected channel bandwidth (10 MHz, if selected) and scan all selected frequencies across both the 5.4 GHz and 5.7 GHz frequency bands.

After this scan, if a wider channel bandwidth is selected (20 MHz), the SM/BHS automatically changes to 20 MHz channel bandwidth and then scans for APs/BHSs. After the SM/BHS finishes this final scan it will evaluate the best AP/BHM with which to register. If required for registration, the SM/BHS changes its channel bandwidth back to 10 MHz to match the best AP/BHM.

The SM/BHS will attempt to connect to an AP/BHM based on power level (which affects the modulation state), channel bandwidth (which affects throughput) and number of SM/BHS registrations to the AP/BHM (which affects system contention performance).

If it is desired to prioritize a certain AP/BHM over other available APs/BHMs, operators may use the Color Code Priority feature on the SM/BHS. Utilization of the Color Code feature on the AP/BHM is recommended to further constrain the AP selection.

If the SM does not find any suitable APs/BHMs for registration after scanning all channel bandwidths, the SM restarts the scanning process beginning with the smallest configured channel bandwidth.

Selecting multiple frequencies and multiple channel bandwidths impacts the SM/BHS scanning time. The biggest consumption of time is in the changing of the SM/BHS channel bandwidth setting.

The worst case scanning time is approximately two minutes after boot up (SM/BHS with all frequencies and channel bandwidths selected and registering to an AP/BHM at 10 MHz). If only one channel bandwidth is selected the time to scan all the available frequencies and register to an AP/BHM is approximately one minute after boot up.

Other scanning features such as Color Code, Installation Color Code, and RADIUS authentication are unaffected by the Full Band Scan feature.

Dedicated Multicast Virtual Circuit (VC)

A Multicast VC allows to configure multicast packets to be transmitted over a dedicated channel at a configurable rate of 1X, 2X, 4X or 8X. This feature is available only for the PMP 450 and PMP 450i and is not backward compatible with PMP 430 series of radios.

To configure Multicast VC, the AP must have this enabled. This can be enabled in the “Multicast Data Control” section (under **Configuration > Radio** page). The default value is “Disable”. If set to the *default* value, all multicast packets are transmitted over the Broadcast VC data path. To enable, select the data rate that is desired for the Multicast VC Data Rate parameter and click **Save Changes** button. The radio requires no reboot after any changes to this parameter.

The multicast VC allows three different parameters to be configured on the AP. These can be changed on the fly and are saved on the flash memory.

**Note**

If the Multicast VC Data Rate is set to a modulation that the radio is not currently capable of or operates in non-permitted channel conditions, multicast data is sent but not received.

Ex: If Multicast VC Data Rate is set to 6x and the channel conditions only permit 4x mode of operation, then multicast data is sent at 6x modulation but the SM will not receive the data.

**Note**

The PMP 450 AP supports up to 119 VCs (instead of 238 VCs) when configured for 30 MHz channel bandwidth or 5 ms Frame Period. This limitation is not applicable for PMP 450i Series.

**Note**

- Actual Multicast CIR honored by the AP = Configured Multicast CIR / (Multicast Repeat Count + 1).
- Increasing the Multicast data rate has no impact on the Unicast data rate.
- For multicast and unicast traffic mix scenario examples, see [Table 147](#).

Table 147 Example for mix of multicast and unicast traffic scenarios

Repeat Count	Multicast Data Rate (Mbps)	Unicast Data Rate (Mbps)	Aggregate DL Data Rate (Mbps)
0	10	40	50
1	5	40	45
2	3.33	40	43.33

The statistics have been added to the **Data VC** page (under **Statistics > Data VC**). The table displays the multicast row on the PMP 450 Platform Family AP. The SM displays the multicast row if it is a PMP 450 Platform Family.

Figure 130 Multicast VC statistics

Data VC Statistics (CoS: 00 = Lowest Priority, 07 = Highest Priority)																	
Note: To measure the receive modulation of every fragment, Receive Quality Debug must be enabled.																	
Subscriber	VC	CoS	Inbound Statistics								Outbound Statistics					Queue Overflow	High Priority Queue
			octets	ucast pkts	nuclast pkts	discards	errors	QPSK frgmts	16-QAM frgmts	64-QAM frgmts	256-QAM frgmts	octets	ucast pkts	nuclast pkts	discards	errors	
Site Name - LUID: 002	018	00	2144887	6558	1121	0	0	56492098	33781656	20191607	19501199	2060928	7088	63	0	0	3972
Multicast	016	00	NA	NA	NA	NA	NA	NA	NA	NA	NA	0	0	0	0	0	NA
Broadcast	012	00	NA	NA	NA	NA	NA	NA	NA	NA	NA	592059	16	8523	0	0	NA

The AP and SM display Transmit and Receive Multicast Data Count (under the **Statistics > Scheduler** page), as shown in [Figure 131](#).

Figure 131 Multicast scheduler statistics

Radio Statistics	
Transmit Unicast Data Count :	20778
Transmit Broadcast Data Count :	13
Transmit Multicast Data Count :	0
Receive Unicast Data Count :	20828
Receive Broadcast Data Count :	206042
Receive Multicast Data Count :	0
Transmit Control Count :	160
Receive Control Count :	39
In Sync Count :	62
Out of Sync Count :	0
Overflow Count :	0
Underrun Count :	0
Receive Corrupt Data Count :	0
Receive Corrupt Control Data Count :	0
Receive Bad Broadcast Control Count :	0
Unsupported Feature Beacon Received :	0
Unknown Feature Beacon Received :	0
Old Version Beacon Received :	0
Wrong Frequency Beacon Received :	0
Non Lite Beacon Received :	0
Bad In Sync ID Received :	0
Rcv LT Start :	0
Rcv LT Start HS :	0
Rcv LT Result :	0
Xmt LT Result :	0
Frame Too Big :	0
Bad Acknowledgment :	0

Custom Frequencies page

In addition to the **Radio** tab, AP/SM/BH has another tab called **Custom Frequencies** as shown in [Table 148](#).

The custom frequency tab allows to configure custom frequency at 1 KHz raster. It means that the custom frequencies can be at granularity of 1 KHz e.g. 4910.123 MHz, 4922.333 MHz, 4933.421 MHz etc.



Note
Ensure that a customer frequency exists before using SNMP to set the radio to a Custom Frequency.

Table 148 450 Platform Family AP/SM/BH Custom Frequencies page – 5 GHz

Custom Frequencies Configuration

Custom Frequency Configuration : 4950.000 MHz (Range: 4902.500 — 4997.500 MHz)

Add Frequency

Remove Frequency

Add Default Frequencies

Remove All Custom Frequencies

Custom Frequencies

Number of Custom Frequencies : 12

4905.000 MHz
4910.000 MHz
4915.000 MHz
4920.000 MHz
4925.000 MHz
4930.000 MHz
4935.000 MHz
4940.000 MHz
4945.000 MHz
4950.000 MHz
4980.000 MHz
4990.001 MHz

Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 KHz can be added from the available range by keying in the frequency and then clicking the Add Frequency button. Click Remove Frequency button to delete a specific frequency keyed in the text box. Click Default Frequencies button to add a pre-defined list of frequencies that can be used in this band. This list can be reduced or increased by manually removing or adding other custom frequencies.
Custom Frequencies	Displays the complete list of user configured custom frequencies.

Table 149 PMP/PTP 450 SM/BH Custom Frequencies page – 3.65 GHz

Custom Frequencies Configuration

Custom Frequency Configuration : 0000.000 MHz (Range: 3552.500 — 3797.500 MHz)

Add Frequency

Remove Frequency

Default Frequencies

Custom Frequencies

Number of Custom Frequencies : 27

3552.500 MHz
3554.500 MHz
3555.000 MHz
3564.100 MHz
3564.200 MHz
3564.500 MHz
3652.500 MHz
3655.000 MHz
3657.500 MHz
3660.000 MHz
3662.500 MHz
3665.000 MHz
3667.500 MHz
3670.000 MHz
3672.500 MHz
3675.000 MHz
3677.500 MHz
3680.000 MHz
3682.500 MHz
3685.000 MHz
3687.500 MHz
3690.000 MHz
3692.500 MHz
3695.000 MHz
3697.500 MHz
3700.000 MHz
3750.000 MHz

Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 KHz can be added from the available range by keying in the frequency and then clicking the Add Frequency button. Click Remove Frequency button to delete a specific frequency keyed in the text box. Click Default Frequencies button to add a pre-defined list of frequencies that can be used in this band. This list can be reduced or increased by manually removing or adding other custom frequencies.
Custom Frequencies	Displays the complete list of user configured custom frequencies.

Table 150 PMP/PTP 450 SM/BH Custom Frequencies page – 3.5 GHz

Custom Frequencies Configuration Custom Frequency Configuration : 0000.000 MHz (Range: 3302.500 — 3597.500 MHz) Add Frequency Remove Frequency Default Frequencies	
Custom Frequencies Number of Custom Frequencies : 66 3302.500 MHz 3302.501 MHz 3302.555 MHz 3302.600 MHz 3302.655 MHz 3305.000 MHz 3310.000 MHz 3315.000 MHz 3320.000 MHz 3325.000 MHz 3330.000 MHz 3335.000 MHz 3340.000 MHz 3345.000 MHz 3350.000 MHz 3355.000 MHz 3360.000 MHz 3365.000 MHz 3370.000 MHz 3375.000 MHz 3380.000 MHz 3385.000 MHz 3390.000 MHz 3395.000 MHz 3400.000 MHz 3405.000 MHz 3410.000 MHz 	
Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 KHz can be added from the available range by keying in the frequency and then clicking the Add Frequency button. Click Remove Frequency button to delete a specific frequency keyed in the text box. Click Default Frequencies button to add a pre-defined list of frequencies that can be used in this band. This list can be reduced or increased by manually removing or adding other custom frequencies.

DFS for 5 GHz Radios

Dynamic Frequency Selection (DFS) is a requirement in several countries and regions for 5 GHz unlicensed systems to detect radar systems and avoid co-channel operation. DFS and other regulatory requirements drive the settings for the following parameters, as discussed in this section:

- Country Code
- Primary Frequency
- Alternate 1 and Alternate 2 Frequencies
- External Antenna Gain

On the AP, the **Home > DFS Status** page shows current DFS status of all three frequencies and a DFS log of past DFS events.

Figure 132 AP DFS Status

Current DFS Status	
Primary RF Carrier Frequency :	Active, 5485 Mhz, Normal Transmit
Alternate RF Carrier Frequency 1 :	Standby, 5570 Mhz, Available for use
Alternate RF Carrier Frequency 2 :	Standby, 5585 Mhz, Available for use
DFS Detections :	0

DFS Event History	
Time: 01/01/2011 : 04:39:52 UTC Event: Channel Availability Check, Freq: 5485 MHz	
Time: 01/01/2011 : 04:40:58 UTC Event: Start Transmit, Freq: 5485 MHz	

DFS operation

The ODUs use region-specific DFS based on the **Country Code** selected on the module's Configuration, General page. By directing installers and technicians to set the Country Code correctly, the operator gains confidence the module is operating according to national or regional regulations without having to deal with the details for each region.

The details of DFS operation for each Country Code, including whether DFS is active on the AP, SM, and which DFS regulations apply is shown in [Table 242](#) on page [10-37](#).

Contention slots

The SM uses reserved Contention slots and unused data slots for bandwidth requests.

Uplink Data Slots are used first for data. If they are not needed for data in a given frame, the remaining data slots can be used by the SMs for bandwidth requests. This allows SMs in sectors with a small number of Contention slots configured to still successfully transmit bandwidth requests using unused data slots.

A higher number of Contention slots give higher probability that a SM's bandwidth request is correctly received when the system is heavily loaded, but with the tradeoff that sector capacity is reduced, so there is less capacity to handle the request. The sector capacity reduction is about 200 kbps for each Contention slot configured in a 20 MHz channel at QPSK MIMO-A modulation. The reduction in sector capacity is proportionally higher at MIMO-B modulations (2 times at QPSK MIMO-B, 4 times at 16 QAM MIMO-B, 6 times at 64 QAM MIMO-B and 8 times at 256 QAM MIMO-B). If very few reserved Contention slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced.

The suggested Contention slot settings as a function of the number of active ~~VCs~~ SMs in the sector are shown in the table below.

Table 151 Contention slots and number of VCs

Number of VCs <u>SMs</u>	Recommended Number of Contention slots
1 to 10	3
11 to 50	4
51 to 150	6
151 and above	8

~~Note that each SM uses one or two VCs. All SMs have a Low Priority Channel that uses one VC; if the High Priority Channel is enabled for the SM, then the SM uses a second VC. Therefore the number of active VCs in a sector is greater than or equal to the number of SMs registered to the AP in the sector. For example, a network including 20 SMs with High Priority Channel disabled and 20 SMs with High Priority Channel enabled has 60 active VCs and may be configured with 6 Contention slots.~~

In a typical cluster, each AP must be set to the same number of Contention slots to assure proper timing in the send and receive cycles. However, where high incidence of small packets exists, as in a sector that serves several VoIP streams, additional Contention slots may provide better results. For APs in a cluster of mismatched Contention slots setting, or where PMP 450/450i Series is collocated with radios using different technologies, like PMP 430 or FSK, in the same frequency band, use the frame calculator. To download the PMP 450 Contention Slots Paper, see <http://www.cambiumnetworks.com/solution-papers/pmp-450-contention-slots>.

MIMO-A mode of operation

450 Platform Family supports MIMO-B mode using the following modulation levels: QPSK, 16-QAM, 64-QAM and 256-QAM. System Release 13.2 introduces MIMO-A mode of operation using the same modulation levels as the MIMO-B mode. With MIMO-B, the radio sends different streams of data over the two antennas whereas with MIMO-A, the radio uses a scheme that tries to optimize coverage by transmitting the same data over both antennas. This redundancy improves the signal to noise ratio at the receiver making it more robust, at the cost of throughput.

In addition to introducing MIMO-A modes, improvements have been made to the existing rate adapt algorithm to switch between MIMO-A and MIMO-B seamlessly without any intervention or added configuration by the operator. The various modulation levels used by the 450 Platform Family are shown in [Table 152](#).

Table 152 450 Platform Family Modulation levels

Rate	MIMO-B	MIMO-A
QPSK	2X MIMO-B	1X MIMO-A
16-QAM	4X MIMO-B	2X MIMO-A
64-QAM	6X MIMO-B	3X MIMO-A
256-QAM	8X MIMO-B	4X MIMO-A

System Performance

For System Performance details of all the 450 Platform Family ODUs please refer below tools:

- Link Capacity Planner for PMP/PTP 450 and 450i:
<https://support.cambiumnetworks.com/files/capacityplanner/>
- Link planner for PMP/PTP 450/450i and PMP 450m:
<https://support.cambiumnetworks.com/files/linkplanner/>

Table 153 Co-channel Interference per (CCI) MCS

MCS of Victim	MCS of Interferer	Channel BW (MHz)	CCI
1X (QPSK SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	10 dB
2X (16-QAM SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	17 dB
3X (64-QAM SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	25 dB
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	7 dB
2X (16-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	14 dB
3X (64-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	22 dB
4X (256-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	30 dB
2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	10 dB
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	17 dB
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	25 dB
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	33 dB

Table 154 Adjacent Channel Interference (ACI) per MCS

MCS of Victim	MCS of Interferer	Channel BW (MHz)	ACI	Guard Band
1X (QPSK SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-16 dB	None
2X (16-QAM SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-16 dB	None
3X (64-QAM SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-16 dB	None
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-13 dB	None
2X (16-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-13 dB	None
3X (64-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-13 dB	None
4X (256-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-10 dB	None
2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-16 dB	None
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-16 dB	None
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-16 dB	None
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20 or 30	-10 dB	None

Guard Band

When synchronized, no Guard Bands are needed for the 450* and 450i Series.

* For PMP 450 AP 3.6 GHz, Configuration -> Radio -> Power Control -> Adjacent Channel Support must be enabled.

Improved PPS performance of 450 Platform Family

The 450m and 450i Series provides improved packets per second (PPS) performance compared to 450 Series.

Through hardware and software enhancements, the PPS performance of the PMP 450i Series AP has been improved to 40k packets/second, measured through a standard RFC2544 test using 64 bytes packets. With this enhancement, operators are able to provide higher bandwidth including better VoIP and video services to end customers using existing SM deployments.

PMP 450m supports 100k packets/second.

Setting up SNMP agent

Operators may use SNMP commands to set configuration parameters and retrieve data from the AP and SM modules. Also, if enabled, when an event occurs, the SNMP agent on the 450 Platform Family sends a trap to whatever SNMP trap receivers configured in the management network.

- SNMPv2c
- SNMPv3

Configuring SM/BHS's IP over-the-air access

To access the SM/BHS management interface from a device situated above the AP, the SM/BHS's **Network Accessibility** parameter (under the web GUI at **Configuration > IP**) may be set to **Public**.

Table 155 LAN1 Network Interface Configuration tab of IP page attributes

LAN1 Network Interface Configuration	
IP Address :	169.254.1.1
Network Accessibility :	☐ Public ☒ Local
Subnet Mask :	255.255.255.0
Gateway IP Address :	169.254.0.0
DHCP state :	☐ Enabled ☒ Disabled
DHCP DNS IP Address :	☒ Obtain Automatically ☐ Set Manually
Preferred DNS Server :	10.120.10.12
Alternate DNS Server :	10.120.10.13
Domain Name :	example.com

Attribute	Meaning
IP Address	Internet Protocol (IP) address. This address is used by family of Internet protocols to uniquely identify this unit on a network.
Network Accessibility	Specify whether the IP address of the SM/BHS must be visible to only a device connected to the SM/BHS by Ethernet (Local) or be visible to the AP/BHM as well (Public).
Subnet Mask	If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the subnet mask of the SM/BHS for RF management traffic.
Gateway IP Address	If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the gateway IP address for the SM/BHS for RF management traffic.
DHCP state	If Enabled is selected, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable (read only), in the Network Interface tab of the Home page.
DNS IP Address	Canopy devices allow for configuration of a preferred and alternate DNS server IP address either automatically or manually. Devices must set DNS server IP address manually when DHCP is disabled for the management interface of the device. The default DNS IP addresses are 0.0.0.0 when configured manually.
Preferred DNS Server	The first address used for DNS resolution.

Alternate DNS Server	If the Preferred DNS server cannot be reached, the Alternate DNS Server is used.
Domain Name	The operator’s management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator’s network. The default domain name is example.com, and is only used if configured as such.

Configuring SNMP

The SNMP page configuration is explained below.



Note
The SNMP page for AP, SM, BHM and BHS has the same parameter attributes.

SNMP page – AP/SM/BHM/BHS

The SNMP page is explained in [Table 156](#).

Table 156 SNMP page attributes

SNMPv2c Settings	
SNMP Community String 1 :	Canopy
SNMP Community String 1 Permissions :	☐ Read Only ☒ Read / Write
SNMP Community String 2 (Read Only) :	Canopyro

SNMPv3 Settings	
Engine ID :	800000a1030a003ea004be Use Default Engine ID
SNMPv3 Security Level :	noAuth,noPriv ▼
SNMPv3 Authentication Protocol :	md5 ▼
SNMPv3 Privacy Protocol :	cbc-des ▼
SNMPv3 Read-Only User :	Username Canopyro Authorization Key Privacy Key
SNMPv3 Read/Write User :	☐ Enable R/W User Note:Also enable SNMPv2c Permission to be R/W ☒ Disable R/W User Username Canopy Authorization Key Privacy Key
SNMPv3 Trap Configuration :	Disabled ▼

SNMP Accessing Addresses	
Accessing IP / Subnet Mask 1 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 2 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 3 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 4 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 5 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 6 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 7 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 8 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 9 :	0.0.0.0 / 0
Accessing IP / Subnet Mask 10 :	0.0.0.0 / 0

Trap Addresses	
SNMP Trap Server DNS Usage :	☐ Append DNS Domain Name ☒ Disable DNS Domain Name
Trap Address 1 :	0.0.0.0
Trap Address 2 :	0.0.0.0
Trap Address 3 :	0.0.0.0
Trap Address 4 :	0.0.0.0
Trap Address 5 :	0.0.0.0
Trap Address 6 :	0.0.0.0
Trap Address 7 :	0.0.0.0
Trap Address 8 :	0.0.0.0
Trap Address 9 :	0.0.0.0
Trap Address 10 :	0.0.0.0

Trap Enable	
Sync Status :	☐ Enabled ☒ Disabled
Session Status :	☐ Enabled ☒ Disabled

Site Information	
Site Information Viewable to Guest Users :	☒ Enabled ☐ Disabled
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Attribute	Meaning
SNMP Community String 1	Specify a control string that can allow a Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is Canopy .
SNMP Community String 1 Permissions	You can designate the SNMP Community String 1 to be the password for WM, for example, to have Read / Write access to the module via SNMP or for all SNMP access to the module to be Read Only .
SNMP Community String 2 (Read Only)	Specify an additional control string that can allow a Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is Canopyro . This password will never authenticate a user or an NMS to read/write access. The Community String value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the Accessing Subnet , Trap Address , and Permission parameters.
Engine ID	The Engine ID may be between 5 and 32 hex characters. The hex character input is driven by RFC 3411 recommendations on the Engine ID. The default Engine ID is the MAC address of the device
SNMPv3 Security Level	Specify security model where users are defined and authenticated before granting access to any SNMP service. Each device can configure the security level of SNMPv3 to No authentication/No privacy, Authentication/No privacy, or Authentication/Privacy.
SNMPv3 Authentication Protocol	Currently, the SNMPv3 authentication protocol MD5 is supported.
SNMPv3 Privacy Protocol	Currently, the SNMPv3 privacy protocol CBC-DES is supported.
SNMPv3 Read-Only User	This filed allows for a read-only user per devices. The default values for the Read-Only users is: • Username = Canopyro • Authentication Password = authCanopyro • Privacy Password = privacyCanopyro
SNMPv3 Read/Write User	Read-write user by default is disabled. The default values for the Read/Write users is : • Username = Canopy • Authentication Password = authCanopy • Privacy Password = privacyCanopy
SNMPv3 Trap Configuration	When enabling transmission of SNMPv3 traps the read-only or read-write user credentials must be used and selected properly in order for the SNMP manager to correctly interpret the traps. By default transmission of SNMPv3 traps is disabled and all traps sent from the radios are in SNMPv2c format.

Accessing IP / Subnet Mask 1 to 10	Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both • The network IP address in the form xxx.xxx.xxx.xxx • The CIDR (Classless Interdomain Routing) prefix length in the form /xx For example: • the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet). • 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct Community String value. The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on "Classless Interdomain Routing." You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations. RECOMMENDATION: The subscriber can access the SM/BHS by changing the subscriber device to the accessing subnet. This hazard exists because the Community String and Accessing Subnet are both visible parameters. To avoid this hazard, configure the SM/BHS to filter (block) SNMP requests.
SNMP Trap Server DNS Usage	The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.
Trap Address 1 to 10	Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) or DNS names to which SNMP traps must be sent. Traps inform Wireless Manager or an NMS that something has occurred. For example, trap information is sent • after a reboot of the module. • when an NMS attempts to access agent information but either • supplied an inappropriate community string or SNMP version number. • is associated with a subnet to which access is disallowed.
Trap Enable, Sync Status	If the sync status traps (sync lost and sync regained) have to be sent to Wireless Manager or an NMS, select Enabled. If these traps have to be suppressed, select Disabled.
Trap Enable, Session Status	If you want session status traps sent to Wireless Manager or an NMS, select Enabled.

Site Information Viewable to Guest Users	Operators can enable or disable site information from appearing when a user is in GUEST account mode.
Site Name	Specify a string to associate with the physical module. This parameter is written into the <i>sysName</i> SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Contact	Enter contact information for the module administrator. This parameter is written into the <i>sysContact</i> SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Location	Enter information about the physical location of the module. This parameter is written into the <i>sysLocation</i> SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.

Configuring syslog

450 Platform Family includes:

- [Syslog event logging](#)
- [Configuring system logging](#)

Syslog event logging

Following events are logged in syslog as explained in [Table 157](#).

Table 157 Syslog parameters

Attribute	Meaning
Timestamp	All syslog messages captured from the radio have a timestamp.
Configuration Changes	This includes any device setting that has changed and includes the old or new parameter value, including the device reboots.
User Login and Logout	Syslog records each user login and logout, with username.
Add or Delete of user accounts through GUI and SNMP	Syslog captures any user accounts that are added or deleted.
Spectrum Analysis	Syslog records a message every time Spectrum Analysis runs.
 Note Since the AP/BHM must be set to a SM/BHS for Spectrum Analysis, syslog messages are not reported from the radio until the scan is done and the radio mode is switched back to AP/BHM.	
Link Test	Syslog records a message every time a Link Test is run.
Clear Statistics	Syslog sends a message when Statistics are cleared. This is done individually for each statistics page that is cleared.
SM Register or De-register	Syslog records a message when a SM registers or deregisters.
BHS Connect or Disconnect	Syslog records a message when a BHS connects or disconnects.

Configuring system logging

To configure system logging, select the menu option **Configuration > Syslog**.

Syslog page of AP/BHM

The Syslog Configuration page for AP/BHM is shown in [Table 158](#).

Table 158 Syslog Configuration attributes - AP

Syslog Server Configuration	
Syslog DNS Server Usage :	☐ Append DNS Domain Name ☒ Disable DNS Domain Name
Syslog Server :	0.0.0.0
Syslog Server Port :	514 <i>Default port number is 514</i>

Syslog Transmission	
AP Syslog Transmit :	☐ Enabled ☒ Disabled
SM Syslog Transmit :	☐ Enabled ☒ Disabled

Syslog Level	
Syslog Minimum Level :	info

Attribute	Meaning
Syslog DNS Server Usage	To configure the AP/BHM to append or not append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
AP Syslog Transmit Or BHM Syslog Transmit	When enabled, syslog messages are sent from the AP/BHM.
SM Syslog Transmit Or BHS Syslog Transmit	When enabled, syslog messages are sent from all the registered SMs/BHS, unless they are individually set to override this.
Syslog Minimum Level	This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity). For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

Syslog page of SM

To configure system logging, select the menu option **Configuration > Syslog**. The Syslog Configuration page is shown in [Table 159](#).

Table 159 Syslog Configuration attributes - SM

Syslog Server Configuration	
Syslog Configuration Source :	☒ AP preferred, use local when AP configuration unavailable ☐ Local only
Syslog DNS Server Usage :	☐ Append DNS Domain Name ☒ Disable DNS Domain Name
Syslog Server :	0.0.0.0
Syslog Server Port :	514 <i>Default port number is 514</i>

Syslog Transmission	
Syslog Transmission :	Obtain from AP, default disabled ▼

Syslog Level	
Syslog Minimum Level Source :	☒ AP preferred, use local when AP configuration unavailable ☐ Local only
Syslog Minimum Level :	info ▼

Attribute	Meaning
Syslog Configuration Source	This control determines whether the SM will attempt to use the syslog server definition from the AP, or whether it will use a local server definition. When set to AP preferred, use local when AP configuration unavailable, and if the SM can register with an AP, then it uses the syslog server defined on that AP. If the SM cannot register then it will syslog to its locally defined syslog server through its wired connection, if any. When set to Local only the SM ignores the AP's definition of the syslog server and allows the syslog server to be configured individually for each SM.
Syslog DNS Server Usage	To configure the SM to append or not the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
Syslog Transmission	Controls the SMs ability to transmit syslog messages. When set to "Learn from AP" the AP will control whether this SM transmits syslog messages. When set to "enable" or "disable" the SM will control whether it sends syslog messages. This allows an operator to override the AP settings for individual SMs in a sector.
Syslog Minimum Level Source	This control determines whether the SM attempts to use the minimum syslog level defined by the AP, or whether it uses a local defined value using the "Syslog Minimum Level" parameter. When set to "AP preferred, use local when AP configuration unavailable", and if the SM can register with an AP, then it uses the Syslog Minimum Level defined on that AP. If the SM cannot register then it uses its own Syslog Minimum Level setting. When set to "Local only" the SM will always use its own Syslog Minimum Level setting and ignores the AP's setting.

Syslog Minimum Level

This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity).

For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

Syslog page of BHS

The Syslog Configuration page is shown in [Table 160](#).

Table 160 Syslog Configuration attributes - BHS

Attribute	Meaning
Syslog Configuration Source	This control determines whether the BHS will attempt to use the syslog server definition from the BHM, or whether it will use a local server definition. - When set to BHM preferred, use local when BHM configuration unavailable, and if the BHS can register with a BHM, then it uses the syslog server defined on that BHM. If the BHS cannot register then it will syslog to its locally defined syslog server through its wired connection, if any. - When set to Local only the BHS ignores the BHM's definition of the syslog server and allows the syslog server to be configured individually for each BHS.
Syslog DNS Server Usage	To configure the BHS to append or not to append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
Syslog Transmission	Controls the BHSs ability to transmit syslog messages. When set to Learn from BHM the BHM will control whether this BHS transmits syslog messages. When set to enable or disable the BHS will control

	whether it sends syslog messages. This allows an operator to override the BHM settings for individual BHSs in a sector.
Syslog Minimum Level Source	This control determines whether the BHS attempts to use the minimum syslog level defined by the BHM, or whether it uses a local defined value using the Syslog Minimum Level parameter. When set to BHM preferred, use local when BHM configuration unavailable, and if the BHS can register with a BHM, then it uses the Syslog Minimum Level defined on that BHM. If the BHS cannot register then it uses its own Syslog Minimum Level setting. When set to Local only the BHS will always use its own Syslog Minimum Level setting and ignores the BHM's setting.
Syslog Minimum Level	This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity). For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

Configuring remote access

Accessing SM/BHS over-the-air by Web Proxy

The SM/BHS may be accessed via the AP/BHM management GUI by navigating to **Home > Session Status** (or **Home > Remote Subscribers** for AP only) and clicking on the SM's hyperlink.

For example, to access one of the SMs, click **LUID: 002 – [0a-00-3e-37-b9-fd]**, as shown in [Figure 133](#).

Figure 133 AP Session Status page

Home → Session Status

5.4GHz MIMO OFDM - Access Point - 0a-00-3e-a1-35-75

Session Status Configuration

Show Idle Sessions : ☒ Enabled ☐ Disabled

Session List Tools

Last Session Counter Reset : None [Reset Session Counters](#)

Last Time Idle SMs Removed : None [Remove Idle SMs](#)

Session Status List

Data : [SessionStatus.xml](#)

Device	Session	Power	Configuration
Subscriber	Hardware	Software Version	FPGA Version
LUID: 002 - [0a-00-3e-a0-a0-66] No Site Name	PMP 450	CANOPY 14.1.1	110615 (DES, Sched, US/ETSI) P

The **SessionStatus.xml** hyper link allows user to export all displayed SM data in Session Status table into an xml file.

To access any one of the SMs, click 450 Platform Family - SM hyperlink, as shown in [Figure 134](#).

Figure 134 AP Remote Subscribers page

Home → Remote Subscribers

5.4GHz MIMO OFDM - Access Point - 0a-00-3e-bb-00-fb

Remote Subscriber Modules

01. [Site Name - \[0a-00-3e-bb-01-04\] - LUID: 002](#)

Monitoring the Link

Link monitoring procedure

After configuring the link, either an operator in the network office or the SM/BHS INSTALLER user in the field (if read access to the AP/BHM is available to the INSTALLER) must perform the following procedure. Who is authorized and able to do this depends on local operator password policy, management VLAN setup and operational practices.

To monitor the link for performance, follow these instructions:

Procedure 22 Monitoring the AP-SM link

- 1 Access the web interface of the AP/BHM
- 2 In the left-side menu of the AP/BHM interface, select **Home**.
- 3 Click the **Session Status** tab.

Figure 135 Session Status page

Session Status Configuration

Show Idle Sessions : ☒ Enabled ☐ Disabled

Session List Tools

Last Session Counter Reset : None [Reset Session Counters](#)

Last Time Idle SMs Removed : None [Remove Idle SMs](#)

Session Status List

Data : [SessionStatus.xml](#)

Device Session Power Configuration

Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-b2-c6-aa] SM_01	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 003 - [0a-00-3e-b2-c6-9f] SM_04	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 004 - [0a-00-3e-b2-c5-f1] SM_08	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 005 - [0a-00-3e-b2-b2-6c] SM_07	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 006 - [0a-00-3e-b2-b3-fb] SM_12	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 007 - [0a-00-3e-b2-c7-14] SM_19	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)

- 4 The **Device** tab of Session Status List display all displayed SMs – MAC address, PMP/PTP Hardware, Software Version, FPGA Version and State

5 Click **Session Count** tab of Session Status List to display values for **Session Count**, **Reg Count**, and **Re-Reg Count**.

- **Session Count:** This field displays how many sessions the SM/BHS has had with the AP/BHM. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.
- **Reg Count:** When a SM/BHS makes a Registration Request, the AP/BHM checks its local session database to see whether it was registered earlier. If the AP/BHM concludes that the SM/BHS is not currently in session database and it is valid Registration Request, then the request increments the value of this field.
- **Re-Reg Count:** When a SM/BHS makes a Registration Request, the AP/BHM checks its local session database to see whether it was registered earlier. If the AP/BHM concludes that the SM/BHS is currently in session database, then the request increments the value of this field.
- Typically, a Re-Reg is the case where both
 - SM/BHS attempts to reregister for having lost communication with the AP/BHM.
 - AP/BHM has not yet observed the link to the SM/BHS as being down.

See [Session tab](#) on page 9-23

6 Click **Power** tab of Session Status list to display Downlink Rate, AP Rx Power (dBm), Signal Strength Radio (dB) for Uplink and Signal to Noise Radio (dB) for Uplink.

See [Power tab](#) on page 9-25

7 Click **Configuration** tab of Session Status list to get QoS configuration details:

- Sustained Data Rate (kbps)
- Burst Allocation (kbit)
- Max Burst Rate (kbit)
- Low Priority CIR (kbps)

See [Configuration tab](#) on page 9-26

8 Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.

9 If these values are low (for example, 1, 1, and 0, respectively, meaning that the SM/BHS registered and started a stable session once) and are not changing:

- Consider the installation successful.
- Monitor these values from the network office over the next several hours and days.

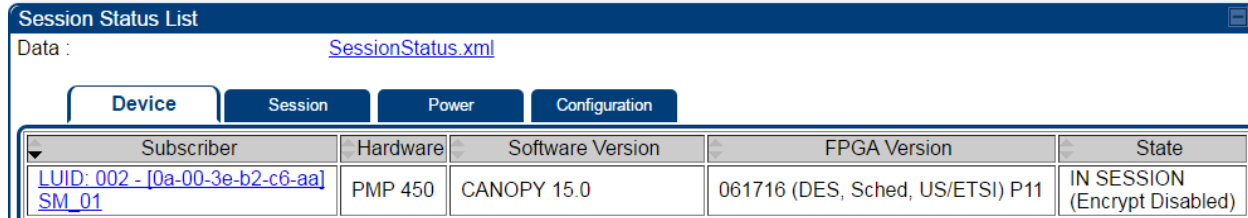
If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, Use **Receive Power Level** for aiming and then use Link Tests to confirm alignment).

Refer [Viewing Session Status](#) on page 9-22 for more details.

Exporting Session Status page of AP/BHM

The SessionStatus.xml hyper link allows user to export all displayed SMs or BHS data in Session Status table into an xml file.

Figure 136 Exporting Session Status page of PMP 450m AP



The screenshot shows a web interface titled "Session Status List". Below the title, there is a "Data:" label followed by a blue hyperlink "SessionStatus.xml". Below this, there are four tabs: "Device", "Session", "Power", and "Configuration". The "Device" tab is selected. Below the tabs is a table with five columns: "Subscriber", "Hardware", "Software Version", "FPGA Version", and "State". The table contains one row of data.

Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-b2-c6-aa] SM_01	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)

In case of PMP, if the session status page does not list any SM, the SessionStatus.xml will still be visible but the file would be empty. The file will contain data from all of the 5 different tables.

Export from command line

The scripts users can also get this file from command line, you have to authenticate successfully in order to download the file.

Wget

<http://169.254.1.1/SessionStatus.xml?CanopyUsername=test&CanopyPassword=test>

Configuring quality of service

Maximum Information Rate (MIR) Parameters

Point-to-multipoint links use the following MIR parameters for bandwidth management:

- Sustained Uplink Data Rate (kbps)
- Uplink Burst Allocation (kb)
- Sustained Downlink Data Rate (kbps)
- Downlink Burst Allocation (kb)
- Max Burst Downlink Data Rate (kbps)
- Max Burst Uplink Data Rate (kbps)

Set each of these parameters per AP or per SM independently.



Note

You can refer below whitepaper for 450 Platform Family Max Burst MIR:

<http://www.cambiumnetworks.com/resources/pmp-450-maxburst/>

Token Bucket Algorithm

The software uses a *token bucket* algorithm that has the following features:

- Stores credits (tokens) for the SM to spend on bandwidth for reception or transmission.
- Drains tokens during reception or transmission.
- Refills with tokens at the sustained rate set by the network operator.

For each token, the SM can send toward the network in the uplink (or the AP can send toward the SM in the downlink) an equivalent number of kilobits. Two buckets determine the permitted throughput: one in the SM for uplink and one in the AP for downlink.

The applicable set of **Uplink Burst Allocation** and **Downlink Burst Allocation** parameters determine the *number* of tokens that can fill each bucket. When the SM transmits (or the AP transmits) a packet, the equivalent number of tokens is removed from the uplink (or downlink) bucket.

Except when full, the bucket is continuously being refilled with tokens at *rates* that the applicable set of **Sustained Uplink Data Rate** and **Sustained Downlink Data Rate** parameters specify. The bucket often drains at a rate that is much faster than the sustained data rate but can refill at only the sustained data rate. Thus, the effects of the allocation and rate parameters on packet delay are as follows:

- The burst allocation affects how many kilobits are processed before packet delay is imposed.
- The sustained data rate affects the packet delay that is imposed.

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in [Figure 137](#).



Note

In these figures, *entry* refers to the setting in the data rate parameter, not the burst allocation parameter.

Figure 137 Uplink and downlink rate caps adjusted to apply aggregate cap

$$\text{uplink cap enforced} = \frac{\text{uplink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

$$\text{downlink cap enforced} = \frac{\text{downlink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

For example, in the SM, if you set the **Sustained Uplink Data Rate** parameter to 2,000 kbps and the **Sustained Downlink Data Rate** parameter to 10,000 kbps, then the uplink and downlink MIR that is enforced for the SM can be calculated as shown in [Figure 138](#).

Figure 138 Uplink and downlink rate cap adjustment example

$$\text{uplink cap enforced} = \frac{2,000 \text{ kbps} \times 7,000 \text{ kbps}}{2,000 \text{ kbps} + 10,000 \text{ kbps}} = 1,167 \text{ kbps}$$

$$\text{downlink cap enforced} = \frac{10,000 \text{ kbps} \times 7,000 \text{ kbps}}{2,000 \text{ kbps} + 10,000 \text{ kbps}} = 5,833 \text{ kbps}$$

In this example case, the derived 1,167-kbps uplink and 5,833-kbps downlink MIR sum to the fixed 7,000-kbps aggregate cap of the SM.

Committed Information Rate (CIR)

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum unless CIR is oversubscribed or RF conditions are degraded. CIR is oversubscribed when there is not enough available bandwidth to support CIR configuration for all subscribers. In this condition, SMs which are configured with a nonzero CIR will all operate at the maximum data rate supported by the link (subject to Maximum Information Rate and Burst Rate/Allocations). SMs which are configured with a CIR of 0 kbps will not transmit until CIR-configured SMs have completed transmission. CIR may be configured independently for high priority traffic and for low priority traffic.

CIR parameters may be configured in the following ways:

- Web-based management GUI
- SNMP
- Authentication Server (RADIUS) - when an SM successfully registers and authenticates, CIR information is retrieved from the RADIUS server.

Active CIR configuration can be verified via the AP's **Home > Session Status** page.

Bandwidth from the SM Perspective

In the SM, normal web browsing, e-mail, small file transfers and short streaming video are rarely rate limited with practical bandwidth management (QoS) settings. When the SM processes large downloads such as software upgrades and long streaming video or a series of medium-size downloads, the bucket rapidly drains, the burst limit is reached, and some packets are delayed. The subscriber experience is more affected in cases where the traffic is more latency sensitive.

Interaction of Burst Allocation and Sustained Data Rate Settings

If the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps, a data burst of 1000 kb is transmitted at full speed because the Burst Allocation is set high enough. After the burst, the bucket experiences a significant refill at the Sustained Data Rate. This configuration uses the advantage of the settable Burst Allocation.

If both the Burst Allocation and the Sustained Data Rate are set to 128 kb, a burst is limited to the Burst Allocation value. This configuration does not take advantage of the settable Burst Allocation.

If the Burst Allocation is set to 128 kb and the Sustained Data Rate is set to 256 kbps, the actual rate is the burst allocation (but in kbps). As above, this configuration does not take advantage of the settable Burst Allocation.

High-priority Bandwidth

To support low-latency traffic such as VoIP (Voice over IP) or video, the system implements a high-priority channel. This channel does not affect the inherent latencies in the system but allows high-priority traffic to be immediately served. The high-priority pipe separates low-latency traffic from traffic that is latency tolerant, such as standard web traffic and file downloads.

The number of channels available on the AP is reduced by the number of SMs configured for the high-priority channel (each SM operating with high-priority enabled uses two channels (virtual circuits) instead of one).

A module prioritizes traffic by

- reading the Low Latency bit (Bit 3) in the IPv4 Type of Service (ToS) byte in a received packet. Bit 3 is set by a device outside the system.
- reading the 802.1p field of the 802.1Q header in a received packet, where VLAN is enabled on the module.
- comparing the 6-bit Differentiated Services Code Point (DSCP) field in the ToS byte of a received packet to a corresponding value in the **Diffserv** tab of the Configuration page of the module. A packet contains no flag that indicates whether the encoding is for the Low Latency bit or the DSCP field. For this reason, you must ensure that all elements in your trusted domain, including routers and endpoints, set and read the ToS byte with the same scheme.

Modules monitor ToS bytes with DSCP fields, but with the following differences:

- The 6-bit length of the field allows it to specify one of 64 service differentiations.

- These correlate to 64 individual (**CodePoint**) parameters in the **Diffserv** tab of the Configuration page.
- Per RFC 2474, 3 of these 64 are preset and cannot be changed. (See <http://www.faqs.org/rfcs/rfc1902.html>.)
- For any or all of the remaining 61 CodePoint parameters, you can specify a value of
 - 0 through 3 for low-priority handling.
 - 4 through 7 for high-priority handling.

**Note**

Ensure that your Differentiated Services domain boundary nodes mark any entering packet, as needed, so that it specifies the appropriate Code Point for that traffic and domain. This prevents theft of service level.

An example of the **Diffserv** page in the Configuration menu and parameter descriptions are provided under [DiffServ attributes – AP/BHM](#) on page 7-62. This tab and its rules are identical from module type to module type. However, any of the 61 configurable Code Points can be set to a different value from module to module, thus defining unique per-hop behavior for some traffic.

This tab in the AP sets the priorities for the various packets in the downstream (sent from the public network). This tab in the SM sets the priorities for the various packets in the upstream (sent to the public network).

Typically, some SMs attach to older devices that use the ToS byte as originally formatted, and others to newer devices that use the DSCP field. The *default* values in the **Diffserv** page allow your modules to prioritize traffic from the older devices roughly the same as they traditionally have. However, these default values may result in more high-priority traffic as DSCP fields from the newer devices are read and handled. So, after making changes in the **Diffserv** page, carefully monitor the high-priority channel for high packet rates

- in SMs that you have identified as those to initially set and watch.
- across your network when you have broadly implemented Code Point values, such as via SNMP.

Traffic Scheduling

The characteristics of traffic scheduling in a sector are summarized in [Table 161](#).

Table 161 Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	132 Mbps
Latency	Number of frames required for the scheduling process	1
	Round-trip latency	≈ 6 ms
	AP broadcast the download schedule	No
High-priority Channel	Allocation for <i>uplink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for <i>downlink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	CIR high-priority
		CIR low-priority
		Other high-priority
		Other low-priority



Caution

Power requirements affect the recommended maximums for power cord length feeding the CMM4. See the dedicated user guide that supports the CMM that you are deploying.

Packets that have a priority of 4 to 7 in either the DSCP or a VLAN 802.1p tag are automatically sent on the high-priority channel, but only where the high-priority channel is enabled.

Setting the Configuration Source

The AP includes a **Configuration Source** parameter, which sets where SMs that register to the AP are controlled for MIR, CIR, VLAN, and the high-priority channel as follows. The **Configuration Source** parameter affects the source of:

- all MIR settings:
 - Sustained Uplink Data Rate
 - Uplink Burst Allocation
 - Max Burst Uplink Data Rate
 - Sustained Downlink Data Rate
 - Downlink Burst Allocation
 - Max Burst Downlink Data Rate
- all CIR settings:
 - Low Priority Uplink CIR
 - Low Priority Downlink CIR
 - Hi Priority Uplink CIR
 - Hi Priority Downlink CIR
- all SM VLAN settings
 - Dynamic Learning
 - Allow Only Tagged Frames
 - VLAN Aging Timeout
 - Untagged Ingress VID
 - Management VID
 - VLAN Membership
- the Hi Priority Channel setting

Table 162 Recommended combined settings for typical operations

Most operators who use...	must set this parameter...	in this web page/tab...	in the AP to...
no authentication server	Authentication Mode	Configuration/ Security	Disabled
	Configuration Source	Configuration/ General	SM
Wireless Manager (Authentication Server)	Authentication Mode	Configuration/ Security	Authentication Server
	Configuration Source	Configuration/ General	Authentication Server
RADIUS AAA server	Authentication Mode	Configuration/ Security	RADIUS AAA
	Configuration Source	Configuration/ General	Authentication Server

Table 163 Where feature values are obtained for a SM with authentication required

Configuration Source Setting in the AP	Values are obtained from		
	MIR Values	VLAN Values	High Priority Channel State
Authentication Server	Authentication Server	Authentication Server	Authentication Server
SM	SM	SM	SM
Authentication Server+SM	Authentication Server	Authentication Server, then SM	Authentication Server, then SM

**Note**

HPC represents the Hi Priority Channel (enable or disable).

Where Authentication Server, then SM is the indication, parameters for which Authentication Server does not send values are obtained from the SM. This is the case where the Authentication Server is operating on an Authentication Server release that did not support the feature. This is also the case where the feature enable/disable flag in Authentication Server is set to disabled. The values are those previously set or, if none ever were, then the default values.

Where Authentication Server is the indication, values in the SM are disregarded.

Where SM is the indication, values that Authentication Server sends for the SM are disregarded.

For any SM whose **Authentication Mode** parameter *is not* set to 'Authentication Required', the listed settings are derived as shown in [Table 164](#).

Table 164 MIR, VLAN, HPC, and CIR Configuration Sources, Authentication Disabled

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	VLAN Values	High Priority Channel State	CIR Values
Authentication Server	AP	AP	AP	AP
SM	SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM	SM

Configuring Quality of Service (QoS)

Quality of Service (QoS) page of AP

The QoS page of AP is explained in [Table 165](#).

Table 165 QoS page attributes - AP

The screenshot displays the 'AP Bandwidth Settings' and 'Priority Settings' sections of a configuration interface. The 'AP Bandwidth Settings' section is titled '(Uplink + Downlink) Sustained Data Rate <= 100000 kbps' and contains the following fields:

- Max Burst Uplink Data Rate : 0 (kbps) (Range: 0— 100000 kbps)
- Sustained Uplink Data Rate : 50000 (kbps) (Range: 0— 100000 kbps)
- Uplink Burst Allocation : 2500000 (kbits) (Range: 0— 2500000 kbits)
- Max Burst Downlink Data Rate : 0 (kbps) (Range: 0— 100000 kbps)
- Sustained Downlink Data Rate : 50000 (kbps) (Range: 0— 100000 kbps)
- Downlink Burst Allocation : 2500000 (kbits) (Range: 0— 2500000 kbits)
- Broadcast Downlink CIR : 200 (kbps) (Range: 0— 2333 kbps)

The 'Priority Settings' section contains the following fields:

- Priority Precedence : 802.1p Then DiffServ (dropdown menu)
- PPPoE Control Message Priority : ☐ High, ☒ Normal
- Prioritize TCP ACK : ☒ Enabled, ☐ Disabled

Attribute	Meaning
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Uplink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Sustained Uplink Data Rate	Specify the rate that each SM registered to this AP is replenished with credits for transmission. This default imposes no restriction on the uplink. See • Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73
Uplink Burst Allocation	Specify the maximum amount of data to allow each SM to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. See Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73

Max Burst Downlink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Downlink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Sustained Downlink Data Rate	Specify the rate at which the AP is replenished with credits (tokens) for transmission to each of the SMs in its sector. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the Sustained Downlink Data Rate . See • Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73
Broadcast Downlink CIR	Broadcast Downlink CIR (Committed Information Rate, a minimum) supports system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default. Broadcast Downlink CIR is closely related to the Broadcast Repeat Count parameter, which is settable in the Radio tab of the Configuration page in the AP: when the Broadcast Repeat Count is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the Broadcast Repeat Count parameter.
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the SM to utilize the high priority channel for PPPoE control messages. Configuring the SM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the SM.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled . This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements.

Quality of Service (QoS) page of SM

The QoS page of SM is explained in [Table 166](#).

Table 166 QoS page attributes - SM

MIR Bandwidth Settings	
(Uplink + Downlink) Sustained Data Rate <= 130000 kbps	
Sustained Uplink Data Rate :	50000 (kbps) (Range: 0 — 130000 kbps)
Sustained Downlink Data Rate :	50000 (kbps) (Range: 0 — 130000 kbps)
Uplink Burst Allocation :	2500000 (kbits) (Range: 0 — 2500000 kbits)
Downlink Burst Allocation :	2500000 (kbits) (Range: 0 — 2500000 kbits)
Max Burst Uplink Data Rate :	0 (kbps) (Range: 0 — 130000 kbps)
Max Burst Downlink Data Rate :	0 (kbps) (Range: 0 — 130000 kbps)
Enable Broadcast/ Multicast Data Rate :	☐ Enabled ☒ Disabled
Broadcast/ Multicast Uplink Data Rate :	Kbps ▼ 130000 (Range: 1 — 130000 kbps/65535 pps)

Priority Settings	
(Uplink + Downlink)(Low Priority + High Priority) CIR Data Rate <= 65534 kbps	
Low Priority Uplink CIR :	0 (kbps) (Range: 0 — 65534 kbps)
Low Priority Downlink CIR :	0 (kbps) (Range: 0 — 65534 kbps)
Hi Priority Channel :	☒ Enabled ☐ Disabled
Hi Priority Uplink CIR :	0 (kbps) (Range: 0 — 65534 kbps)
Hi Priority Downlink CIR :	0 (kbps) (Range: 0 — 65534 kbps)
Priority Precedence :	802.1p Then DiffServ ▼
PPPoE Control Message Priority :	☐ High ☒ Normal
Prioritize TCP ACK :	☒ Enabled ☐ Disabled

Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73
Sustained Downlink Data Rate	Specify the rate at which the AP is replenished with credits (tokens) for transmission to this SM. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters on Page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73
Uplink Burst Allocation	Specify the maximum amount of data to allow this SM to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. See Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191

	• Configuration Source on page 7-73
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the Sustained Downlink Data Rate with transmission credits. See Maximum Information Rate (MIR) Parameters on page 7-189 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-191 • Configuration Source on page 7-73
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Uplink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Max Burst Downlink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Downlink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Enable Broadcast / Multicast Data Rate	This parameter allows the operator to specify if Broadcast and Multicast data is rate-limited. This data rate can be entered in Kbps or PPS (Packets Per Second).
Broadcast / Multicast Data Rate	This parameter allows the operator to specify a data rate at which Broadcast and Multicast traffic is sent via the radio link.
Low Priority Uplink CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-190 • Setting the Configuration Source on page 7-194
Low Priority Downlink CIR	This field indicates the minimum rate at which low priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-190 • Setting the Configuration Source on page 7-194
Hi Priority Channel	See • High-priority Bandwidth on page 7-191 • Configuration Source on page 7-73
Hi Priority Uplink CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-190 • Setting the Configuration Source on page 7-194

Hi Priority Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-190 • Setting the Configuration Source on page 7-194
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the SM to utilize the high priority channel for PPPoE control messages. Configuring the SM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the SM.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to Disabled .

Quality of Service (QoS) page of BHM

The QoS page of BHM is explained in [Table 167](#).

Table 167 QoS page attributes - BHM

Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHM to utilize the high priority channel for PPPoE control messages. Configuring the BHM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to Disabled .

Quality of Service (QoS) page of BHS

The QoS page of BHS is explained in [Table 168](#).

Table 168 QoS page attributes - BHS

Priority Settings	
Priority Precedence :	802.1p Then DiffServ ▼
PPPoE Control Message Priority :	☐ High ☒ Normal
Prioritize TCP ACK :	☒ Enabled ☐ Disabled

Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHS to utilize the high priority channel for PPPoE control messages. Configuring the BHS in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to Disabled .

Installation Color Code

With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. When using the Installation Color Code feature, ensure that the SM is configured with the factory default Color Code configuration (Color Code 1 is “0”, Color Code 2-10 set to “0” and “Disable”). The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message “SM is registered via ICC – Bridging Disabled!” is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the **Rescan APs** functionality on the AP Eval page).

Figure 139 Installation Color Code of AP

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5490.0 ▾
Channel Bandwidth :	10 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	☐ 5.0 ms ☒ 2.5 ms
Color Code :	254 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	☐ Enabled ☒ Disabled

Zero Touch Configuration Using DHCP Option 66

This feature allows an SM to get its configuration via DHCP option 66. This can be used for the initial configuration of an SM as well as managing the configuration of SMs on an ongoing basis. Here is how it works in brief:

- When the SM boots up, if it is set to use DHCP client, it will send out a DHCP Discover packet which includes a request for DHCP Option 66.
- In case of a brand new SM out of the box, the DHCP Discover packet is sent out if the SM connects to an AP using Installation Color Code (ICC), even though DHCP client is not enabled in factory default config.
- An appropriately configured DHCP server will respond with a DHCP Offer and include a URL in response to the Option 66 request. The URL should point to the configuration file.
- The device will download the configuration file and apply it. The device will reboot automatically if needed. (Note: this requires “rebootIfRequired” flag to be added to the config file. See [Creating a Golden config file](#) on page 7-204.

Configuration Steps

Procedure 23 Zero Touch Configuration steps

- 1 Create the golden config file(s)
- 2 Host it on an TFTP/FTP/HTTP/HTTPS server
- 3 Configure the DHCP server to return the URL of the golden config file in option 66

When the SM boots up, it will get the URL for the golden config from the DHCP server via option 66, download it and apply it.

If all the SMs are configured exactly the same, then you can create just new golden config file that can be used with all SMs.

If the SMs are not configured the same, see if it is possible to group the SMs such that SMs with the same configuration are served by the same DHCP pool. User can then create multiple golden config files and configure the DHCP server to use the appropriate config file for each pool.

User can also create one config file per SM. This provides the most flexibility, but is practical only if you have a software tool/script to generate the config files for each MAC address. The files should be named <mac>.cfg where <mac> is the MAC address of the SM, and stored in the same directory on the file server. The DHCP server should be configured to return the directory name ending with a '/' in option 66. The SM will automatically add "<mac>.cfg" to the path and get its config file.

If some configuration is unique per SM, but rest of the configuration is common, the SMs can be staged with the unique part, and use option 66 to manage the common part. For example, if each SM needs to have its coordinates set, don't include the coordinates in the golden config file. Instead, configure the coordinates for each SM manually. Manage the rest of the configuration using DHCP option 66.

Creating a Golden config file

The easiest way to create the golden config file is to configure an SM, export its configuration and edit it. To export the configuration file from the GUI of the SM, go to "Configuration > Unit Settings" tab, go to the "Download Configuration File" section and click on the "<mac>.cfg" link. This will give you a text file in JSON format. You can edit this file in a text editor but it's easier to use a JSON editor like <https://www.jsoneditoronline.org/>.

Strip down the config file to remove sections and entries that don't care about, and keep only the items that require changes. If there are many required changes, it can easily get confusing. To identify the exact items changes, first reset the SM to factory default, export the config file, make the necessary changes, export a second config file, then use a tool like WinMerge (<http://winmerge.org/>) to identify the differences.

The config file contains the following informational entries at the top level.

```
"cfgUtcTimestamp": "cfgUtcTimestamp",
"swVersion": "CANOPY 13.3 (Build 15) SM-AES",
"cfgFileString": "Canopy configuration file",
"srcMacAddress": "0a-00-3e-a2-c2-74",
"deviceType": "5.4/5.7GHz MIMO OFDM - Subscriber Module",
"cfgFileVersion": "1.0"
```

The "cfgUtcTimestamp", "swVersion", "srcMacAddress" and "deviceType" lines can be deleted. Do not delete the "cfgFileString" and "cfgFileVersion" entries.

Next, create an object named "configFileParameters" at the top level. Under that, add a parameter called "rebootIfRequired" and set it to true. This tells the SM to reboot automatically if a reboot is needed to apply the new configuration.

A sample configuration file that has been edited for use via DHCP option 66 is given below.

```
{
  "userParameters": {
    "smNetworkConfig": {
      "networkAccess": 1
    },
    "location": {
      "siteName": "Test site"
    },
    "smRadioConfig": {
```

```

    "frequencyScanList": [
        5475000,
        5480000
    ],
    "colorCodeList": [
        {
            "colorCode": 42,
            "priority": 1
        }
    ]
},
"networkConfig": {
    "lanDhcpState": 1
}
},
"cfgFileVersion": "1.0",
"cfgFileString": "Canopy configuration file",
"configFileParameters": {
    "rebootIfRequired": true
}
}

```

When configuration is imported, only the items that exist in the configuration file are modified. Parameters that are not in the imported file are not changed. If user wish to revert those settings to their factory default values, please add a “setToDefaults” item under “configFileParameters” section with a value of true.

```

"cfgFileVersion": "1.0",
"cfgFileString": "Canopy configuration file",
"configFileParameters": {
    "rebootIfRequired": true,
    "setToDefaults": true
}

```

In case, the SM needs to fetch the configuration file on each boot up even when not connecting to AP via ICC, set “Network Accessibility” to “Public” and “DHCP State” to “Enabled” in the “Configuration > IP” page before exporting the configuration.

Hosting the config file

Copy the golden configuration file to an FTP, TFTP, HTTP or HTTPS server. This location can be password protected; you just have to include the user name and password in the URL.

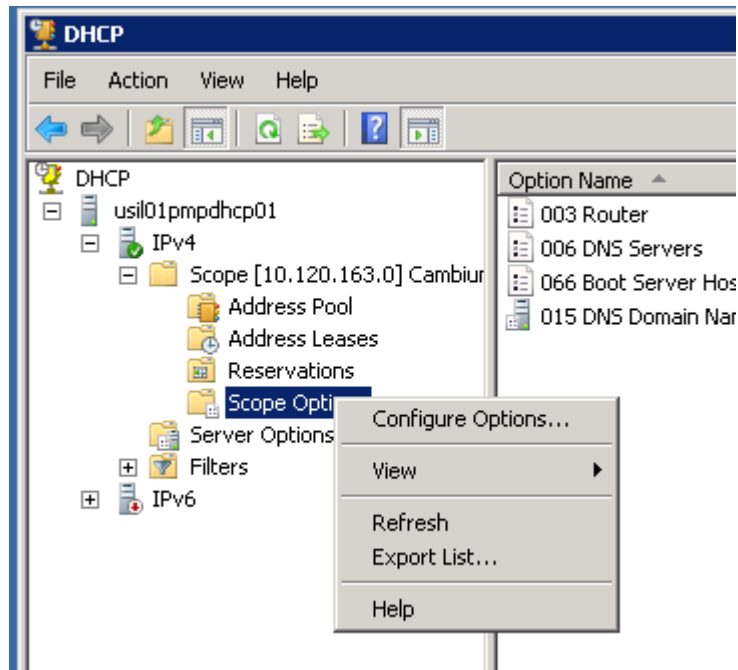
DHCP server configuration

Configure DHCP server to return the full URL to the golden config file as the value of DHCP option 66.

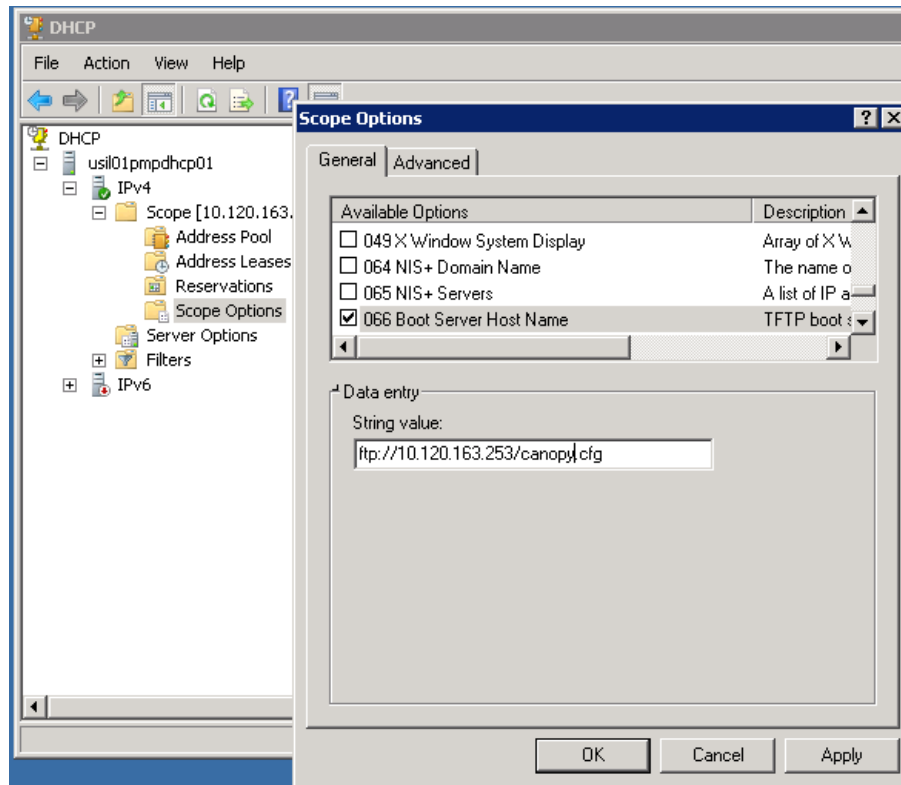
The following example explains how to make the change for Windows Server 2008. Adapt it to your specific DHCP server.

Procedure 24 DHCP server configuration

- 1 Click “Start > Administrative Tools > DHCP”
- 2 If you have multiple “Scopes” defined, identify the correct “Scope” that will serve IP addresses for the SMs
- 3 Right click on “Scope Option” under the correct “Scope” and select “Configure Options”



- 4 In the “Scope Options” dialog, scroll down to “066 Boot Server Host Name”, select the checkbox and enter the full URL to the golden config file as the “String value”. Then click “OK”.



- 5 In the DHCP snap-in window, right click and “Refresh” to see the DHCP option 66 in the list of DHCP options

Supported URL Formats

FTP, TFTP, HTTP and HTTPS URLs are supported. Some examples are given below.

- <ftp://10.120.163.253/canopy.cfg>
- <ftp://admin:admin123@10.120.163.253/canopy.cfg> (login as admin with password admin123)
- <tftp://10.120.163.253/canopy.cfg>
- <http://10.120.163.253/golden-config.cfg>
- <https://10.120.163.253/smconfig/golden-config.cfg>

User can also specify the URL pointing to a directory and not a specific file. Terminate the URL with a “/” to indicate that it is a directory and not a file. Use this format when each SM has its own individual config file. The directory should contain files named “<mac>.cfg”, one for each SM.

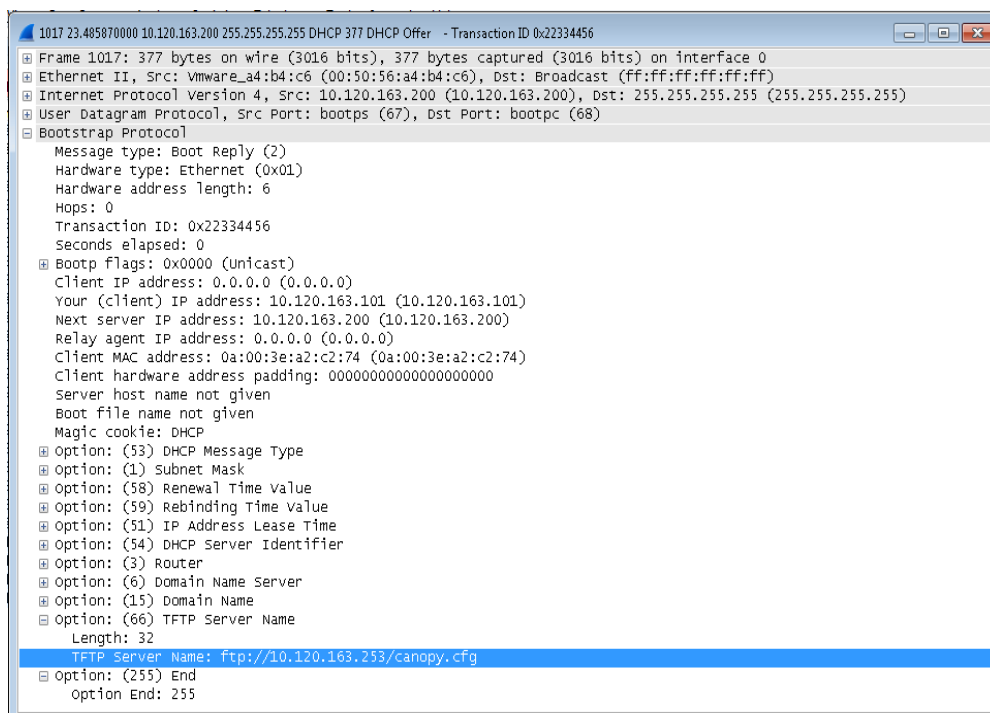
For example:

<ftp://10.120.163.253/smconfig/>

In this case, the SM will append “<mac>.cfg” to the path and try to get that file. For example, if the SM’s MAC address is 0a-00-3e-a2-c2-74, it will request for <ftp://10.120.163.253/smconfig/0a003ea2c274.cfg>. This mechanism can be used to serve individual config file for each SM.

Troubleshooting

- 1 Ensure that the ___14 SM is running 13.3 or newer version of software.
- 2 If the SM has factory default config, confirm ICC is enabled on the AP, so the SM can connect to it.
- 3 If the SM is connecting to the AP using a color code other than ICC, make sure the SM has “Network Accessibility” set to “Public” and “DHCP State” set to “Enabled” in the “Configuration > IP” page.
- 4 Make sure the golden config file does not turn off “Network Accessibility” or “DHCP State”. If it does, the SM will no longer request the config file when it is rebooted.
- 5 Check the event log of the SM to see the status of the configuration file import including any errors that prevented it from importing the file.
- 6 Capture the DHCP Offer packet from the DHCP server to the SM and verify that Option 66 has the expected URL.



Configuring Radio via config file

The 450 Platform Family supports export and import of a configuration file from the AP or SM as a text file. The configuration file is in JSON format.

To export or import the configuration file, the logged in user needs to be an ADMINISTRATOR and it must not be a “read-only” account.

The exported configuration file contains the complete configuration including all the default values. To keep a backup of the current configuration, the file can be saved as-is and imported later.

While importing a configuration file, it can be either imported the full configuration or a sparse configuration containing only the items that need to be changed. If a sparse configuration file is imported, only the items in the file will be imported. Other configuration will remain unchanged. There could also be used a special flag in the configuration file to tell the device to apply the configuration starting from factory default (Refer [Special Headers for configuration file](#) on page 7-210).

Import and Export of config file

The config file import and export is supported in **Configuration > Unit Settings** page. The procedure for importing and exporting config file is explained below.

Figure 140 Configuration File upload and download page

The screenshot displays the 'Configuration File upload and download page' with three tabs. The first tab, 'Download Configuration File', is active and shows a text input field containing the filename '0a003ea0007d.cfg'. The second tab, 'Upload and Apply Configuration File', is also visible and contains a 'File:' label, a 'Choose File' button, the text 'No file chosen', an 'Upload' button, and an 'Apply Configuration File' button. The third tab, 'Status of Configuration File', is empty.

The DHCP server configuration procedure is as follows:

Procedure 25 DHCP server configuration

- 1 Login to the GUI and go to **Configuration > Unit Settings**.
- 2 Under Download Configuration File tab, click on the “<mac>.cfg” link, where <mac> is the MAC address of the device (for example, “01003ea2c274.cfg”).
- 3 Save the file to the local disk.

The below procedure is to be followed for Importing a config file

Procedure 26 Import the configuration from the GUI

- 1 Login to the GUI and go to Configuration → Unit Settings.
- 2 Click on "Browse" button under "Upload and Apply Configuration File" tab and select the configuration file from disk.
- 3 Click "Upload" followed by "Apply Configuration File" button click.
- 4 The "Status of Configuration File" section will show the results of the upload.
- 5 Review it to make sure there are no errors. Then click on "Reboot" to reboot with the imported configuration

The special headers for config file is explained below:

Procedure 27 Special Headers for configuration file

- 1 A "configFileParameters" section can be added to the header to control the behavior of the device when importing configuration.
- 2 The "**setToDefaults**" when set to "true" tell the device to reset to factory default configuration and apply the configuration in the file on top of that. So any attribute not in the configuration file will be set to its factory default value. By default, the configuration in the file is merged with the existing configuration on the device.
The "**rebootIfRequired**" flag when set to "true" tell the device to reboot automatically if needed to apply the configuration change. By default, the device will not reboot automatically.

```
{
  "cfgFileString": "Canopy configuration file",
  "cfgFileVersion": "1.0",
  "configFileParameters": {
    "setToDefaults": true,
    "rebootIfRequired": true,
  }
}
```

Configuring cnMaestro™ Connectivity

450 Platform Family network can be onboarded, configured and managed using cnMaestro™ Cloud or On Premises Server.

Onboarding

Onboarding can be done in one of several ways:

- Using Cambium ID and Onboarding key
- Using Manufacturer's Serial Number (Only if it starts with an "M" and is 12 characters long)
- On Premises Zero Touch onboarding of AP/SM using DHCP option 43 and 15
- PMP SM Zero touch onboarding to the cnMaestro server where PMP AP is onboarded.

To configure the PMP devices, enable Remote Management under Configuration->cnMaestro as shown in [Table 169](#).

Table 169 Configuring cnMaestro

The screenshot displays the cnMaestro configuration interface with three main sections:

- Configuration:**
 - Remote Management: ☒ Enable, ☐ Disable
 - cnMaestro URL:
 - Connection Status: Cambium-ID Not Configured
- Credentials:**
 - Cambium ID:
 - Onboarding Key:
 - AccountID:
- Device Agent Information:**
 - Device Agent Version: 2.54

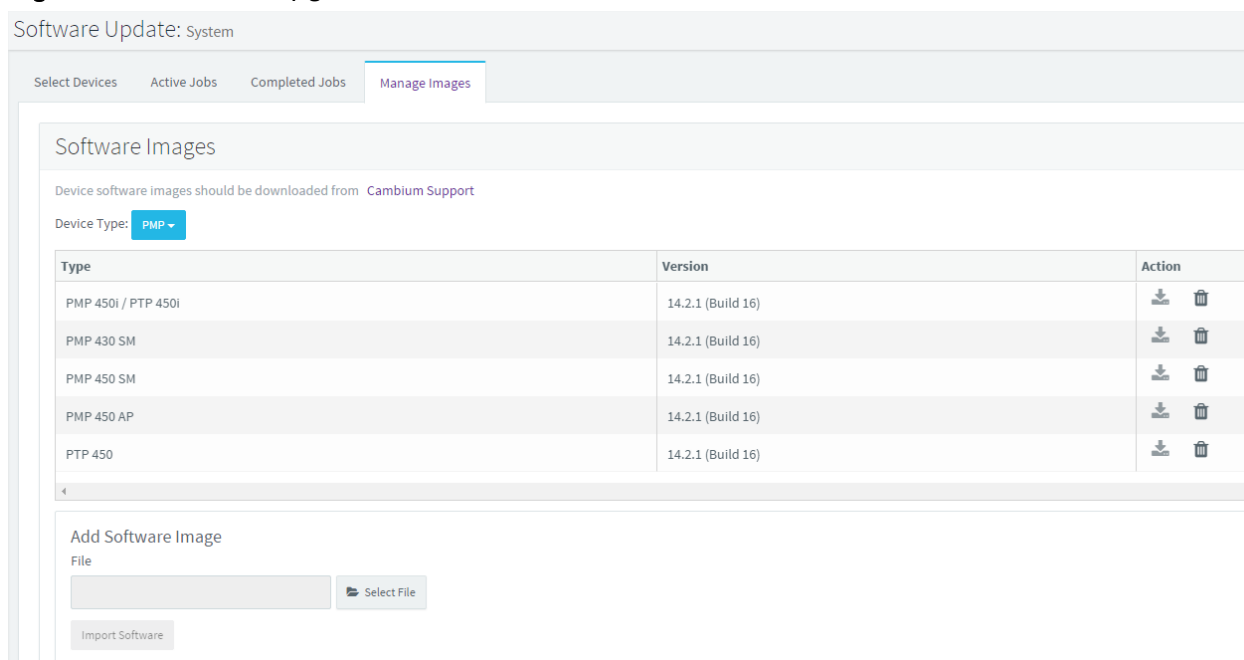
Attribute	Meaning
Remote Management	This field enables/disables remote management of 450 Platform Family products.
cnMaestro URL	This field allows to enter cnMaestro URL e.g. https://cloud.cambiumnetworks.com Or cnMaestro on premises URL
Connection Status	This field indicates cnMaestro connectivity status.
Cambium ID	This field allows to enter Cambium ID for onboarding 450 Platform devices.
Onboarding Key	This field allows to enter Onboarding Key for onboarding.
AccountID	This field indicates Account ID of the customer.

Device Agent Version	This field shows device agent version.
----------------------	--

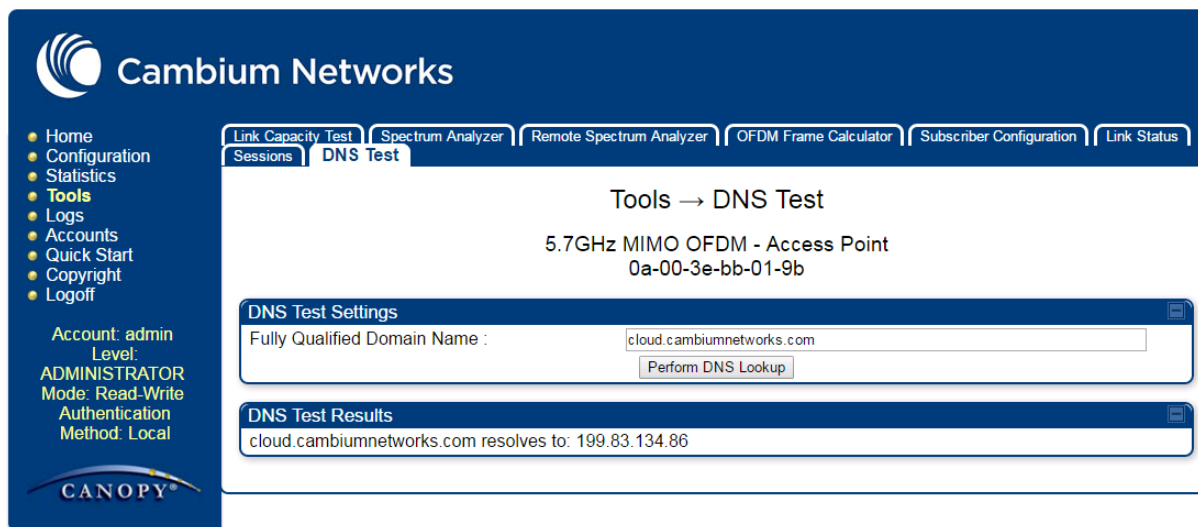
Prerequisites for onboarding to cnMaestro™

- Devices types must be PMP 450m Series, PMP/PTP 450 Series, PMP/PTP 450i Series or PMP 430 Series SMs (interoperability mode only).
- Minimum required software version of 14.2.1. Device software images can be downloaded from <http://support.cambiumnetworks.com> or from the On Premises cnMaestro server by navigating to Operate >Software Update->Manage Images. Select
- Device type to display the available images and then click the download icon as shown in [Figure 141](#).

Figure 141 Software Upgrade from cnMaestro™



- IP connectivity between PMP Device and the cnMaestro server is established. Ensure Port 443 is open in the firewall as this port is used for secure communication between the PMP device and the cnMaestro server through web sockets. In addition, if the PMP device and cnMaestro™ server are on different subnets, proper routes should be established for communication.
- For PMP AP, a valid DNS setting is required so that the AP will be able to resolve the cnMaestro URL. DNS settings can be verified by performing a DNS lookup under Tools->DNS Test on the AP as shown in [Figure 142](#).

Figure 142 DNS Test for cnMaestro™ connectivity

- If the SM is in Bridge mode, then LAN1 must have public accessibility with a public IP assigned and corresponding DNS setting.
- If the SM is in NAT mode, then Remote Management should be enabled with the standalone configuration option and DNS settings.

Knowledge Based articles for onboarding

For onboarding the devices to cloud server and troubleshooting the onboarding issues in cloud server please see the following link:

<http://community.cambiumnetworks.com/t5/cnMaestro/Device-On-boarding/td-p/51484>

For onboarding the devices to on Premises server and configuring the DHCP server options for on boarding please see the following link:

<http://community.cambiumnetworks.com/t5/cnMaestro/Device-Onboarding-and-Linux-DHCP-Options-for-cnMaestro-On/m-p/55187#U55187>

Order of Device Onboarding

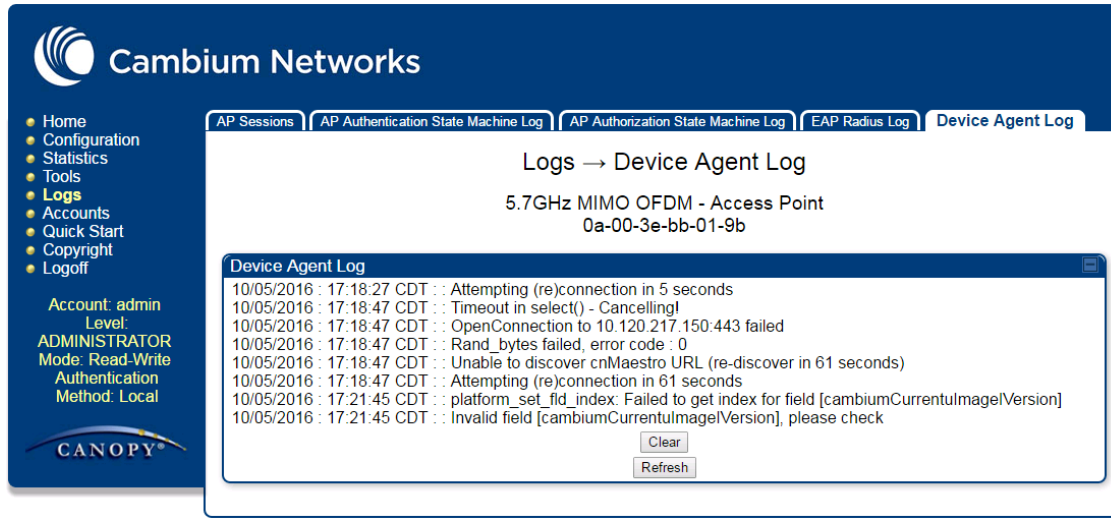
The device discovery order is as follows in On Permisses cnMaestro™ Server. If any of the options is not configured, the discovery method will fallback to the next option:

1. Static cnMaestro URL
2. Zero Touch token (on boarding of PMP SMs when the corresponding AP is on boarded)
3. DHCP Option 43
4. DHCP Option 15
5. <https://cloud.cambiumnetworks.com>

Device Agent Logs

For debugging any onboarding issues please check the device agent logs by navigating to Logs->Device Agent Logs on the PMP device GUI as shown in [Figure 143](#). In addition, a tech support dump can for the PMP device can be obtained from cnMaestro™ by navigating to Monitor->Tools menu after selecting the particular PMP device in the tree and clicking the tech support file icon. This can be send to Cambium support for further troubleshooting.

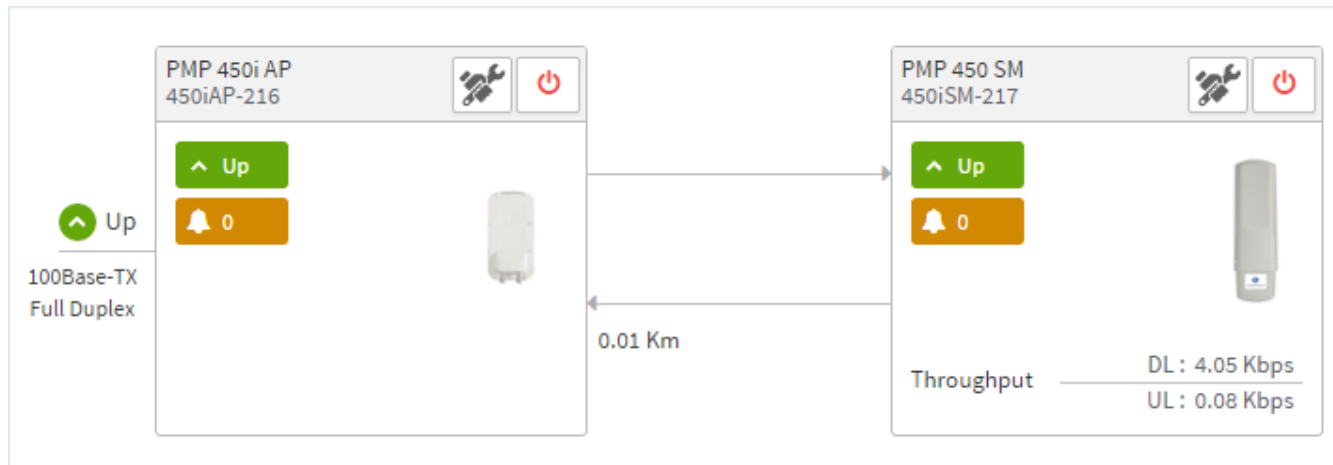
Figure 143 Device Agent Logs



Monitoring Tools for PMP Devices on cnMaestro™

cnMaestro™ as of this release offers several debugging tools for PMP devices. Some examples are:

- Pictorial view of network hierarchy
- Device status
- Tech support file
- Throughput
- Alarms
- Reboot
- Debug Logs
- Network connectivity – ping and DNS lookup

Figure 144 Example cnMaestro™ screenshot

For more information on these tools please see

<http://community.cambiumnetworks.com/t5/cnMaestro/How-to-use-the-cnMaestro-Tools-for-Troubleshooting-Device-or/m-p/54503#U54503>

Zero Touch on boarding of the PMP SMs when the corresponding AP is on boarded

First a link should be established between the PMP AP and SM either by configuring manually or using the ICC. Once the AP and SM link is established, the AP must be onboarded to cnMaestro™ using one of several ways detailed above under the Onboarding section. Once the AP is onboarded to cnMaestro™ Cloud or On premises cnMaestro™ server, the SMs under the AP will automatically onboard to cnMaestro™ using a Zero touch token that is communicated between the AP and SMs. This is applicable to existing SMs registered to the AP as well as new SMs registering to the AP for the first time. The SMs appear on the onboarding queue of cnMaestro™ and the operator must “Approve” the devices in order to manage them.

The following operations for PMP Devices are available on cnMaestro™

- Monitor the device details in the Dashboard page by navigating to the **Monitor >Dashboard** menu and selecting the PMP AP/SM in the tree.
- Monitor notifications related to the PMP AP/SM by navigating to the **Monitor >Notifications** Menu and selecting the PMP AP/SM in the tree.
- Monitor device statistics on the statistics page by navigating to the **Monitor >Statistics** menu and selecting the PMP AP/SM in the tree, then selecting the PMP AP or PMP SM in the Device type dropdown.
- Monitor Performance graphs related to the PMP AP/SM by navigating to the **Monitor >Performance** menu and selecting the required performance graph (i.e Throughput, SMs, Modulation) and selecting the PMP AP/SM in the tree.
- Troubleshoot the device on the Troubleshooting page by navigating to the **Monitor >Tools** menu and selecting the PMP AP/SM in the tree.

- Configure the devices by navigating to the **Configure > Devices** menu and selecting the PMP AP/SM in the tree and selecting the config template that needs to be pushed to the device. Configuration templates need to be created before the configuration can be pushed to the device. The template can be created by copying the existing configuration from the view device configuration link provided in the same page and then modifying the template as needed and then pushing to the same device or other similar devices. Template needs to be properly reviewed for IP Address and other critical parameters to avoid stranding SMs (resulting in a truck roll) by pushing an incorrect configuration. Configuration templates can be created by navigating to the Configure->Templates page and selecting the PMP device type while creating the template.
- Once on 14.2.1, PMP devices can be upgraded to future supported versions from cnMaestro™ by navigating to the **Operate > Software Update** page and selecting the “PMP Sectors” option from the device type drop down and the version to which the device needs to be upgraded. It is recommended to upgrade the AP first, then the SMs.
- PMP Device Inventory details can be reviewed by navigating to the **Monitor > Inventory** page.

Configuring a RADIUS server

Configuring a RADIUS server in a PMP 450 Platform network is optional, but can provide added security, increase ease of network management and provide usage-based billing data.

Understanding RADIUS for PMP 450 Platform Family

PMP 450 Platform modules include support for the RADIUS (Remote Authentication Dial In User Service) protocol supporting Authentication and Accounting.

RADIUS Functions

RADIUS protocol support provides the following functions:

- **SM Authentication** allows only known SMs onto the network (blocking “rogue” SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to “rogue” APs). RADIUS authentication is used for SMs, but is not used for APs.
- **SM Configuration:** Configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when a SM registers to an AP.
- **User Authentication** allows users to configure a separate User authentication server along with the SM authentication server. If firmware is upgraded while using this functionality and no User authentication servers are configured, then AP continues to use the SM authentication server for User authentication
- **SM Accounting** provides support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP.
- **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed IP** allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).
- —

Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

- FreeRADIUS, Version 2.1.8
- Aradial RADIUS, Version 5.1.12

- Microsoft RADIUS (Windows Server 2012 R2 version)
- Cisco ACS, Version 5.7.0.15

**Note**

Aradial 5.3 has a bug that prevents “remote device login”, so doesn’t support the user name and password management feature.

Choosing Authentication Mode and Configuring for Authentication Servers - AP

On the AP’s **Configuration > Security** tab, select the **RADIUS AAA Authentication Mode**. The following describes the other **Authentication Mode** options for reference, and then the **RADIUS AAA** option.

- **Disabled:** Requires no authentication. Any SM (except a SM that itself has been configured to *require* RADIUS authentication by enabling Enforce Authentication as described below) is allowed to register to the AP.
- **Authentication Server:** Authentication Server in this instance refers to Wireless Manager in BAM-only mode. Authentication is required for a SM to register to the AP. Only SMs listed by MAC address in the Wireless Manager database is allowed to register to the AP.
- **AP Pre-Shared Key:** Canopy offers a pre-shared key authentication option. In this case, an identical key must be entered in the Authentication Key field on the AP’s Configuration > Security tab and in the Authentication Key field on each desired SM’s Configuration > Security tab.
- **RADIUS AAA:** To support RADIUS authentication of SMs, on the AP’s Configuration > Security tab select RADIUS AAA. Only properly configured SMs with a valid certificate is allowed to register to the AP.

When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.

The default IP address is 0.0.0.0. The default Shared Secret is “CanopySharedSecret”. The Shared Secret can be up to 32 ASCII characters (no diacritical marks or ligatures, for example).

Table 170 Security tab attributes

Authentication Server Settings			
Authentication Mode :	Disabled ▼		
Authentication Server DNS Usage :	☐ Append DNS Domain Name ☒ Disable DNS Domain Name		
Authentication Server 1 :	10.120.226.6	Shared Secret	
Authentication Server 2 :	0.0.0.0	Shared Secret	
Authentication Server 3 :	0.0.0.0	Shared Secret	
Authentication Server 4 (BAM ONLY) :	0.0.0.0		
Authentication Server 5 (BAM ONLY) :	0.0.0.0		
Radius Port :	1812	Default port number is 1812	
Authentication Key :		(Using All 0xFF's Key)	
Select Key :	☐ Use Key above ☒ Use Default Key		

Airlink Security	
Encryption Setting :	None ▼

AP Evaluation Configuration	
SM Display of AP Evaluation Data :	☐ Disable Display ☒ Enable Display

Session Timeout	
Web, Telnet, FTP Session Timeout :	3600 Seconds

IP Access Filtering			
IP Access Control :	☐ IP Access Filtering Enabled - Only allow access from IP addresses specified below ☒ IP Access Filtering Disabled - Allow access from all IP addresses		
Allowed Source IP 1 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)

Security Mode	
Web Access :	HTTP Only ▼
SNMP :	SNMPv3 Only ▼
Telnet :	☒ Enabled ☐ Disabled
FTP :	☒ Enabled ☐ Disabled
TFTP :	☒ Enabled ☐ Disabled

Attribute	Meaning
Authentication Mode	Operators may use this field to select the following authentication modes: Disabled—the AP requires no SMs to authenticate. Authentication Server —the AP requires any SM that attempts registration to be authenticated in Wireless Manager before registration. AP PreShared Key - The AP acts as the authentication server to its SMs and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP and all SMs desired to register to that AP. There is also an option of leaving the AP and SMs at their default setting of using the “Default Key”. Due to the nature of the authentication operation, if you want to set a specific authentication key, then you MUST configure the key on all of the SMs and reboot them BEFORE enabling the key and option on the AP. Otherwise, if you configure the AP first, none of the SMs is able to register. RADIUS AAA - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network and does not progress trying the other servers.
Authentication Server DNS Usage	The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.
Authentication Server 1	
Authentication Server 2	Enter the IP address or server name of the authentication server (RADIUS or WM) and the Shared Secret configured in the authentication server. When Authentication Mode RADIUS AAA is selected, the default value of Shared Secret is “CanopySharedSecret”. The Shared Secret may consist of up to 32 ASCII characters.
Authentication Server 3	
Authentication Server 4 (BAM Only)	
Authentication Server 5 (BAM Only)	
Radius Port	This field allows the operator to configure a custom port for RADIUS server communication. The default value is <i>1812</i> .
Authentication Key	The authentication key is a 32-character hexadecimal string used when Authentication Mode is set to AP Pre-Shared Key . By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.

Selection Key	This option allows operators to choose which authentication key is used: Use Key above means that the key specified in Authentication Key is used for authentication Use Default Key means that a default key (based off of the SM's MAC address) is used for authentication
Encryption Key	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. None provides no encryption on the air link. DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. AES (Advanced Encryption Standard): An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
SM Display of AP Evaluation Data	You can use this field to suppress the display of data about this AP on the AP Evaluation tab of the Tools page in all SMs that register.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the AP.
IP Access Control	You can permit access to the AP from any IP address (IP Access Filtering Disabled) or limit it to access from only one, two, or three IP addresses that you specify (IP Access Filtering Enabled). If you select IP Access Filtering Enabled , then you must populate at least one of the three Allowed Source IP parameters or have no access permitted from any IP address
Allowed Source IP 1	If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the AP from any IP address. You may populate as many as all three.
Allowed Source IP 2	If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.
Allowed Source IP 3	
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • HTTP Only – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • HTTPS Only – provides a secured web access. The radio to be accessed via https1://<IP of Radio>.