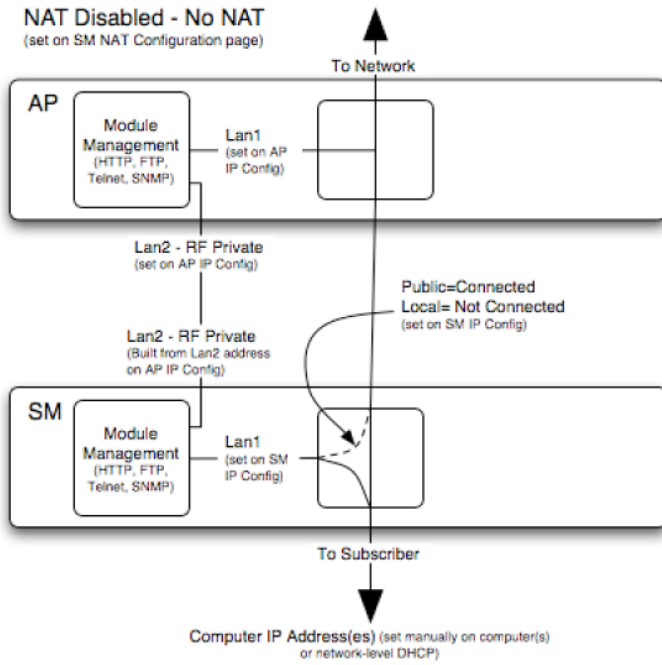


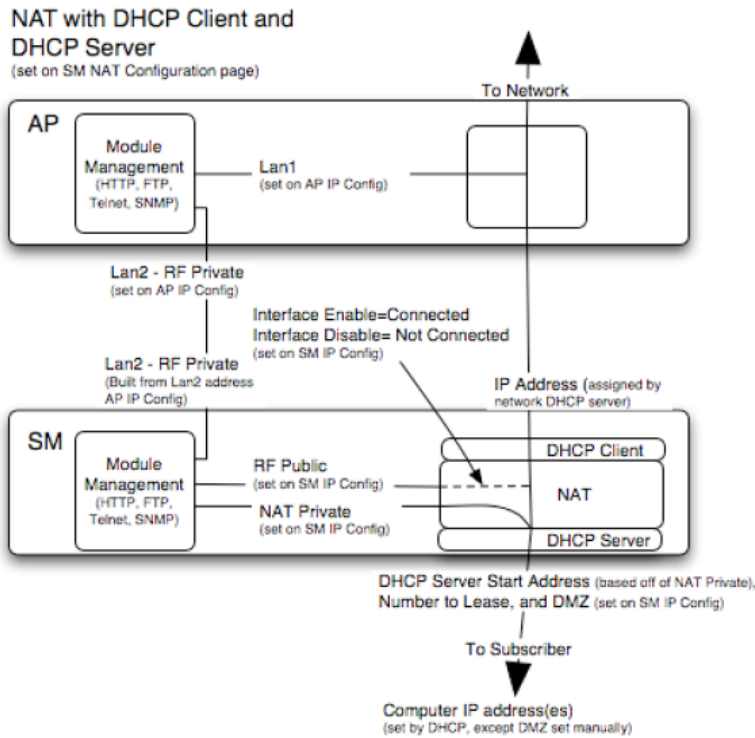
Figure 103 NAT disabled implementation



NAT with DHCP Client and DHCP Server

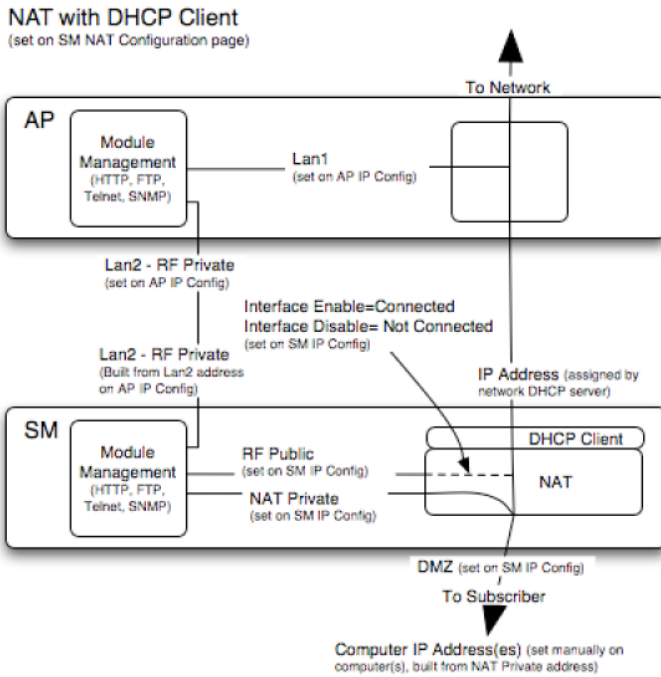
The NAT with DHCP Client and DHCP server is illustrated in [Figure 104](#).

Figure 104 NAT with DHCP client and DHCP server implementation



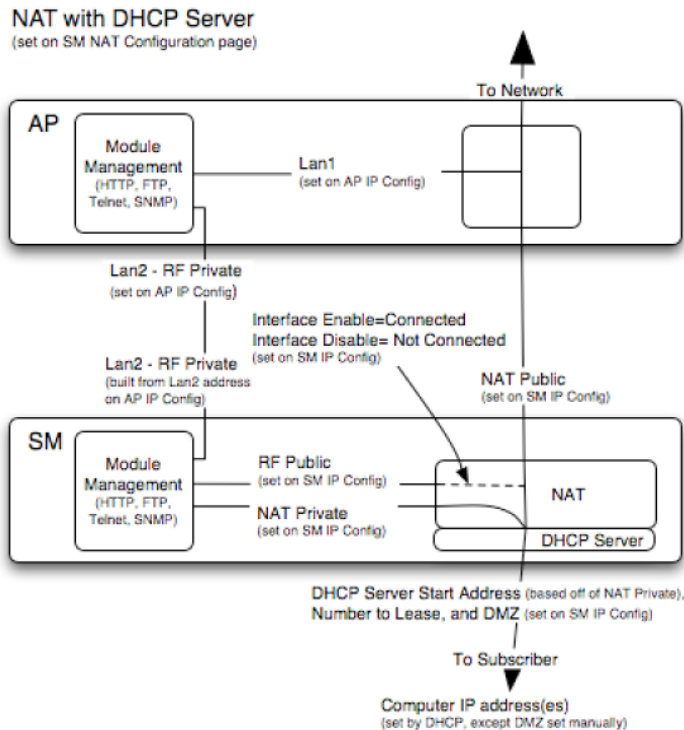
NAT with DHCP Client

Figure 105 NAT with DHCP client implementation



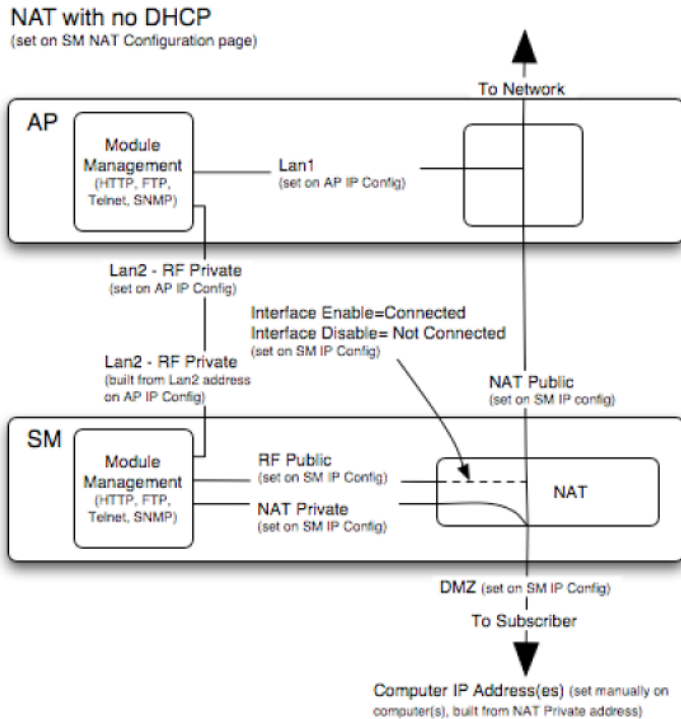
NAT with DHCP Server

Figure 106 NAT with DHCP server implementation



NAT without DHCP

Figure 107 NAT without DHCP implementation



NAT and VPNs

VPN technology provides the benefits of a private network during communication over a public network. One typical use of a VPN is to connect employees remotely (who are at home or in a different city), with their corporate network through a public Internet. Any of several VPN implementation schemes is possible. By design, NAT translates or changes addresses, and thus interferes with a VPN that is not specifically supported by a given NAT implementation.


With NAT enabled, SM supports L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs. With NAT disabled, SM supports all types of VPNs.

IP interface with NAT disabled - SM

The IP page of SM with NAT disabled is explained in [Table 77](#).

Table 77 IP attributes - SM with NAT disabled

LAN1 Network Interface Configuration	
IP Address :	10.120.216.15
Network Accessibility :	<input checked="" type="radio"/> Public <input type="radio"/> Local
Subnet Mask :	255.255.255.0
Gateway IP Address :	10.120.216.254
DHCP state :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DHCP DNS IP Address :	<input type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

Attribute	Meaning
IP Address	<p>Enter the non-routable IP address to associate with the Ethernet connection on this SM. (The default IP address from the factory is 169.254.1.1.) If you forget this parameter, you must both:</p> <ul style="list-style-type: none"> physically access the module. use recovery mode to access the module configuration parameters at 169.254.1.1. See Radio recovery mode – Radio Recovery Console / Default Mode (fka Default Plug) on page 1-20
	<p> Note</p> <p>Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.</p>
Network Accessibility	<p>Specify whether the IP address of the SM must be visible to only a device connected to the SM by Ethernet (Local) or be visible to the AP/BHM as well (Public).</p>
Subnet Mask	<p>Enter an appropriate subnet mask for the SM to communicate on the network. The default subnet mask is 255.255.0.0.</p>
Gateway IP Address	<p>Enter the appropriate gateway for the SM to communicate with the network. The default gateway is 169.254.0.0.</p>
DHCP state	<p>If you select Enabled, 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, but not settable, in the Network Interface tab of the Home page.</p> <p>In this tab, DHCP State is settable only if the Network Accessibility</p>

parameter in the IP tab is set to **Public**. This parameter is also settable in the NAT tab of the Configuration web page, but only when NAT is enabled.

If the **DHCP state** parameter is set to **Enabled** in the **Configuration > IP** sub-menu of the SM/BHS, do not check the **BootpClient** option for **Packet Filter Types** in its Protocol Filtering tab, because doing so can block the DHCP request. (Filters apply to all packets that leave the SM via its RF interface, including those that the SM itself generates.) If you want to keep DHCP enabled and avoid the blocking scenario, select the **Bootp Server** option instead. This will result in responses being appropriately filtered and discarded.

DHCP 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. DNS servers may be configured automatically from the DHCP response when DHCP is enabled for the management interface of the device. Optionally devices may be configured to set the DNS server IP address manually when DHCP is enabled for the management interface. The default DNS IP addresses are 0.0.0.0 when configured manually.
Preferred DNS Server	The first DNS server used for DNS resolution.
Alternate DNS Server	The second DNS server used for DNS resolution.
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.

IP interface with NAT enabled - SM

The IP page of SM with NAT enabled is explained in [Table 78](#).

Table 78 IP attributes - SM with NAT enabled

NAT Network Interface Configuration	
IP Address :	169.254.1.1
Subnet Mask :	255.255.255.0

Attribute	Meaning
IP Address	Assign an IP address for SM/BHS management through Ethernet access to the SM/BHS. Set only the first three bytes. The last byte is permanently set to 1. This address becomes the base for the range of DHCP-assigned addresses.
Subnet Mask	Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.

NAT tab with NAT disabled - SM

The NAT tab of SM with NAT disabled is explained in [Table 79](#).

Table 79 NAT attributes - SM with NAT disabled

NAT Enable	
NAT Enable/Disable :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<input type="button" value="Save Changes"/>	
WAN Interface	
Connection Type :	DHCP
IP Address :	0.0.0.0
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.0.0.0
Reply to Ping on WAN Interface :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
LAN Interface	
IP Address :	10.120.216.19
Subnet Mask :	255.255.255.xxx
DMZ Enable :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ IP Address :	xxx.xxx.xxx.52
LAN DHCP Server	
DHCP Server Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DHCP Server Lease Timeout :	30 Days (Range : 1 — 30)
DHCP Start IP :	xxx.xxx.xxx.2
Number of IP's to Lease :	50
DNS Server Proxy :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically (From WAN DHCP or PPPoE) <input type="radio"/> Set Manually
Preferred DNS IP Address :	0.0.0.0
Alternate DNS IP Address :	0.0.0.0
Remote Configuration Interface	
Remote Management Interface :	Disable
Connection Type :	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address :	0.0.0.0
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.0.0.0
DHCP DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com
NAT Protocol Parameters	
ARP Cache Timeout :	20 Minutes (Range : 1 — 30)
TCP Session Garbage Timeout :	120 Minutes (Range : 4 — 1440)
UDP Session Garbage Timeout :	4 Minutes (Range : 1 — 1440)
Translation Table Size :	2048 Translations (Range : 1024 — 8192)

Attribute	Meaning
NAT Enable/Disable	<p>This parameter enables or disables the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet or wired side of a SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet or wired side of the SM.</p> <p>When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP/BHM, but this may constrain network design.</p>
IP Address	This field displays the IP address for the SM. DHCP Server <i>will not</i> automatically assign this address when NAT is disabled.
Subnet Mask	This field displays the subnet mask for the SM. DHCP Server <i>will not</i> automatically assign this address when NAT is disabled.
Gateway IP Address	This field displays the gateway IP address for the SM. DHCP Server <i>will not</i> automatically assign this address when NAT is disabled.
ARP Cache Timeout	If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 minutes.
TCP Session Garbage Timeout	Where a large network exists behind the SM, you can set this parameter to lower than the default value of 120 minutes. This action makes additional resources available for greater traffic than the default value accommodates.
UDP Session Garbage Timeout	You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 minutes.
Translation Table Size	Total number of minutes that have elapsed since the last packet transfer between the connected device and the SM/BHS.

**Note**

When NAT is disabled, the following parameters are not required to be configurable:

WAN Interface > Connection Type, IP Address, Subnet Mask, Gateway IP address

LAN Interface > IP Address

LAN DHCP Server > DHCP Server Enable/Disable, DHCP Server Lease Timeout, Number of IP's to Lease, DNS Server Proxy, DNS IP Address, Preferred DNS IP address, Alternate DNS IP address

Remote Management Interface > Remote Management Interface, IP address, Subnet Mask, DHCP DNS IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name

NAT Protocol Parameters > ARP Cache Timeout, TCP Session Garbage Timeout, UDP Session Garbage Timeout, Translation Table Size

NAT tab with NAT enabled - SM

The NAT tab of SM with NAT enabled is explained in [Table 80](#).

Table 80 NAT attributes - SM with NAT enabled

NAT Enable	
NAT Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<input type="button" value="Save Changes"/>	
WAN Interface	
Connection Type :	DHCP
IP Address :	0.0.0.0
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.0.0.0
Reply to Ping on WAN Interface :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
LAN Interface	
IP Address :	169.254.1.1
Subnet Mask :	255.255.255.0
DMZ Enable :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ IP Address :	169.254.1.52
LAN DHCP Server	
DHCP Server Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DHCP Server Lease Timeout :	30 Days (Range : 1 — 30)
DHCP Start IP :	169.254.1.2
Number of IP's to Lease :	50
DNS Server Proxy :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically (From WAN DHCP or PPPoE) <input type="radio"/> Set Manually
Preferred DNS IP Address :	0.0.0.0
Alternate DNS IP Address :	0.0.0.0
Remote Configuration Interface	
Remote Management Interface :	Enable (Standalone Config)
Connection Type :	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address :	169.254.1.2
Subnet Mask :	255.255.0.0
Gateway IP Address :	169.254.0.0
DHCP DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com
NAT Protocol Parameters	
ARP Cache Timeout :	20 Minutes (Range : 1 — 30)
TCP Session Garbage Timeout :	120 Minutes (Range : 4 — 1440)
UDP Session Garbage Timeout :	4 Minutes (Range : 1 — 1440)

Attribute	Meaning
NAT Enable/Disable	This parameter enables or disabled the Network Address Translation

	<p>(NAT) feature for the SM. NAT isolates devices connected to the Ethernet or wired side of a SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic separate from its address for management, terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet or wired side of the SM.</p> <p>When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design.</p>
WAN Interface	The WAN interface is the RF-side address for transport traffic.
Connection Type	<p>This parameter may be set to</p> <p>Static IP—when this is the selection, all three parameters (IP Address, Subnet Mask, and Gateway IP Address) must be properly populated.</p> <p>DHCP—when this is the selection, the information from the DHCP server configures the interface.</p> <p>PPPoE—when this is the selection, the information from the PPPoE server configures the interface.</p>
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 for RF transport 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 for RF transport traffic.
Reply to Ping on WAN Interface	By default, the radio interface <i>does not</i> respond to pings. If you use a management system (such as WM) that will occasionally ping the SM, set this parameter to Enabled .
LAN Interface	The LAN interface is both the management access through the Ethernet port and the Ethernet-side address for transport traffic. When NAT is enabled, this interface is redundantly shown as the NAT Network Interface Configuration on the IP tab of the Configuration web page in the SM.
IP Address	Assign an IP address for SM/BHS management through Ethernet access to the SM. This address becomes the base for the range of DHCP-assigned addresses.
Subnet Mask	Assign a subnet mask of 255.255.255.0 or a more restrictive subnet mask. Set only the last byte of this subnet mask. Each of the first three bytes is permanently set to 255.
DMZ Enable	Either enable or disable DMZ for this SM/BHS.
DMZ IP Address	If you enable DMZ in the parameter above, set the last byte of the DMZ host IP address to use for this SM when DMZ is enabled. Only one such address is allowed. The first three bytes are identical to those of the NAT

	private IP address. Ensure that the device that receives network traffic behind this SM is assigned this address. The system provides a warning if you enter an address within the range that DHCP can assign.
DHCP Server	This is the server (in the SM) that provides an IP address to the device connected to the Ethernet port of the SM.
DHCP Server Enable/Disable	<p>Select either Enabled or Disabled.</p> <p>Enable to:</p> <ul style="list-style-type: none"> • Allow this SM to assign IP addresses, subnet masks, and gateway IP addresses to attached devices. • Assign a start address for DHCP. • Designate how many IP addresses may be temporarily used (leased). <p>Disable to:</p> <ul style="list-style-type: none"> • Restrict SM/BHS from assigning addresses to attached devices.
DHCP Server Lease Timeout	Based on network performance, enter the number of days between when the DHCP server assigns an IP address and when that address expires. The range of values for this parameter is 1 to 30 days. The default value is 30 days.
DHCP Start IP	If you enable DHCP Server below, set the last byte of the starting IP address that the DHCP server assigns. The first three bytes are identical to those of the NAT private IP address.
Number of IPs to Lease	Enter how many IP addresses the DHCP server is allowed to assign. The default value is 50 addresses.
DNS Server Proxy	This parameter enables or disables advertisement of the SM/BHS as the DNS server. On initial boot up of a SM with the NAT WAN interface configured as DHCP or PPPoE, the SM module will not have DNS information immediately. With DNS Server Proxy disabled, the clients will renew their lease about every minute until the SM has the DNS information to give out. At this point the SM will go to the full configured lease time period which is 30 days by default. With DNS Server Proxy enabled, the SM will give out full term leases with its NAT LAN IP as the DNS server.
DNS IP Address	<p>Select either:</p> <p>Obtain Automatically to allow the system to set the IP address of the DNS server</p> <p><i>or</i></p> <p>Set Manually to enable yourself to set both a preferred and an alternate DNS IP address.</p>
Preferred DNS IP Address	Enter the preferred DNS IP address to use when the DNS IP Address parameter is set to Set Manually .
Alternate DNS IP	Enter the DNS IP address to use when the DNS IP Address parameter is

Address	set to Set Manually and no response is received from the preferred DNS IP address.
Remote Management Interface	<p>To offer greater flexibility in IP address management, the NAT-enabled SM's configured WAN Interface IP address may now be used as the device Remote Management Interface (unless the SM's PPPoE client is set to Enabled)</p> <p>Disable: When this interface is set to "Disable", the SM is not directly accessible by IP address. Management access is only possible through either the LAN (Ethernet) interface or a link from an AP web page into the WAN (RF-side) interface.</p> <p>Enable (Standalone Config): When this interface is set to "Enable (Standalone Config)", to manage the SM/BHS the device must be accessed by the IP addressing information provided in the Remote Configuration Interface section.</p> <hr/> <p> Note When configuring PPPoE over the link, use this configuration option (PPPoE traffic is routed via the IP addressing specified in section Remote Configuration Interface).</p> <hr/> <p>Enable (Use WAN Interface): When this interface is set to "Enable (Use WAN Interface)", the Remote Configuration Interface information is greyed out, and the SM is managed via the IP addressing specified in section WAN Interface).</p> <hr/> <p> Note When using this configuration, the ports defined in section Configuration, Port Configuration are consumed by the device. For example, if FTP Port is configured as 21 by the SM, an FTP server situated below the SM must use a port other than 21. This also applies to DMZ devices; any ports specified in section Configuration, Port Configuration will not be translated through the NAT, they are consumed by the device's network stack for management.</p> <hr/>
Connection Type	<p>This parameter can be set to:</p> <p>Static IP—when this is the selection, all three parameters (IP Address, Subnet Mask, and Gateway IP Address) must be properly populated.</p> <p>DHCP—when this is the selection, the information from the DHCP server configures the interface.</p>
IP Address	If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the IP address of the SM for RF management traffic.
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 for RF management

	traffic.
Gateway IP Address	<p>If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the gateway IP address for the SM for RF management traffic.</p> <p>Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.</p>
DHCP DNS IP Address	<p>Select either:</p> <p>Obtain Automatically to allow the system to set the IP address of the DNS server.</p> <p><i>or</i></p> <p>Set Manually to enable yourself to set both a preferred and an alternate DNS IP address.</p>
Preferred DNS Server	Enter the preferred DNS IP address to use when the DNS IP Address parameter is set to Set Manually .
Alternate DNS Server	Enter the DNS IP address to use when the DNS IP Address parameter is set to Set Manually and no response is received from the preferred DNS IP address.
Domain Name	Domain Name to use for management DNS configuration. This domain name may be concatenated to DNS names used configured for the remote configuration interface.
ARP Cache Timeout	If a router upstream has an ARP cache of longer duration (as some use 30 minutes), enter a value of longer duration than the router ARP cache. The default value of this field is 20 (minutes).
TCP Session Garbage Timeout	Where a large network exists behind the SM, you can set this parameter to lower than the default value of 120 (minutes). This action makes additional resources available for greater traffic than the default value accommodates.
UDP Session Garbage Timeout	You may adjust this parameter in the range of 1 to 1440 minutes, based on network performance. The default value of this parameter is 4 (minutes).

NAT DNS Considerations - SM

SM DNS behavior is different depending on the accessibility of the SM. When NAT is enabled the DNS configuration that is discussed in this document is tied to the RF Remote Configuration Interface, which must be enabled to utilize DNS Client functionality. Note that the WAN DNS settings when NAT is enabled are unchanged with the addition of the management DNS feature discussed in this document.

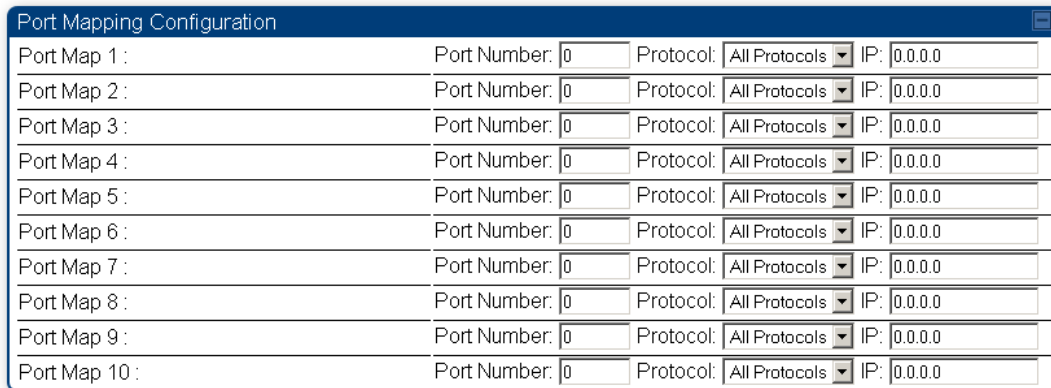
Table 81 SM DNS Options with NAT Enabled

NAT Configuration	Management Interface Accessibility	DHCP Status	DNS Status
NAT Enabled	RF Remote Management Interface Disabled	N/A	DNS Disabled
	RF Remote Management Interface Enabled	DHCP Disabled	DNS Static Configuration
		DHCP Enabled	DNS from DHCP or DNS Static Configuration

NAT Port Mapping tab - SM

The NAT Port Mapping tab of the SM is explained in [Table 82](#).

Table 82 NAT Port Mapping attributes - SM



Attribute	Meaning
Port Map 1 to 10	Separate parameters allow you to distinguish NAT ports from each other by assigning a unique combination of port number, protocol for traffic through the port, and IP address for access to the port

DHCP – BHS

Applicable products

PTP: BHM

DHCP enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the Cambium system.

In conjunction with the NAT features, each BHS provides:

- A DHCP server that assigns IP addresses to computers connected to the BHS by Ethernet protocol.
- A DHCP client that receives an IP address for the BHS from a network DHCP server.

Reconnecting to the management PC

If the IP Address, Subnet Mask and Gateway IP Address of the unit have been updated to meet network requirements, then reconfigure the local management PC to use an IP address that is valid for the network. See [Configuring the management PC](#) on page 7-3.

Once the unit reboots, log in using the new IP address. See [Logging into the web interface](#) on page 7-5.

VLAN Remarking and Priority bits configuration – AP/SM

Applicable products

PMP : AP SM

VLAN Remarking

VLAN Remarking feature allows the user to change the VLAN ID and priority of both upstream and downstream packets at the Ethernet Interface. The remarking configuration is available for:

1. VLAN ID re-marking
2. 802.1p priority re-marking



Note

For Q-in-Q VLAN tagged frame, re-marking is performed on the outer tag.

VLAN ID Remarking

SM supports the ability to re-mark the VLAN ID on both upstream and downstream VLAN frames at the Ethernet interface. For instance, a configuration can be added to re-mark VLAN ID 'x' to VLAN ID 'y' as shown in [Table 83](#). AP does not support VLAN ID remarking.

Table 83 VLAN Remarking Example

VLAN frame direction	Remarking
Upstream	SM receives VLAN ID 'x' frame at the Ethernet interface, checks the configuration and re-marks to VLAN ID 'y'. So VLAN ID 'y' frame comes out of AP's Ethernet interface. When SM re-marks, a dynamic entry in VLAN membership table for 'y' is added to allow reception of VLAN ID 'y' downstream packet.
Downstream	AP receives VLAN ID 'y' frame at the Ethernet interface and sends to SM. SM accepts the frame as it has an entry in the membership table and re-marks to VLAN ID 'x'. This reverse re-marking is necessary because the downstream devices do not know of re-marking and are expecting VLAN 'x' frames. This remarking is done just before sending the packet out on Ethernet interface.

802.1P Remarking

AP/BHM and SM/BHS allow re-marking of 802.1p priority bits for the frames received at the Ethernet interface. Priority bits are not re-marked for the packets sent out of Ethernet interface (reverse direction).

Configuration must be added at SM/BHS for upstream frames and at AP/BHM for downstream frames.

VLAN Priority Bits configuration

VLAN Priority Bits Configuration feature allows the user to configure the three 802.1p bits upon assigning VLAN to an ingress packet. The priority bits configuration is available for:

- Default Port VID
- Provider VID
- MAC Address mapped Port VID
- Management VID

Default Port VID

This VID is used for untagged frames and will correspond to the Q-Tag for 802.1Q frames (if VLAN Port Type is Q), or the C-Tag for 802.1ad frames (if the VLAN Port Type is QinQ).

The priority bits used in the Q-tag/C-tag are configurable.

The configuration can be:

- **Promote IPv4/IPv6 priority** – The priority in the IP header is copied to the Q-tag/C-tag.
- **Define priority** – Specify the priority in the range of 0 to 7. This value is used as priority in the Q-tag/C-tag.

MAC Address Mapped VID

If a packet arrives at the SM/BHS that is sourced from a device whose MAC address is in the table, then the corresponding VID is used for that frame's Q-tag (Q port) or C-tag (QinQ port). The priority bits used in the Q-tag/C-tag are configurable similar to default port VID.

Provider VID

The provider VID is used for the S-tag. The priority bits used in the S-tag are configurable similar to default port VID. Provider VID has an extra priority configuration:

- **Copy inner tag 802.1p priority** – The priority in the C-tag is copied to the S-tag.

Management VID

This VID is used to communicate with AP/BHM and SM/BHS for management purposes. The priority bits used in the Q-tag are configurable similar to default port VID.

VLAN page of AP

The VLAN tab of the AP/BHM is explained in [Table 84](#).

Table 84 AP/BHM VLAN tab attributes

Attribute	Meaning
VLAN	Specify whether VLAN functionality for the AP and all linked SMs must (Enabled) or may not (Disabled) be allowed. The default value is Disabled .
Always use Local VLAN Config	Enable this option before you reboot this AP as a SM to use it to perform spectrum analysis. Once the spectrum analysis completes, disable this option before you reboot the module as an AP,
Allow Frame Types	Select the type of arriving frames that the AP must tag, using the VID that is stored in the Untagged Ingress VID parameter. The default value is All Frames .
Dynamic Learning	Specify whether the AP must (Enabled) or not (Disabled) add the VLAN IDs (VIDs) of upstream frames to the VID table. (The AP passes frames with VIDs that are stored in the table both upstream and downstream.). The default value is Enabled .
VLAN Aging Timeout	Specify how long the AP must keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is 25 (minutes).


**Note**

VIDs that you enter for the Management VID and VLAN Membership parameters do not time out.


Management VID	Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4095. The default value is 1.								
QinQ EtherType	<p>Modules can be configured with 802.1ad Q-in-Q DVLAN (Double-VLAN) tagging which is a way for an operator to put an 802.1Q VLAN inside of an 802.1ad VLAN. A nested VLAN, which is the original 802.1Q tag and a new second 802.1ad tag, allows for bridging of VLAN traffic across a network and segregates the broadcast domains of 802.1Q VLANs. Q-in-Q can be used with PPPoE and/or NAT.</p> <p>The 802.1ad standard defines the S-VLAN as the Service Provider VLAN and the C-VLAN as the customer VLAN. The radio software does 2 layer Q-in-Q whereby the C-VLAN is the 802.1Q tag and the S-VLAN is the second layer Q tag as shown below:</p> <p>Table 85 Q-in-Q Ethernet frame</p> <table border="1"> <thead> <tr> <th>Ethernet Header</th> <th>S-VLAN EthType 0x88a8</th> <th>C-VLAN EthType 0x8100</th> <th>IP Data EthType 0x0800</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>The 802.1ad S-VLAN is the outer VLAN that is configurable on the Configuration > VLAN web page of the AP. The Q-in-Q EtherType parameter is configured with a default EtherType of 0x88a8 in addition to four alternate EtherTypes that can be configured to aid in interoperability with existing networks that use a different EtherType than the default.</p> <p>The C-VLAN is the inner VLAN tag, which is the same as 802.1Q. As a top level concept, this operates on the outermost tag at any given time, either “pushing” a tag on or “popping” a tag off. This means packets will at most transition from an 802.1Q frame to an 801.ad frame (with a tag “pushed” on) or an untagged 802.1 frame (with the tag “popped” off). Similarly, for an 802.1ad frame, this can only transition from an 802.1ad frame to an 802.1Q frame (with the tag “popped” off) since the radio software only supports 2 levels of tags</p>	Ethernet Header	S-VLAN EthType 0x88a8	C-VLAN EthType 0x8100	IP Data EthType 0x0800				
Ethernet Header	S-VLAN EthType 0x88a8	C-VLAN EthType 0x8100	IP Data EthType 0x0800						
VLAN Not Active	When VLAN is enabled in the AP, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.								
VLAN Membership Table Configuration	For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the Add Member button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID								

and then click the **Remove Member** button.

VLAN Membership table	This field lists the VLANs that an AP is a member of. As the user adds a number between 1 and 4094, this number is populated here.
Source VLAN (Range: 1-4094)	Enter the VID for which the operator wishes to remark the 802.1p priority for the downstream packets. The range of values is 1 to 4094. The default value is 1.
Remark Priority (Range 0-7)	This is the priority you can assign to the VLAN Tagged packet. Priority of 0 is the highest.
VLAN Remarking table	As the user enters a VLAN and a Remarking priority, this information is added in this table.

Accept QinQ Frames	This option is valid for the Q-in-Q port so that the user may force blocking of existing 802.1ad Q-in-Q frames. This way, only untagged or single tagged packets will come in and out of the Ethernet interface. If a Q-in-Q frame is about ingress or egress the Ethernet interface and this is disabled, it is dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.
Allow Frame Types	Select the type of arriving frames that the SM must tag, using the VID that is stored in the Untagged Ingress VID parameter. The default value is All Frames . Tagged Frames Only: The SM only tags incoming VLAN-tagged frames Untagged Frames Only: The SM will only tag incoming untagged frames
Dynamic Learning	Specify whether the SM must (Enable) or not (Disable) add the VIDs of upstream frames (that enter the SM through the wired Ethernet interface) to the VID table. The default value is Enable .
VLAN Aging Timeout	Specify how long the SM/BHS must keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is 25 (minutes).
	 <p>Note VIDs that you enter for the Untagged Ingress VID and Management VID parameters do not time out.</p>
Management VID	Enter the VID that the SM/BHS must share with the AP/BHM. The range of values is 1 to 4095. The default value is 1.
SM Management VID Pass-through	Specify whether to allow the SM/BHS (Enabled) or the AP/RADIUS (Disabled) to control the VLAN settings of this SM. The default value is Enabled . When VLAN is enabled in the AP to whom this SM is registered, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not. If disabled, MVID traffic is not allowed to or from the SM wired interface. Also, if Management VID is the same as a Port VID (Default or MAC-based), then this setting is ignored and assumed to be Enabled.
Default Port VID	This is the VID that is used for untagged frames and will correspond to the Q-Tag for 802.1Q frames (if VLAN Port Type is Q), or the C-Tag for 802.1ad frames (if the VLAN Port Type is Q-in- Q).
Port VID MAC Address Mapping	These parameters allow operators to place specific devices onto different VLANs (802.1Q tag or 802.1ad C-tag) based on the source MAC address of the packet. If the MAC address entry is 00-00-00-00-00-00 then that entry is not used. If a packet arrives at the SM that is sourced from a device whose MAC address is in the table, then the

	<p>corresponding VID is used for that frame's Q-tag (Q port) or C-tag (Q-in-Q port). If there is no match, then the Default Port VID is used. This table is also used in the downstream direction for removal of the tag based on the destination MAC address so that an untagged (for Q port) or Q-Tagged (for Q-in-Q port) frame is delivered to the end device. You may use wildcards for the non-OUI (Organizationally Unique Identifier) portion of the MAC address, which is the last 3 bytes. MAC addresses contain 6 bytes, the first 3 of which are the OUI of the vendor that manufactured the device and the last 3 are unique to that vendor OUI. If you want to cover all devices from a known vendor's OUI, you have to specify 0xFF for the remaining 3 bytes. So, for example, if you wanted all devices from a specific vendor with an OUI of 00-95-5b (which is a Netgear OUI) to be on the same VID of 800, you have to specify an entry with MAC address 00-95-5b-ff-ff-ff. Then, any device underneath of the SM with MAC addresses starting with 00-95-5b is put on VLAN 800.</p>
Provider VID	The provider VID is used for the S-tag. It is only used if the Port Type is Q-in-Q and will always be used for the S-tag. If an existing 802.1Q frame arrives, the Provider VID is what is used for adding and removing of the outer S-tag. If an untagged frame arrives to a Q-in-Q port, then the Provider VID is the S-tag and the Default Port VID (or Port VID MAC Address Mapping , if valid) is used for the C-tag.
Active Configuration, Default Port VID	This is the value of the parameter of the same name, configured above.
Active Configuration, MAC Address VID Map	This is the listing of the MAC address VIDs configured in Port VID MAC Address Mapping .
Active Configuration, Management VID	This is the value of the parameter of the same name, configured above.
Active Configuration, SM Management VID Pass-Through	This is the value of the parameter of the same name, configured above.
Active Configuration, Dynamic Aging Timeout	This is the value of the VLAN Aging Timeout parameter configured above.
Active Configuration, Allow Learning	Yes is displayed if the value of the Dynamic Learning parameter above is Enabled . No is displayed if the value of Dynamic Learning is Disabled .
Active Configuration, Allow Frame Type	This displays the selection that was made from the drop-down list at the Allow Frame Types parameter above.
Active Configuration, QinQ	This is set to Enabled if VLAN Port Type is set to QinQ , and is set to Disabled if VLAN Port Type is set to Q .

Active Configuration, QinQ EthType	This is the value of the QinQ EtherType configured in the AP.
Active Configuration, Allow QinQ Tagged Frames	This is the value of Accept QinQ Frames , configured above.
Active Configuration, Current VID Member Set, VID Number	This column lists the ID numbers of the VLANs in which this module is a member, whether through assignment or through dynamic learning.
Active Configuration, Current VID Member Set, Type	<p>For each VID number in the first column, the entry in this column correlates the way in which the module became and continues to be a member:</p> <p>Permanent—This indicates that the module was assigned the VID number through direct configuration by the operator.</p> <p>Dynamic—This indicates that the module adopted the VID number through enabled dynamic learning, when a tagged packet from a SM behind it in the network or from a customer equipment that is behind the SM in this case, was read.</p>
Active Configuration, Current VID Member Set, Age	<p>For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:</p> <p>Permanent type - Number never times out and this is indicated by the digit 0.</p> <p>Dynamic type - Age reflects what is configured in the VLAN Aging Timeout parameter in the Configuration => VLAN tab of the AP or reflects a fewer number of minutes that represents the difference between what was configured and what has elapsed since the VID was learned. Each minute, the Age decreases by one until, at zero, the AP deletes the learned VID, but can it again from packets sent by elements that are beneath it in the network.</p>
<div data-bbox="518 1371 613 1451" style="display: inline-block; vertical-align: middle;"></div> <div data-bbox="646 1371 1414 1568" style="display: inline-block; vertical-align: middle;"> <p>Note</p> <p>Values in this Active Configuration block can differ from attempted values in configurations:</p> <p>The AP can override the value that the SM has configured for SM Management VID Pass-Through.</p> </div>	

VLAN Membership tab of SM

The **Configuration > VLAN > VLAN Membership** tab is explained in [Table 87](#).

Table 87 SM VLAN Membership attributes

The screenshot shows two panels. The top panel, titled "VLAN Membership Configuration", contains a text input field with the value "10" and a range indicator "(Range : 1 — 4094)". Below the input field are two buttons: "Add Member" and "Remove Member". The bottom panel, titled "VLAN Membership Table", displays a table with the following content:

VLAN Membership Table VID	Number	Type	Age
10	Static		

Attribute	Meaning
VLAN Membership Table Configuration	For each VLAN in which you want the AP to be a member, enter the VLAN ID and then click the Add Member button. Similarly, for any VLAN in which you want the AP to no longer be a member, enter the VLAN ID and then click the Remove Member button.

VLAN configuration for PTP

Applicable products

PTP: BHM BMS

VLAN page of BHM

The VLAN tab of BHS is explained in [Table 88](#).

Table 88 BHM VLAN page attributes

The screenshot shows two panels from a network configuration interface. The top panel, titled 'VLAN Configuration', contains the following fields and values:

- VLAN :** Enabled, Disabled
- VLAN Port Type :** Q
- Accept QinQ Frames :** Enabled, Disabled
- Management VID (Range : 1 — 4094) :** 1, Priority 0, (0 — 7), Promote IPv4/IPv6 priority
- Default Port VID (Range : 1 — 4094) :** 1, Priority 0, (0 — 7), Promote IPv4/IPv6 priority
- QinQ EtherType :** 0x88a8

The bottom panel, titled 'Active Configuration', displays the current state of the configuration:

- Default Port VID : 1 Priority : Promote IPv4/IPv6 priority
- Management VID : 1 Priority : Promote IPv4/IPv6 priority
- QinQ : Disabled
- QinQ EthType : 0x88a8
- Allow QinQ Tagged Frames : No
- Current VID Member Set:

VID Number	Type	Age
1	Permanent	0

Attribute	Meaning
VLAN	Specify whether VLAN functionality for the BHM and all linked BHS must be (Enabled) or may not (Disabled) be allowed. The default value is Disabled .
VLAN Port Type	By default this is Q, indicating that it is to operate in the existing manner. The other option is Q-in-Q, which indicates that it must be adding and removing the S-Tag, and adding a C-Tag if necessary for untagged packets. The VLAN Port type corresponds to the Ethernet port of the BHS. Currently, the internal management interfaces will always operate as Q ports.
Accept QinQ Frames	This option is valid for the Q-in-Q port so that the user may force blocking of existing 802.1ad Q-in-Q frames. This way, only untagged or single tagged packets will come in and out of the Ethernet interface. If a Q-in-Q frame is about ingress or egress the Ethernet interface and this is disabled, it is dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.
Management VID (Range 1-4094)	Enter the VID that the BHS must share with the BHM. The range of values is 1 to 4095. The default value is 1.
Default Port VID (Range 1-4094)	This is the VID that is used for untagged frames and corresponds to the Q-Tag for 802.1Q frames (if VLAN Port Type is Q), or the C-Tag for 802.1ad frames (if the VLAN Port Type is Q-in- Q).
QinQ Ether Type	Modules can be configured with 802.1ad Q-in-Q DVLAN (Double-VLAN) tagging which is a way for an operator to put an 802.1Q VLAN inside of

an 802.1ad VLAN. A nested VLAN, which is the original 802.1Q tag and a new second 802.1ad tag, allows for bridging of VLAN traffic across a network and segregates the broadcast domains of 802.1Q VLANs. Q-in-Q can be used with PPPoE and/or NAT.

The 802.1ad standard defines the S-VLAN as the Service Provider VLAN and the C-VLAN as the customer VLAN. The radio software does 2 layer Q-in-Q whereby the C-VLAN is the 802.1Q tag and the S-VLAN is the second layer Q tag as shown below:

Ethernet Header	S-VLAN EthType 0x88a8	C-VLAN EthType 0x8100	IP Data EthType 0x0800
-----------------	--------------------------	--------------------------	---------------------------

The 802.1ad S-VLAN is the outer VLAN that is configurable on the **Configuration > VLAN** web page of the BHM. The Q-in-Q EtherType parameter is configured with a default EtherType of 0x88a8 in addition to four alternate EtherTypes that can be configured to aid in interoperability with existing networks that use a different EtherType than the default.

The C-VLAN is the inner VLAN tag, which is the same as 802.1Q. As a top level concept, this operates on the outermost tag at any given time, either “pushing” a tag on or “popping” a tag off. This means packets will at most transition from an 802.1Q frame to an 801.ad frame (with a tag “pushed” on) or an untagged 802.1 frame (with the tag “popped” off). Similarly, for an 802.1ad frame, this can only transition from an 802.1ad frame to an 802.1Q frame (with the tag “popped” off) since the radio software only supports 2 levels of tags.

VLAN Not Active

When VLAN is enabled in the BHM, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

VLAN page of BHS

The VLAN tab of BHS is explained in [Table 89](#).

Table 89 BHS VLAN page attributes

The screenshot shows the BHS configuration interface. The 'VLAN Configuration' section includes the following settings:

- VLAN :** Enabled, Disabled
- VLAN Port Type :** Q
- Accept QinQ Frames :** Enabled, Disabled
- Management VID (Range : 1 — 4094) :** 1, Priority 0 (0 — 7), Promote IPv4/IPv6 priority
- Default Port VID (Range : 1 — 4094) :** 1, Priority 0 (0 — 7), Promote IPv4/IPv6 priority

The 'Active Configuration' section below shows 'VLAN Not Active'.

Attribute	Meaning
VLAN	Specify whether VLAN functionality for the BHM and all linked BHS must be (Enabled) or may not (Disabled) be allowed. The default value is Disabled.
VLAN Port Type	By default this is Q, indicating that it is to operate in the existing manner. The other option is Q-in-Q, which indicates that it must be adding and removing the S-Tag, and adding a C-Tag if necessary for untagged packets. The VLAN Port type corresponds to the Ethernet port of the BHS. Currently, the internal management interfaces will always operate as Q ports.
Accept QinQ Frames	This option is valid for the Q-in-Q port so that the user may force blocking of existing 802.1ad Q-in-Q frames. This way, only untagged or single tagged packets will come in and out of the Ethernet interface. If a Q-in-Q frame is about ingress or egress the Ethernet interface and this is disabled, it is dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.
Management VID (Range 1-4094)	Enter the VID that the BHS must share with the BHM. The range of values is 1 to 4095. The default value is 1.
Default Port VID (Range 1-4094)	This is the VID that is used for untagged frames and corresponds to the Q-Tag for 802.1Q frames (if VLAN Port Type is Q), or the C-Tag for 802.1ad frames (if the VLAN Port Type is Q-in-Q).
VLAN Not Active	When VLAN is enabled in the BHM, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

PPPoE page of SM

Applicable products	PMP :	<input checked="" type="checkbox"/> SM
----------------------------	--------------	--

Point-to-Point Protocol over Ethernet (PPPoE) is a protocol that encapsulates PPP frames inside Ethernet frames (at Ethernet speeds). Benefits to the network operator may include

- Access control
- Service monitoring
- Generation of statistics about activities of the customer
- Re-use of infrastructure and operational practices by operators who already use PPP for other networks

PPPoE options are configurable for the SM only, and the AP indicates whether or not PPPoE is enabled for a specific subscriber.

When PPPoE is enabled, once the RF session comes up between the SM and the AP, the SM will immediately attempt to connect to the PPPoE Server. You can monitor the status of this by viewing the PPPoE Session Log in the Logs section (Administrator only). Every time the RF session comes up, the SM will check the status of the link and if it is down, the SM will attempt to redial the link if necessary depending on the Timer Type. Also, on the Configuration page, the user may 'Connect' or 'Disconnect' the session manually. This can be used to override the session to force a manual disconnect and/or reconnect if there is a problem with the session.

In order to enable PPPoE, NAT MUST be enabled on the SM and Translation Bridging MUST be disabled on the AP. These items is strictly enforced for you when you are trying to enable PPPoE. A message will indicate any prerequisites not being met. Also, the NAT Public IP DHCP client cannot be enabled, because the NAT Public IP is received through the IPCP process of the PPPoE discovery stages.

The pre-requisites are:

- NAT MUST be enabled on the SM
 - NAT DHCP Client is disabled automatically. The NAT public IP is received from the PPPoE Server.
 - NAT Public Network Interface Configuration will not be used and must be left to defaults. Also NAT Public IP DHCP is disabled if it is enabled.
- Translation Bridging MUST be DISABLED on the AP
 - This will only be determined if the SM is in session since the SM won't know the AP configuration otherwise. If the SM is not in session, PPPoE can be enabled but if the SM goes into session to a Translation Bridge-enabled AP, then PPPoE will not be enabled.

The PPPoE configuration parameters are explained in [Table 90](#).

Table 90 SM PPPoE attributes

The screenshot shows the 'PPPoE Configuration' window with the following settings:

- PPPoE : Enabled, Disabled
- NAT DHCP Client will be disabled.
- Access Concentrator : []
- Service Name : []
- Authentication Type : None
- User Name : admin
- Password : []
- MTU : Use MTU Received from PPPoE Server, Use User Defined MTU (1492)
- Timer Type : Keep Alive
- Timer Period : 30 seconds (20s Minimum)
- TCP MSS Clamping : Enabled, Disabled

Attribute	Meaning
Access Concentrator	An optional entry to set a specific access concentrator to connect to for the PPPoE session. If this is blank, the SM will accept the first access concentrator which matches the service name (if specified). This is limited to 32 characters.
Service Name	An optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the SM will accept the first service option that comes back from the access concentrator specified above, if any. This is limited to 32 characters.
Authentication Type	None means that no PPPoE authentication is implemented CHAP/PAP means that CHAP authentication is attempted first, then PAP authentication. The same password is used for both types.
User Name	This is the CHAP/PAP user name that is used if CHAP/PAP authentication is selected. If None is selected for authentication then this field is unused. This is limited to 32 characters.
Password	This is the CHAP/PAP password that is used if PAP authentication is selected. If None is selected for authentication then this field is unused. This is limited to 32 characters.
MTU	Use MTU Received from PPPoE Server causes the SM to use the MRU of the PPPoE server received in LCP as the MTU for the PPPoE link. Use User Defined MTU allows the operator to specify an MTU value to use to override any MTU that may be determined in the LCP phase of PPPoE session setup. If this is selected, the user is able to enter an MTU value up to 1492. However, if the MTU determined in LCP negotiations is

	less than this user-specified value, the SM will use the smaller value as its MTU for the PPPoE link.
Timer Type	<p>Keep Alive is the default timer type. This timer will enable a keepalive that will check the status of the link periodically. The user can set a keepalive period. If no data is seen from the PPPoE server for that period, the link is taken down and a reconnection attempt is started. For marginal links, the keep alive timer can be useful so that the session will stay alive over periodic dropouts. The keepalive timer must be set such that the session can outlast any session drop. Some PPPoE servers will have a session check timer of their own so that the timeouts of the server and the SM are in sync, to ensure one side does not drop the session prematurely.</p> <p>Idle Timeout enables an idle timer that checks the usage of the link from the customer side. If there is no data seen from the customer for the idle timeout period, the PPPoE session is dropped. Once data starts flowing from the customer again, the session is started up again. This timer is useful for users who may not be using the connection frequently. If the session is idle for long periods of time, this timer will allow the resources used by the session to be returned to the server. Once the connection is used again by the customer, the link is reestablished automatically.</p>
Timer Period	The length in seconds of the PPPoE keepalive timer.
TCP MSS Clamping	If this is enabled, then the SM will alter TCP SYN and SYN-ACK packets by changing the Maximum Segment Size to be compatible with the current MTU of the PPPoE link. This way, the user does not have to worry about MTU on the client side for TCP packets. The MSS is set to the current MTU – 40 (20 bytes for IP headers and 20 bytes for TCP headers). This will cause the application on the client side to not send any TCP packets larger than the MTU. If the network is exhibiting large packet loss, try enabling this option. This may not be an option on the PPPoE server itself. The SM will NOT reassemble IP fragments, so if the MTUs are incorrect on the end stations, then MSS clamping will solve the problem for TCP connections.

IP4 and IPv6

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

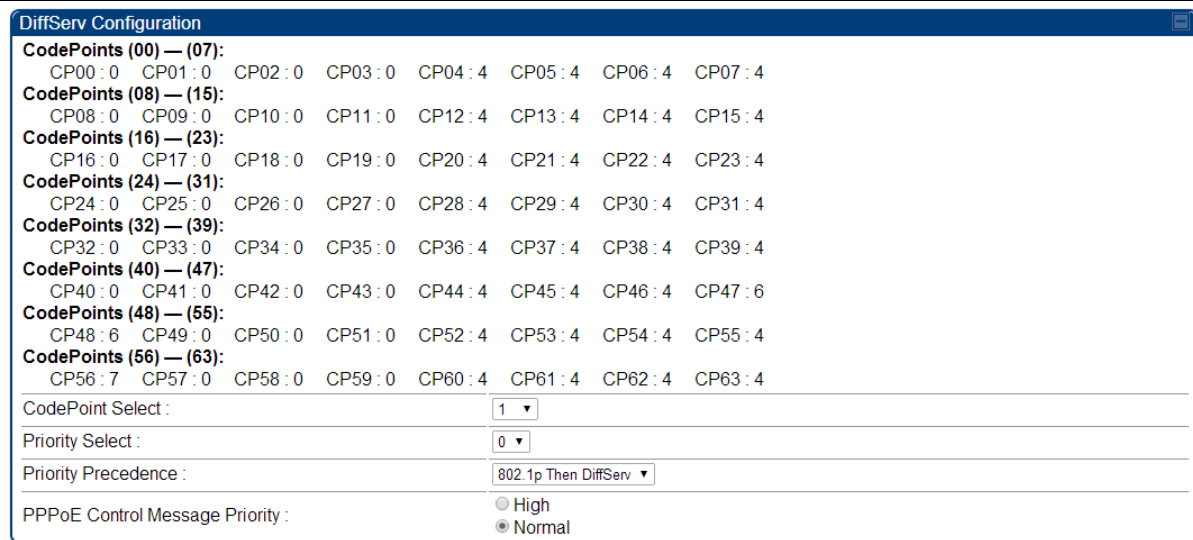
IPv4 and IPv6 Prioritization

PMP/PTP 450 platform provides operators the ability to prioritize IPv6 traffic in addition to IPv4 traffic. IPv6/IPv4 prioritization can be configured by selecting a CodePoint and the corresponding priority from the GUI of the AP/BHM and the IPv6/IPv4 packet is set up accordingly. There is no GUI option for selecting IPv6 or IPv4 priority. Once the priority is set, it is set for IPv4 and IPv6 packets.

Configuring IPv4 and IPv6 Priority

IPv4 and IPv6 prioritization is set using the DiffServ tab on the AP/BHM and SM/BHS (located at **Configuration > DiffServ**). A priority set to a specific CodePoint will apply to both IPv4 and IPv6 traffic.

Table 91 DiffServ attributes – AP/BHM



Attribute	Meaning
CodePoint 1 through CodePoint 47	Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high- priority channel. The mappings are the same as 802.1p VLAN priorities.
CodePoint 49 through CodePoint 55	Consistent with RFC 2474 CodePoint 0 is predefined to a fixed priority value of 0 (low-priority channel).
CodePoint 57 through CodePoint	CodePoint 48 is predefined to a fixed priority value of 6 (high-priority channel). CodePoint 56 is predefined to a fixed priority value of 7 (high-priority channel).

63	Operator cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high or low priority channel) are set in the AP/BHM for all downlinks within the sector and in the SM/BHS for each uplink.
CodePoint Select	This represents the CodePoint Selection to be modified via Priority Select
Priority Select	The priority setting input for the CodePoint selected in CodePoint Select
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 AP/BHM to utilize the high priority channel for PPPoE control messages. Configuring the AP/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 AP/BHM.

IPv4 and IPv6 Filtering

The operator can filter (block) specified IPv6 protocols including IPv4 and ports from leaving the AP/BHM and SM/BHS and entering the network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other.

Configuring IPv4 and IPv6 Filtering

IPv6 filters are set using the Protocol Filtering tab on the AP/BHM and SM/BHS (at **Configuration > Protocol Filtering**). Once a filter is set for a packet type, those packets will not be sent over the RF interface depending on "Filter Direction" setting.

Table 92 Packet Filter Configuration 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 : (Decimal Value)

TCP : Enabled
 Disabled

UDP : Enabled
 Disabled

Port #2 : (Decimal Value)

TCP : Enabled
 Disabled

UDP : Enabled
 Disabled

Port #3 : (Decimal Value)

TCP : Enabled
 Disabled

UDP : Enabled
 Disabled

AP Specialty Filters

RF Telnet Access : Enabled
 Disabled

PPPoE PADI Downlink Forwarding : Enabled
 Disabled

Attribute	Meaning
Packet Filter Types	<p>For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type.</p> <p>To filter packets in any of the user-defined ports, you must do all of the following:</p> <ul style="list-style-type: none"> Check the box for User Defined Port <i>n</i> (See Below) in the Packet Filter Types section of this tab.

	<ul style="list-style-type: none">• Provide a port number at Port #n. in the User Defined Port Filtering Configuration section of this tab• 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.

Upgrading the software version and using CNUT

This section consists of the following procedures:

- [Checking the installed software version](#) on page 7-67
- [Upgrading to a new software version](#) on page 7-67



Caution

If the link is operational, ensure that the remote end of the link is upgraded first using the wireless connection, and then the local end can be upgraded. Otherwise, the remote end may not be accessible.

Use CNUT 4.9.12 or later version and always refer to the software release notes before upgrading system software. The release notes are available at:

<https://support.cambiumnetworks.com/files/pmp450>

<https://support.cambiumnetworks.com/files/ptp450>

Checking the installed software version

To check the installed software version, follow these instructions:

Procedure 17 Checking the installed software version

- 1 Click on **General** tab under **Home** menu.
- 2 Note the installed Software Version (under Device Information):
PMP/PTP 450/450i

Software Version :	CANOPY 14.1.1 AP-DES
--------------------	----------------------
- 3 Go to the support website (see [Contacting Cambium Networks](#) on page 1) and find Point-to-Multipoint software updates. Check that the latest PMP/PTP 450 platform software version is the same as the installed Software Version.
- 4 To upgrade software to the latest version, see [Upgrading to a new software version](#) on page 7-67.

Upgrading to a new software version

PMP/PTP 450i modules are upgraded using the Canopy Network Updater Tool. The Canopy Network Updater Tool (CNUT) manages and automates the software and firmware upgrade process for a Canopy radio, or CMM4 (but not its 14-port switch) across the network. This eliminates the need for an administrator to visit each radio in the network (or each AP/BHM while using the Autoupdate feature) to upgrade the modules.

**Note**

Please ensure that you have the most up-to-date version of CNUT by browsing to the Customer Support Web Page located:

<http://www.cambiumnetworks.com/support/management-tools/cnut>

This section includes an example of updating a single unit before deployment. System-wide upgrading procedures may be found in the *CNUT Online Help* manual, which can be found on the Cambium support website (see [Contacting Cambium Networks](#) on page 1).

CNUT functions

The Canopy Network Updater tool has the following functions:

- Automatically discovers all network elements
- Executes a UDP command that initiates and terminates the Auto-update mode within APs/BHMs. This command is both secure and convenient:
 - For security, the AP/BHM accepts this command from only the IP address that you specify in the Configuration page of the AP/BHM.
 - For convenience, Network Updater automatically sets this Configuration parameter in the APs/BHMs to the IP address of the Network Updater server when the server performs any of the update commands.
- CNUT supports HTTP and HTTPS
- Allows you to choose the following among updating:
 - Your entire network.
 - Only elements that you select.
 - Only network branches that you select.
- Provides a Script Engine that you can use with any script that:
 - You define.
 - Cambium supplies.
- Configurability of any of the following to be the file server for image files:
 - The AP/BHM, for traditional file serving via UDP commands and monitoring via UDP messaging
 - CNUT HTTP/HTTPS Server, for upgrading via SNMP commands and monitoring via SNMP messaging. This also supports an option to either set the image order specifically for this file server or to allow the AP to determine the order.
 - Local TFTP Server, for traditional file serving via UDP commands and monitoring via UDP messaging. This supports setting the number of simultaneous image transfers per AP/BHM
- The capability to launch a test of connectivity and operational status of the local HTTP, HTTPS and TFTP file servers
- An interface that supports efficient specification of the proper IP address for the local file server(s) where Network Updater resides on a multi-homed computer
- An md5 checksum calculator utility for identifying corruption of downloaded image files before Network Updater is set to apply them.

Network element groups

With the Canopy Network Updater Tool, you can identify element groups composed of network elements that you select. Identifying these element groups does the following:

- Organizes the display of elements (for example, by region or by AP/BHM cluster).
- Allows to:
 - Perform an operation on all elements in the group simultaneously.
 - Set group-level defaults for ftp password access and SNMP Community String (defaults that can be overridden in an individual element when necessary).

Network layers

A typical network contains multiple layers of elements, with each layer farther from the Point of Presence. For example, SMs (or BHS) are behind an AP/BHM and thus, in this context, at a lower layer than the AP/BHM. Correctly portraying these layers in Network Updater is essential so that Network Updater can perform radio and AP/BHM cluster upgrades in an appropriate order.

Script engine

Script Engine is the capability in Network Updater that executes any user-defined script against any network element or element group. This capability is useful for network management, especially for scripts that you repetitively execute across your network.

The Autodiscovery capability in Network Updater finds all of your network elements.

This comprehensive discovery:

- Ensures that, when you intend to execute a script against *all* elements, the script is indeed executed against *all* elements.
- Maintains master lists of elements (element groups) against which you selectively execute scripts.

The following scripts are included with CNUT:

- Gather Customer Support Information
- Set Access Point Authentication Mode
- Set Autoupdate Address on APs/BHMs
- Set SNMP Accessibility
- Reset Unit

Software dependencies for CNUT

CNUT functionality requires

- one of the following operating systems
 - Windows® 2000
 - Windows Server 2003
 - Windows 7 and Windows 8
 - Windows XP or XP Professional
 - Red Hat Enterprise Linux (32-bit) Version 4 or 5
- Java™ Runtime Version 2.0 or later (installed by the CNUT installation tool)

CNUT download

CNUT can be downloaded together with each system release that supports CNUT. Software for these system releases is available from <http://www.cambiumnetworks.com/support/management-tools/cnut/>, as either:

- A .zip file for use without the CNUT application.
- A .pkg file that the CNUT application can open.

Upgrading a module prior to deployment

To upgrade to a new software version, follow this:

Procedure 18 Upgrading a module prior to deployment

- 1 Go to the support website (see [Contacting Cambium Networks](#) on page 1) and find Point-to-Multipoint software updates. Download and save the required software image.
- 2 Start CNUT
- 3 If you don't start up with a blank new network file in CNUT, then open a new network file with the **New Network Archive** operation (located at **File > New Network**).
- 4 Enter a new network element to the empty network tree5-9 using the **Add Elements to Network Root** operation (located at **Edit > Add Elements to Network Root**).
- 5 In the **Add Elements** dialogue, select a type of **Access Point** or **Subscriber Module** and enter the IP address of **169.254.1.1**.
- 6 Make sure that the proper Installation Package is active with the **Package Manager** dialogue (located at **Update > Manage Packages**).
- 7 To verify connectivity with the radio, perform a **Refresh, Discover Entire Network** operation (located at **View > Refresh/Discover Entire Network**). You must see the details columns for the new element filled in with ESN and software version information.
- 8 Initiate the upgrade of the radio using **Update Entire Network Root** operation (located at **Update > Update Entire Network Root**). When this operation finishes, the radio is done being upgraded.

General configuration

The **Configuration > General** page of the AP/BMH or BHM/BHS contains many of the configurable parameters that define how the ratio's operate in sector or backhaul.

Applicable products	PMP :	<input checked="" type="checkbox"/>	AP	<input checked="" type="checkbox"/>	SM	PTP:	<input checked="" type="checkbox"/>	BHM	<input checked="" type="checkbox"/>	BMS
----------------------------	--------------	-------------------------------------	----	-------------------------------------	----	-------------	-------------------------------------	-----	-------------------------------------	-----

PMP/PTP 450i Series

General page - PMP 450i AP


The General page of AP is explained in [Table 93](#). The General page of PMP 450 SM looks same as PMP 450i AP.

Table 93 General page attributes – PMP 450i AP

Device Type	
Device Setting :	<input checked="" type="radio"/> AP <input type="radio"/> SM
Link Speeds	
Link Speed :	Auto 1000F/100F/100H/10F/10H ▼
Bandwidth Configuration Source	
Configuration Source :	SM ▼
Sync Setting	
Sync Input :	AutoSync ▼
AP Type :	<input checked="" type="radio"/> Standard AP <input type="radio"/> Remote AP
Verify GPS Message Checksum :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Sync Output to Aux Port :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
UGPS Power :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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)
Translation Bridging :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Send Untranslated ARP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SM Isolation :	Disable SM Isolation ▼
Packet Flooding :	<input type="radio"/> Bridge Flooding Enabled - Forward unknown unicast packets to all SMs. <input checked="" type="radio"/> Bridge Flooding Disabled - Only forward learned unicast packets.

Update Application Information		
Update Application Address :	0.0.0.0	
TCP Settings		
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> LLDP Multicast	
DHCP Relay Agent		
DHCP Relay Agent :	Disable	
DHCP Server (Name or IP Address) :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name	
	255.255.255.255	
Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

Attribute	Meaning
Device Setting	Allows the Spectrum Analyzer to be run directly from AP now.
Link Speeds	<p>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: Auto 100F/100H/10F/10H. In this setting, the two ends of the link automatically negotiate with each other whether the speed that they will use is 10 Mbps or 100 Mbps and whether the Ethernet traffic is full duplex or half duplex. However, 137 Ethernet links work best when either:</p> <ul style="list-style-type: none"> • both ends are set to the same forced selection • both ends are set to auto-negotiate and both have capability in least one common speed and traffic type combination.
Configuration Source	See Setting the Configuration Source on page 7-190.
Sync Input	See Configuring synchronization on page 7-95
AP Type	<p>Standard AP: The Autosync mechanism will source GPS synchronization from the AP's RJ-11 port, the AP's power port, or from the device on-board GPS module.</p> <p>Remote AP: The Autosync mechanism will source GPS synchronization from the AP's RJ-11 port or from the device on-board GPS module.</p>
Region	From the drop-down list, select the region in which the radio is operating.

Country	<p>From the drop-down list, select the country in which the radio is operating.</p> <p>Unlike selections in other parameters, your Country selection requires a Save Changes and a Reboot cycle before it will force the context-sensitive GUI to display related options (for example, Alternate Frequency Carrier 1 and 2 in the Configuration > Radio tab).</p> <p>PMP 450i equipment 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.</p> <p>Country Code settings affect the radios in the following ways:</p> <ul style="list-style-type: none"> • Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain) • DFS operation is enabled based on the configured region code, if applicable <p>For more information on how transmit power limiting and DFS is implemented for each country, see the <i>PMP 450 Planning Guide</i>.</p>
Webpage Auto Update	<p>Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.</p>
Bridge Entry Timeout	<p>Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout must be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.</p>
	<p>Caution</p> <p>An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.</p>
Translation Bridging	<p>Optionally, you can configure the AP to change the source MAC address in every packet it receives from its SMs to the MAC address of the SM that bridged the packet, before forwarding the packet toward the public network. If you do, then:</p> <p>Not more than 10 IP devices at any time are valid to send data to the AP from behind the SM.</p> <p>AP populates the Translation Table tab of its Statistics web page, displaying the MAC address and IP address of all the valid connected devices.</p> <p>Each entry in the Translation Table is associated with the number of minutes that have elapsed since the last packet transfer between the connected device and the SM.</p> <p>If 10 are connected and another attempts to connect:</p>

	<p>If no Translation Table entry is older than 255 minutes, the attempt is ignored.</p> <p>If an entry is older than 255 minutes, the oldest entry is removed and the attempt is successful.</p> <p>the Send Untranslated ARP parameter in the General tab of the Configuration page can be:</p> <p>Disabled, so that the AP overwrites the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.</p> <p>Enabled, so that the AP forwards ARP packets regardless of whether it has overwritten the MAC address.</p> <p>When this feature is disabled, the setting of the Send Untranslated ARP parameter has no effect, because all packets are forwarded untranslated (with the source MAC address intact).</p>
Send Untranslated ARP	<p>If the Translation Bridging parameter is set to Enabled, then the Send Untranslated ARP parameter can be:</p> <p>Disabled - so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.</p> <p>Enabled - so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.</p> <p>If the Translation Bridging parameter is set to Disabled, then the Send Untranslated ARP parameter has no effect.</p>
SM Isolation	<p>Prevent or allow SM-to-SM communication by selecting from the following drop-down menu items:</p> <p>Disable SM Isolation (the default selection). This allows full communication between SMs.</p> <p>Block SM Packets from being forwarded. This prevents both multicast/broadcast and unicast SM-to-SM communication.</p> <p>Block and Forward SM Packets to Backbone. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise are handled SM to SM, through the Ethernet port of the AP.</p>
Packet Flooding	<p>Enabled: All unknown Unicast packets (no entry in the AP's bridge table) received via the AP's Ethernet LAN interface are forwarded to registered SMs. If the target device is situated beneath a particular SM, when the device responds the SM and AP will learn and add the device to their bridge tables so that subsequent packets to that device is bridged to the proper SM.</p> <p>Disabled: All unknown Unicast packets (no entry in the AP's bridge table) received via the AP's Ethernet LAN interface are discarded at the AP.</p>
Update Application Address	<p>Enter the address of the server to access for software updates on this AP and registered SMs.</p>

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 set this parameter to Disable .
Multicast Destination Address	Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMM4, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the Multicast Destination Address parameter value in the connected device that has it populated.
DHCP Relay Agent	<p>The AP may act as a DHCP relay for SMs and CPEs underneath it. The AP will make use of the DHCP Option 82 (DHCP Relay Agent Information) from RFC 3046 when performing relay functions. The AP offers two types of DHCP relay functionality:</p> <p>Full Relay Information. Configuring the DHCP Full Relay Operation will take broadcast DHCP packets and send them to a Unicast server in unicast mode. This way the DHCP requests and replies can be routed like any other UDP packet.</p> <p>Only Insert Option 82. This option leaves the DHCP request on its broadcast domain as opposed to DHCP Full Relay Operation which will turn it into a unicast packet.</p> <p>In order to accommodate setting up pools or classes for different VLANs, the Option 82 field will include information to tell the server what VLAN the client is on.</p>
DHCP Server (Name or IP Address)	The DHCP relay server may be either a DNS name or a static IP address in dotted decimal notation. Additionally the management DNS domain name may be toggled such that the name of the DHCP relay server only needs to be specified and the DNS domain name is automatically appended to that name. The default DHCP relay server addresses is 255.255.255.255 with the appending of the DNS domain name disabled.
Latitude Longitude Height	Physical radio location data may be configured via the Latitude , Longitude and Height fields. Latitude and Longitude is measured in <i>Decimal Degree</i> while the Height is calculated in <i>Meters</i> .


General page - PMP 450i SM

The General page of PMP 450i SM is explained in [Table 94](#). The General page of PMP 450 SM looks same as PMP 450i SM.

Table 94 General page attributes – PMP 450i SM

Link Speeds		
Link Speed :	Auto 1000F/100F/100H/10F/10H ▼	
Ethernet Link Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 :	<input checked="" type="radio"/> Enable (If SM out of sync then do not propagate the frame timing pulse) <input type="radio"/> Disable (Always propagate the frame timing pulse)	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> LLDP Multicast	
Coordinates		
Latitude :	+0.000000	Decimal Degree
Longitude :	+0.000000	Decimal Degree
Height :	0	Meters

Attribute	Meaning
Link Speeds	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 APs and SMs in the operator network.
Ethernet Link Enable/Disable	<p>Specify whether to enable or disable Ethernet/802.3 connectivity on the wired port of the SM. This parameter has no effect on the wireless link. When you select Enable, this feature allows traffic on the Ethernet/802.3 port. This is the factory default state of the port. When you select Disable, this feature prevents traffic on the port. Typical cases of when you may want to select Disable include:</p> <p>The subscriber is delinquent with payment(s).</p> <p>You suspect that the subscriber is sending or flooding undesired broadcast packets into the network, such as when</p> <ul style="list-style-type: none"> a virus is present in the subscriber's computing device.

	<ul style="list-style-type: none"> the subscriber's home router is improperly configured.
Region	<p>This parameter allows you to set the region in which the radio will operate.</p> <p>The SM radio automatically inherits the Region type of the master. This behavior ignores the value of the Region parameter in the SM, 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.</p>
Country	<p>This parameter allows you to set the country in which the radio will operate.</p> <p>The SM radio automatically inherits the Country Code type of the master. This behavior ignores the value of the Country parameter in the SM, 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.</p> <p>PMP/PTP 450i equipment 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.</p>
Webpage Auto Update	See Table 93 General page attributes – PMP 450i AP on page 7-72
Bridge Entry Timeout	<p>Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the AP encounters no activity with the SM (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.</p> <p> Caution</p> <p>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).</p> <p>An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.</p>
Frame Timing Pulse Gated	<p>If this SM extends the sync pulse to a BH master or an AP, select either</p> <p>Enable—If this SM loses sync from the AP, then <i>do not</i> propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync.</p> <p>Disable—If this SM loses sync from the AP, then propagate the sync</p>

	pulse to the BH timing master or other AP.
Multicast Destination Address	Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMM4, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the Multicast Destination Address parameter value in the connected device that has it populated.
Coordinates	Physical radio location data may be configured via the Latitude , Longitude and Height fields.

General page - PTP 450i BHM

The General page of BHM is explained in [Table 95](#). The General page of PTP 450 BHM looks same as PTP 450i BHM.

Table 95 General page attributes – PTP 450i BHM

Device Type		
Timing Mode :	<input checked="" type="radio"/> Timing Master <input type="radio"/> Timing Slave	
Link Speeds		
Link Speed :	Auto 1000F/100F/100H/10F/10H	
Sync Setting		
Sync Input :	Generate Sync	
Regional Settings		
Region :	Asia	
Country :	India	
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 :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Update Application Information		
Update Application Address :	0.0.0.0	
TCP Settings		
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> 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	See Table 93 General page attributes – PMP 450i AP on page 7-72
Sync Input	See Configuring synchronization on page 7-95
Region	
Country	See Table 93 General page attributes – PMP 450i AP on page 7-72
Webpage Auto Update	
Bridge Entry Timeout	
Bridging Functionality	<p>Select whether you want bridge table filtering active (Enable) or not (Disable) on this BH.</p> <p>Disable: allows user to use redundant BHs without causing network addressing problems. Through a spanning tree protocol, this reduces the convergence time from 25 minutes to few seconds. However, you must disable bridge table filtering as only a deliberate part of your overall network design since disabling it allows unwanted traffic across the wireless interface.</p> <p>Enable: Allows user to enable bridge functionality.</p>
	<div data-bbox="558 947 656 1026" data-label="Image"> </div> <p>Note</p> <p>Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout must be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.</p>
Prioritize TCP ACK	
Multicast Destination Address	See Table 93 General page attributes – PMP 450i AP on page 7-72
Latitude	
Longitude	
Height	


General page - PTP 450i BHS

The General page of PTP 450i BHS is explained in [Table 96](#). The General page of PTP 450 BHS looks same as PTP 450i BHS.

Table 96 General page attributes – PTP 450i BHS

Link Speeds	
Link Speed :	Auto 1000F/100F/100H/10F/10H ▾
Ethernet Link Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
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 :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Frame Timing	
Frame Timing Pulse Gated :	<input checked="" type="radio"/> Enable (If SM out of sync then do not propagate the frame timing pulse) <input type="radio"/> Disable (Always propagate the frame timing pulse)
Layer 2 Discovery Destination Address	
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> 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 BHS in the operator network.
Region	This parameter allows you to set the region in which the radio will

	<p>operate.</p> <p>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.</p>
Country	<p>This parameter allows you to set the country in which the radio will operate.</p> <p>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.</p> <p>PMP/PTP 450i equipment 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.</p>
Webpage Auto Update	See Table 93 General page attributes – PMP 450i AP on page 7-72
Bridge Entry Timeout	<p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Caution</p> <p>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).</p> <p>An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.</p> </div>
Bridging Functionality	See Table 93 General page attributes – PMP 450i AP on page 7-72
Frame Timing Pulse Gated	<p>If this BHS extends the sync pulse to a BH master or an BHM, select either</p> <p>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.</p> <p>Disable—If this BHS loses sync from the BHM, then propagate the sync</p>

	pulse to the BH timing master or other BHM.
Multicast Destination Address	See Table 93 General page attributes – PMP 450i AP on page 7-72
Latitude Longitude Height	See Table 93 General page attributes – PMP 450i AP on page 7-72

PMP/PTP 450 Series

**Note**

Refer [Table 93](#) and [Table 94](#) for PMP 450 AP/SM General page parameters details.

General page - PMP 450 AP

Figure 108 General page attributes - PMP 450 AP

Device Type		
Device Setting :	<input checked="" type="radio"/> AP <input type="radio"/> SM	
Link Speeds		
Link Speed :	Auto 100F/100H/10F/10H	
Bandwidth Configuration Source		
Configuration Source :	SM	
Sync Setting		
Sync Input :	AutoSync	
AP Type :	<input checked="" type="radio"/> Standard AP <input type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Send Untranslated ARP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
SM Isolation :	Disable SM Isolation <input type="radio"/> Bridge Flooding Enabled - Forward unknown unicast packets to all SMS. <input checked="" type="radio"/> Bridge Flooding Disabled - Only forward learned unicast packets.	
Update Application Information		
Update Application Address :	0.0.0.0	
TCP Settings		
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Layer 2 Discovery Destination Address		
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> LLDP Multicast	
DHCP Relay Agent		
DHCP Relay Agent :	Disable	
DHCP Server (Name or IP Address) :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> 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 109 General page of PMP 450 SM

Link Speeds		
Link Speed :	Auto 100F/100H/10F/10H	
Ethernet Link Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 :	<input checked="" type="radio"/> Enable (If SM out of sync then do not propagate the frame timing pulse) <input type="radio"/> Disable (Always propagate the frame timing pulse)	

Layer 2 Discovery Destination Address		
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> LLDP Multicast	

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

General page – PTP 450 BHM

Figure 110 General page of PTP 450 BHM

Device Type	
Timing Mode :	<input checked="" type="radio"/> Timing Master <input type="radio"/> 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 :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

Update Application Information	
Update Application Address :	0.0.0.0

TCP Settings	
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Layer 2 Discovery Destination Address	
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> LLDP Multicast

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

General page – PTP 450 BHS

Figure 111 General page of PTP 450 BHS

Device Type		
Timing Mode :	<input type="radio"/> Timing Master <input checked="" type="radio"/> 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 :	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

Frame Timing	
Frame Timing Pulse Gated :	<input checked="" type="radio"/> Enable (If SM out of sync then do not propagate the frame timing pulse) <input type="radio"/> Disable (Always propagate the frame timing pulse)

Layer 2 Discovery Destination Address	
Multicast Destination Address :	<input type="radio"/> Broadcast <input checked="" type="radio"/> 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 PMP/PTP 450 platform contains following options:

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

**Note**

LED Panel setting is applicable for SM only.

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

The PMP/PTP 450 platform 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 Import and Export procedure of configuration file is described in [Import and Export of config file](#) on page 7-205.

Unit Settings page of PMP/PTP 450 platform AP/BHM

The Unit Setting page of AP/BHM is explained in [Table 97](#).

Table 97 Unit Settings attributes – PMP/PTP 450 platform AP/BHM

Default Plug

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

Unit-Wide Changes


Download Configuration File


Configuration File : [0a003ebb00fb.cfg](#)

Upload and Apply Configuration File

File: No file chosen

Status of Configuration File

Attribute	Meaning
Set to Factory Defaults Upon Default Mode Detection	<p>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.</p> <p>If Disabled is checked, then the default mode functions is disabled.</p> <p>See Radio recovery mode – Radio Recovery Console / Default Mode (fka Default Plug) on page 1-20</p>
<div style="display: flex; align-items: center; justify-content: center;">  <div> <p>Caution</p> <p>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.</p> </div> </div>	
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	When you click this button, <i>all configurable parameters on all tabs</i> are

Defaults	<p>reset to the factory settings.</p> <hr/> <div style="display: flex; align-items: center;">  <div> <p>Note</p> <p>This can be reverted by selecting "Undo Unit-Wide Saved Changes", <i>before</i> rebooting the radio, though this is not recommended.</p> </div> </div>
Configuration File	<p>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".</p>
Apply Configuration File	<p>This allows to import and apply configuration to the AP.</p> <p>Chose File: Select the file to upload the configuration. The configuration file is named as "<file name>.cfg".</p> <p>Upload: Import the configuration to the AP.</p> <p>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.</p>
Status of Configuration file	<p>This section shows the results of the upload.</p>

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

The Unit Settings page of PMP/PTP 450i SM/BHS is explained in [Table 98](#).

Table 98 SM Unit Settings attributes

Attribute	Meaning
Set to Factory Defaults Upon Default Plug Detection	See Table 97 Unit Settings attributes – PMP/PTP 450 platform AP/BHM on page 7-90
Undo Unit-Wide Saved Changes	
Set to Factory Defaults	See Table 97 Unit Settings attributes – PMP/PTP 450 platform AP/BHM on page 7-90
Configuration File	
Status of Configuration file	

Setting up time and date

Time page of PMP/PTP 450 platform AP/BHM

Applicable products PMP : AP PTP: BHM

The Time page of PMP/PTP 450 platform AP/BHM is explained in [Table 99](#).

Table 99 PMP/PTP 450 platform 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 : 20 : 33 : 13 UTC

Date : 06 / 26 / 2013

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)	
	<ul style="list-style-type: none"> • 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 7-71).

PMP/PTP 450i has following sysnchronization options:

- AutoSync
- AutoSync + Free Run
- Generate Sync

Figure 112 Sync Setting configuration

Sync Setting	
Sync Input :	Generate Sync ▼
AP Type :	AutoSync AutoSync + Free Run Generate Sync
Verify GPS Message Checksum :	<input type="radio"/> Enabled <input type="radio"/> Disabled
Sync Output to Aux Port :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
UGPS Power :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

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 AP” 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.

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 PMP/PTP 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 3-22.

Adding a User for Access to a module

The **Account > Add User** page allows to create a new user for accessing PMP/PTP 450 platform AP/SM/BHM/BHS. The Add User page is explained in [Table 100](#).

Table 100 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 3-22.
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 101](#).

Table 101 Delete User page - PMP/PTP 450 platform AP/ SM/BH

Attribute	Meaning
User	<p>Select a user from drop down list which has to be deleted and click Delete button.</p> <p>Accounts that cannot be deleted are</p> <ul style="list-style-type: none"> 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 102](#).

Table 102 Change User Setting page - PMP/PTP 450 platform AP/ SM/BH

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	<p>This tab enables and disables visibility of General Status Page for all Guest user.</p> <p>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.</p>

Figure 113 AP Evaluation Configuration parameter of Security tab for PMP

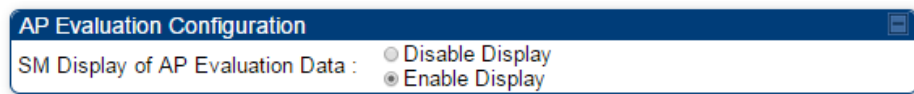
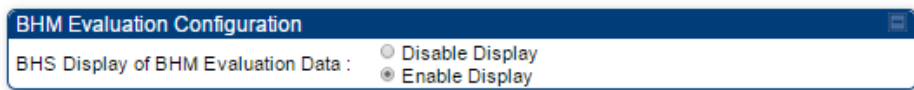


Figure 114 BHM Evaluation Configuration parameter of Security tab for PTP



Users account

The **Account > Users** page allows to view all configured users account for accessing the module. The Users page is explained in [Table 103](#).

Table 103 User page – PMP/PTP 450 platform 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 – Radio Recovery Console / Default Mode \(fka Default Plug\)](#) on page 1-20

See [Recovery mode options](#) on page 1-21

Isolating from the internet – APs/BHMs

Applicable products	PMP: <input checked="" type="checkbox"/> AP	PTP: <input checked="" type="checkbox"/> BHM
---------------------	---	--

See [Isolating AP/BHM from the Internet](#) on page 3-20.

Encrypting radio transmissions

Applicable products	PMP: <input checked="" type="checkbox"/> AP <input checked="" type="checkbox"/> SM	PTP: <input checked="" type="checkbox"/> BHM <input checked="" type="checkbox"/> BMS
---------------------	--	--

See [Encrypting radio transmissions](#) on page 3-20.

Requiring SM Authentication

Applicable products	PMP : <input checked="" type="checkbox"/> AP	<input checked="" type="checkbox"/> 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 7-116.

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 network to utilize a RADIUS server, see [Configuring a RADIUS server](#) on page 7-207.

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 3-23.

Protocol filtering page of PMP/PTP 450 platform AP/BHM

The Protocol Filtering page of PMP/PTP 450 platform AP/BHM is explained in [Table 104](#).

Table 104 AP/BHM Protocol Filtering attributes

Packet Filter Configuration	
Packet Filter Types :	<input checked="" type="checkbox"/> PPPoE
	<input type="checkbox"/> All IPv4
	<input type="checkbox"/> SMB (Network Neighborhood)
	<input type="checkbox"/> SNMP
	<input type="checkbox"/> Bootp Client
	<input type="checkbox"/> Bootp Server
	<input type="checkbox"/> IPv4 Multicast
	<input type="checkbox"/> User Defined Port 1 (See Below)
	<input type="checkbox"/> User Defined Port 2 (See Below)
	<input type="checkbox"/> User Defined Port 3 (See Below)
	<input type="checkbox"/> All other IPv4
	<input type="checkbox"/> All IPv6
	<input type="checkbox"/> SMB (Network Neighborhood)
	<input type="checkbox"/> SNMP
<input type="checkbox"/> Bootp Client	
<input type="checkbox"/> Bootp Server	
<input type="checkbox"/> IPv6 Multicast	
<input type="checkbox"/> All other IPv6	
<input type="checkbox"/> ARP	
<input type="checkbox"/> All others	
Filter Direction :	<input type="checkbox"/> Upstream
	<input type="checkbox"/> Downstream

User Defined Port Filtering Configuration	
Port #1 :	<input type="text" value="0"/> (Decimal Value)
TCP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
UDP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Port #2 :	<input type="text" value="0"/> (Decimal Value)
TCP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
UDP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Port #3 :	<input type="text" value="0"/> (Decimal Value)
TCP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
UDP :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

AP Specialty Filters	
RF Telnet Access :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
PPPoE PADI Downlink Forwarding :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Attribute	Meaning
Packet Filter Types	<p>For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type.</p> <p>To filter packets in any of the user-defined ports, must do all of the following:</p> <p>Check the box for User Defined Port <i>n</i> (See Below) in the Packet Filter Types section of this tab.</p> <p>In the User Defined Port Filtering Configuration section of this tab:</p> <ul style="list-style-type: none"> • provide a port number at Port #<i>n</i>. • enable TCP and/or UDP by clicking the associated radio button
Filter Direction	<p>Operators may choose to filter upstream (uplink) RF packets or downstream (downlink) RF packets.</p>
User Defined Port Filtering Configuration	<p>You can specify ports for which to block subscriber access, regardless of whether NAT is enabled.</p>
RF Telnet Access	<p>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.</p>
PPPoE PADI Downlink Forwarding	<p>Enabled: the AP/BHM allows downstream and upstream transmission of PPPoE PADI packets. By default, PPPoE PADI Downlink Forwarding is set to "Enabled".</p> <p>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).</p>

Protocol filtering page of SM/BHS

The Protocol Filtering page of SM/BHS is explained in [Table 105](#).

Table 105 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 : (Decimal Value)

TCP : Enabled Disabled

UDP : Enabled Disabled

Port #2 : (Decimal Value)

TCP : Enabled Disabled

UDP : Enabled Disabled

Port #3 : (Decimal Value)

TCP : Enabled Disabled

UDP : Enabled Disabled

Attribute	Meaning
Packet Filter Configuration tab	See Table 104 AP/BHM Protocol Filtering attributes on page 7-103
User Defined Port Filtering Configuration tab	See Table 104 AP/BHM Protocol Filtering attributes on page 7-103

Port configuration

PMP/PTP 450 platform devices 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 106](#).

Table 106 Port Configuration attributes – AP/SM/BHM/BMS

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 3-27.

Isolating SMs

See [Isolating SMs in PMP](#) on page 3-27.

Filtering management through Ethernet

See [Filtering management through Ethernet](#) on page 3-27.

Allowing management only from specified IP addresses

See [Allowing management from only specified IP addresses](#) on page 3-28.

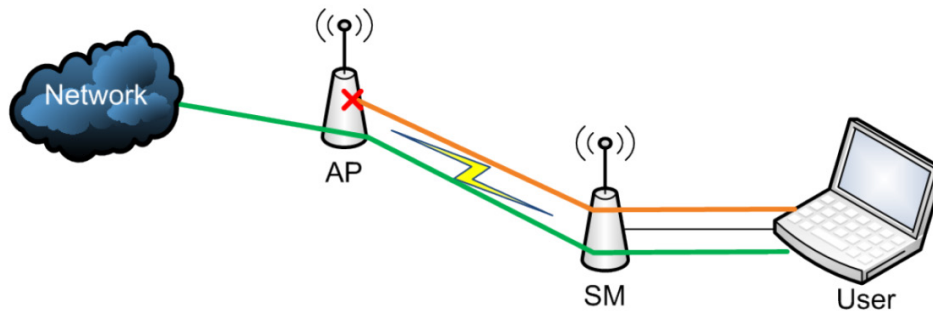
Restricting radio Telnet access over the RF interface

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 115](#)).

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.

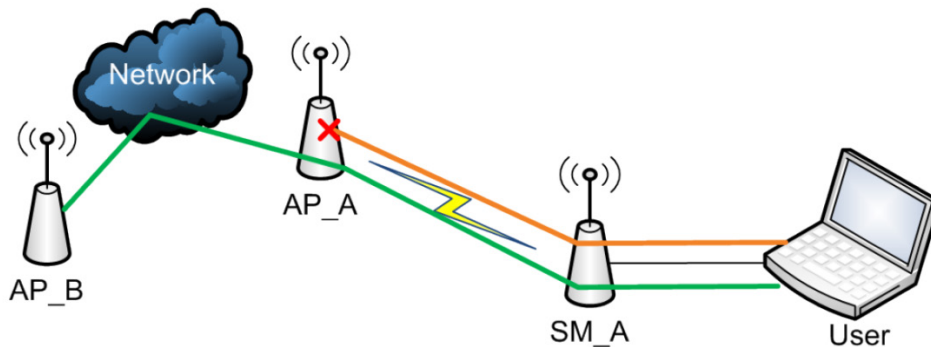
Figure 115 RF Telnet Access Restrictions (orange) and Flow through (green)

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 116](#)) via their Ethernet interfaces (since RF Telnet Access only prevents Telnet sessions originating from the AP’s wireless interface).

Figure 116 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

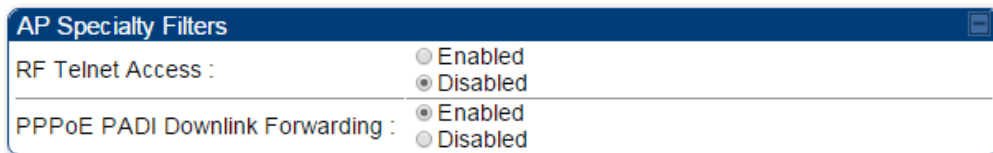
AP Telnet access via the RF interface may be configured in two ways – the AP GUI and SNMP.

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 19 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
PPPoE PADI Downlink Forwarding :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 3-21 for details.

**Note**

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

Procedure 20 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 <input type="button" value="Use Default Engine ID"/>
SNMPv3 Security Level :	noAuth,noPriv ▼
SNMPv3 Authentication Protocol :	md5 ▼
SNMPv3 Privacy Protocol :	cbc-des ▼
SNMPv3 Read-Only User :	Username <input type="text" value="Canopyro"/> Authorization Key <input type="text" value="....."/> Privacy Key <input type="text" value="....."/>
SNMPv3 Read/Write User :	<input type="radio"/> Enable R/W User <input checked="" type="radio"/> Disable R/W User Username <input type="text" value="Canopy"/> Authorization Key <input type="text" value="....."/> Privacy Key <input type="text" value="....."/>
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. PMP/PTP 450 platform supports MD5 authentication and CBC-DES privacy protocols.

SNMPv3 Read-Only and Read/Write User

The user can 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 – PMP/PTP 450 platform AP/BHM

The security page of AP/BHM is explained in [Table 107](#).

Table 107 Security tab of the AP

Authentication Server Settings	
Authentication Mode :	Disabled ▼
Authentication Server DNS Usage :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name
Authentication Server 1 :	<input type="text" value="10.120.226.6"/> Shared Secret
Authentication Server 2 :	<input type="text" value="0.0.0.0"/> Shared Secret
Authentication Server 3 :	<input type="text" value="0.0.0.0"/> Shared Secret
Authentication Server 4 (BAM ONLY) :	<input type="text" value="0.0.0.0"/>
Authentication Server 5 (BAM ONLY) :	<input type="text" value="0.0.0.0"/>
Radius Port :	<input type="text" value="1812"/> <i>Default port number is 1812</i>
Authentication Key :	<input type="text"/> (Using All 0xFF's Key)
Select Key :	<input type="radio"/> Use Key above <input checked="" type="radio"/> Use Default Key




Airlink Security	
Encryption Setting :	None ▼





AP Evaluation Configuration	
SM Display of AP Evaluation Data :	<input type="radio"/> Disable Display <input checked="" type="radio"/> Enable Display

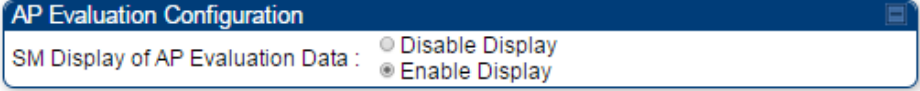
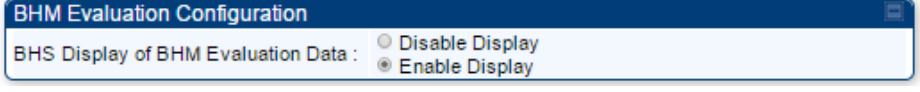
Session Timeout	
Web, Telnet, FTP Session Timeout :	<input type="text" value="3600"/> Seconds

IP Access Filtering	
IP Access Control :	<input type="radio"/> IP Access Filtering Enabled - Only allow access from IP addresses specified below <input checked="" type="radio"/> IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/> Network Mask (set to 32 to disable)
Allowed Source IP 2 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/> Network Mask (set to 32 to disable)
Allowed Source IP 3 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/> Network Mask (set to 32 to disable)

Security Mode	
Web Access :	HTTP Only ▼
SNMP :	SNMPv2c Only ▼
Telnet :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
FTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TFTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Attribute	Meaning
Authentication Mode	<p>Operators may use this field to select from among the following authentication modes:</p> <p>Disabled—the AP/BHM requires no SMs/BHS to authenticate. (Factory default).</p> <p>Authentication Server —the AP/BHM requires any SM/BHS that attempts registration to be authenticated in Wireless Manager before registration.</p> <p>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.</p> <p>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.</p> <hr/> <p> Note This parameter is applicable to BHM.</p>
Authentication Server DNS Usage	<p>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.</p> <hr/> <p> Note This parameter is applicable to BHM.</p>
Authentication Server 1 to 5	<p>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.</p> <hr/> <p> Note This parameter is applicable to BHM.</p>

Radius Port	<p>This field allows the operator to configure a custom port for RADIUS server communication. The default value is <i>1812</i>.</p>
	<p> Note This parameter is applicable to BHM.</p>
Authentication Key	<p>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.</p>
	<p> Note This parameter is applicable to BHM.</p>
Select Key	<p>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</p>
	<p> Note This parameter is applicable to BHM.</p>
Encryption Setting	<p>Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs.</p> <p>None provides no encryption on the air link.</p> <p>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.</p> <p>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.</p>
	<p> Note This parameter is applicable to BHM.</p>
<p>SM Display of AP Evaluation Data Or BHS Display of BHM Evaluation Data</p>	<p>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.</p> <p>PMP 450/450i – SM display of AP Evaluation Data parameter</p>

	
	PTP 450/450i – 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	<p>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.</p> <p>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.</p>
Web Access	<p>The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • 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	<p>This option allows to configure SNMP agent communication version. It can be selected from drop down list :</p> <ul style="list-style-type: none"> • 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 - PMP 450 platform SM

The security page of PMP 450 platform SM is explained in [Table 108](#).

Table 108 Security attributes – PMP 450 platform SM

Authentication Key Settings	
Authentication Key :	<input type="text" value=""/> (Using All 0xFF's Key)
Select Key :	<input type="radio"/> Use Key above <input checked="" type="radio"/> Use Default Key

AAA Authentication Settings	
Enforce Authentication :	Disable ▾
Phase 1 :	eaptls ▾
Phase 2 :	MSCHAPv2 ▾
Identity/Realm :	<input type="radio"/> Enable Realm <input checked="" type="radio"/> Disable Realm Identity <input type="text" value="anonymous"/> @ Realm <input type="text" value="canopy.net"/>
Username :	<input type="text" value="0a-00-3e-a0-00-79"/> <input type="button" value="Use Default Username"/>
Password :	<input type="password" value="*****"/>
Confirm Password :	<input type="password" value=""/>

RADIUS Certificate Settings	
Upload Certificate File	
File:	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Import Certificate"/> <input type="button" value="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 <input type="button" value="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 <input type="button" value="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	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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**

	<p>parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.</p> <p>A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.</p>
Web Access	<p>The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • 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	<p>This option allows to configure SNMP agent communication version. It can be selected from drop down list :</p> <ul style="list-style-type: none"> • 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.

Security page – PTP 450/450i BHS

The Security page of PTP 450/450i BHS is explained in [Table 109](#).

Table 109 Security attributes for PTP 450/450i BHS

Authentication Key Settings	
Authentication Key :	<input type="text"/> (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 :	<input checked="" type="radio"/> IP Access Filtering Enabled - Only allow access from IP addresses specified below <input type="radio"/> 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 :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
FTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TFTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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	<p>Specify the type of airlink security to apply to this BHS. The encryption setting must match the encryption setting of the BHM.</p> <p>None provides no encryption on the air link.</p> <p>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.</p> <p>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</p>

	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	<p>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.</p> <p>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.</p> <p>A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.</p>
Web Access	<p>The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • 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	<p>This option allows to configure SNMP agent communication version. It can be selected from drop down list :</p> <ul style="list-style-type: none"> • 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/PTP 450i – Configuring radio](#) on page 7-124
- [PMP/PTP 450 – Configuring radio](#) on page 7-143
- [Custom Frequencies page](#) on page 7-161
- [DFS for 5 GHz Radios](#) on page 7-164
- [MIMO-A mode of operation](#) on page 7-166
- [Improved PPS performance of PMP 450 and 450i SMs](#) on page 7-167

PMP/PTP 450i – Configuring radio

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 (5/10/20) are displayed.

Table 110 PMP 450i AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5490.0 ▾
Channel Bandwidth :	20 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	-10 dBm (Range: -30 — +27 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																
SM Registration :	<input checked="" type="radio"/> All (450i/450/430) <input type="radio"/> 450i Only															
PMP 430 SM Registration :	<input checked="" type="radio"/> Allow <input type="radio"/> Deny															
PMP 450/430 Legacy Mode :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled															
Control Messages :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A															
PMP 430 Interop Mode :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A															
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled															
	OFF ▼															
	Choose Legacy Mode setting from the table below based on collocated 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
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.
Alternate Frequency Carrier 1 and 2	These parameters are displayed based on Regional Settings. Refer Country on page 7-74
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, 10 and 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.
Frame Period	Select the Frame Period in 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 SM and the AP <i>must</i> match. Color code is not a security feature.

	<p>Instead, color code is a management feature, typically for assigning each sector a different color code.</p> <p>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).</p>
Subscriber Color Code Rescan (When not on a Primary Color Code)	<p>This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code.</p> <p>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</p>
Subscriber Color Code Wait Period for Idle	<p>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.</p>
Installation Color Code	<p>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).</p>
Max Range	<p>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</p> <ul style="list-style-type: none"> • does not increase the power of transmission from the AP.

	<ul style="list-style-type: none"> • can reduce aggregate throughput. <p>Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you <i>must</i> set this parameter on all other APs in the cluster exactly the same, except as described in the NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).</p>
Downlink Data	<p>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.</p>
	<div style="border: 1px solid black; padding: 5px;"> <div style="display: flex; align-items: center;">  <div> <p>Note</p> <p>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.</p> </div> </div> </div>
Contention Slots (a.k.a. Control Slots)	<p>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 7-165.</p>
Broadcast Repeat Count	<p>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).</p> <p>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.</p> <p>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.</p>
Transmitter Output Power	<p>This value represents the combined power of the AP's two transmitters. Nations and regions may regulate transmitter output power. For example</p> <ul style="list-style-type: none"> • 900 MHz, 5.4 GHz and 5.8 GHz modules are available as connectorized radios, which require the operator to adjust power to

	<p>ensure regulatory compliance.</p> <p>The professional installer of the equipment has the responsibility to</p> <ul style="list-style-type: none"> • 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	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.
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 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 SM (450i/450/430) or 450i Series SM only.
PMP 430 SM Registration	<p>This field allows to control of PMP 430 SMs whether PMP 430 SMs are allowed to register to PMP 450 APs. By default, it is enabled and PMP 430 SM registrations are accepted.</p> <p>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.</p> <hr/> <p> Note This option is not displayed if the Frame Period is set to 5 ms. This option applies only to PMP 450 5 GHz APs.</p>
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	<p>Disabled: It is factory default setting. It allows to operate in 450i platform capabilities.</p> <p>Enabled: It allows to operate radio in Legacy mode PMP 450 or 430.</p>
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).
	<hr/> <p> Note Due to CPU load, this will slightly degrade packet per second processing.</p>
Frame Alignment Legacy Mode	<p>In order to align the frame start of the PMP 100 and PMP 450 systems, the Frame Alignment Legacy Mode has to be selected from following options:</p> <ul style="list-style-type: none"> • OFF • ON (Mode 1) • ON (Mode 2) <p>ON (Mode 1): Selected only if the PMP 100 sync source is the power port and the PMP 100 system is at a release between 12.0 to 13.4.</p> <p>ON (Mode 2): Selected only if the PMP 100 sync source is the power port and the PMP 100 system is at release below 12.0.</p> <p>The Alignment Legacy Mode selection assumes that the PMP 100 remains on a fixed sync source. If autosync is enabled, and the PMP 100 changes sync sources, the PMP 450 AP's Alignment Legacy Mode setting would have to be changed to match. Therefore it is best</p>

to ensure only a single sync source is used on the PMP 100 AP.

Radio page – PMP 450i SM 5 GHz

The Radio page of PMP 450i SM is explained in [Table 111](#).

Table 111 PMP 450i SM Radio attributes – 5 GHz

Radio Configuration

4.9 GHz

4980.000

5.1 GHz

<input type="checkbox"/> 5152.5	<input type="checkbox"/> 5155.0	<input type="checkbox"/> 5157.5	<input type="checkbox"/> 5160.0	<input type="checkbox"/> 5162.5	<input type="checkbox"/> 5165.0	<input type="checkbox"/> 5167.5	<input type="checkbox"/> 5170.0
<input type="checkbox"/> 5172.5	<input type="checkbox"/> 5175.0	<input type="checkbox"/> 5177.5	<input type="checkbox"/> 5180.0	<input type="checkbox"/> 5182.5	<input type="checkbox"/> 5185.0	<input type="checkbox"/> 5187.5	<input type="checkbox"/> 5190.0
<input type="checkbox"/> 5192.5	<input type="checkbox"/> 5195.0	<input type="checkbox"/> 5197.5	<input type="checkbox"/> 5200.0	<input type="checkbox"/> 5202.5	<input type="checkbox"/> 5205.0	<input type="checkbox"/> 5207.5	<input type="checkbox"/> 5210.0
<input type="checkbox"/> 5212.5	<input type="checkbox"/> 5215.0	<input type="checkbox"/> 5217.5	<input type="checkbox"/> 5220.0	<input type="checkbox"/> 5222.5	<input type="checkbox"/> 5225.0	<input type="checkbox"/> 5227.5	<input type="checkbox"/> 5230.0
<input type="checkbox"/> 5232.5	<input type="checkbox"/> 5235.0	<input type="checkbox"/> 5237.5	<input type="checkbox"/> 5240.0	<input type="checkbox"/> 5242.5	<input type="checkbox"/> 5245.0	<input type="checkbox"/> 5247.5	

5.2 GHz

<input type="checkbox"/> 5252.5	<input type="checkbox"/> 5255.0	<input type="checkbox"/> 5257.5	<input type="checkbox"/> 5260.0	<input type="checkbox"/> 5262.5	<input type="checkbox"/> 5265.0	<input type="checkbox"/> 5267.5	<input type="checkbox"/> 5270.0
<input type="checkbox"/> 5272.5	<input type="checkbox"/> 5275.0	<input type="checkbox"/> 5277.5	<input type="checkbox"/> 5280.0	<input type="checkbox"/> 5282.5	<input type="checkbox"/> 5285.0	<input type="checkbox"/> 5287.5	<input type="checkbox"/> 5290.0
<input type="checkbox"/> 5292.5	<input type="checkbox"/> 5295.0	<input type="checkbox"/> 5297.5	<input type="checkbox"/> 5300.0	<input type="checkbox"/> 5302.5	<input type="checkbox"/> 5305.0	<input type="checkbox"/> 5307.5	<input type="checkbox"/> 5310.0
<input type="checkbox"/> 5312.5	<input type="checkbox"/> 5315.0	<input type="checkbox"/> 5317.5	<input type="checkbox"/> 5320.0	<input type="checkbox"/> 5322.5	<input type="checkbox"/> 5325.0	<input type="checkbox"/> 5327.5	<input type="checkbox"/> 5330.0
<input type="checkbox"/> 5332.5	<input type="checkbox"/> 5335.0	<input type="checkbox"/> 5337.5	<input type="checkbox"/> 5340.0	<input type="checkbox"/> 5342.5	<input type="checkbox"/> 5345.0	<input type="checkbox"/> 5347.5	

5.4 GHz

<input type="checkbox"/> 5472.5	<input type="checkbox"/> 5475.0	<input type="checkbox"/> 5477.5	<input checked="" type="checkbox"/> 5480.0	<input checked="" type="checkbox"/> 5482.5	<input checked="" type="checkbox"/> 5485.0	<input checked="" type="checkbox"/> 5487.5	<input checked="" type="checkbox"/> 5490.0
<input checked="" type="checkbox"/> 5492.5	<input checked="" type="checkbox"/> 5495.0	<input checked="" type="checkbox"/> 5497.5	<input checked="" type="checkbox"/> 5500.0	<input checked="" type="checkbox"/> 5502.5	<input checked="" type="checkbox"/> 5505.0	<input checked="" type="checkbox"/> 5507.5	<input checked="" type="checkbox"/> 5510.0
<input checked="" type="checkbox"/> 5512.5	<input checked="" type="checkbox"/> 5515.0	<input checked="" type="checkbox"/> 5517.5	<input checked="" type="checkbox"/> 5520.0	<input checked="" type="checkbox"/> 5522.5	<input checked="" type="checkbox"/> 5525.0	<input checked="" type="checkbox"/> 5527.5	<input checked="" type="checkbox"/> 5530.0
<input checked="" type="checkbox"/> 5532.5	<input checked="" type="checkbox"/> 5535.0	<input checked="" type="checkbox"/> 5537.5	<input checked="" type="checkbox"/> 5540.0	<input checked="" type="checkbox"/> 5542.5	<input checked="" type="checkbox"/> 5545.0	<input checked="" type="checkbox"/> 5547.5	<input checked="" type="checkbox"/> 5550.0
<input checked="" type="checkbox"/> 5552.5	<input checked="" type="checkbox"/> 5555.0	<input checked="" type="checkbox"/> 5557.5	<input checked="" type="checkbox"/> 5560.0	<input checked="" type="checkbox"/> 5562.5	<input checked="" type="checkbox"/> 5565.0	<input checked="" type="checkbox"/> 5567.5	<input checked="" type="checkbox"/> 5570.0
<input checked="" type="checkbox"/> 5572.5	<input checked="" type="checkbox"/> 5575.0	<input checked="" type="checkbox"/> 5577.5	<input checked="" type="checkbox"/> 5580.0	<input checked="" type="checkbox"/> 5582.5	<input checked="" type="checkbox"/> 5585.0	<input checked="" type="checkbox"/> 5587.5	<input checked="" type="checkbox"/> 5590.0
<input checked="" type="checkbox"/> 5592.5	<input checked="" type="checkbox"/> 5595.0	<input checked="" type="checkbox"/> 5597.5	<input checked="" type="checkbox"/> 5600.0	<input checked="" type="checkbox"/> 5602.5	<input checked="" type="checkbox"/> 5605.0	<input checked="" type="checkbox"/> 5607.5	<input checked="" type="checkbox"/> 5610.0
<input checked="" type="checkbox"/> 5612.5	<input checked="" type="checkbox"/> 5615.0	<input checked="" type="checkbox"/> 5617.5	<input checked="" type="checkbox"/> 5620.0	<input checked="" type="checkbox"/> 5622.5	<input checked="" type="checkbox"/> 5625.0	<input checked="" type="checkbox"/> 5627.5	<input checked="" type="checkbox"/> 5630.0
<input checked="" type="checkbox"/> 5632.5	<input checked="" type="checkbox"/> 5635.0	<input checked="" type="checkbox"/> 5637.5	<input checked="" type="checkbox"/> 5640.0	<input checked="" type="checkbox"/> 5642.5	<input checked="" type="checkbox"/> 5645.0	<input checked="" type="checkbox"/> 5647.5	<input checked="" type="checkbox"/> 5650.0
<input checked="" type="checkbox"/> 5652.5	<input checked="" type="checkbox"/> 5655.0	<input checked="" type="checkbox"/> 5657.5	<input checked="" type="checkbox"/> 5660.0	<input checked="" type="checkbox"/> 5662.5	<input checked="" type="checkbox"/> 5665.0	<input checked="" type="checkbox"/> 5667.5	<input checked="" type="checkbox"/> 5670.0
<input checked="" type="checkbox"/> 5672.5	<input checked="" type="checkbox"/> 5675.0	<input checked="" type="checkbox"/> 5677.5	<input checked="" type="checkbox"/> 5680.0	<input checked="" type="checkbox"/> 5682.5	<input checked="" type="checkbox"/> 5685.0	<input checked="" type="checkbox"/> 5687.5	<input checked="" type="checkbox"/> 5690.0
<input checked="" type="checkbox"/> 5692.5	<input checked="" type="checkbox"/> 5695.0	<input checked="" type="checkbox"/> 5697.5	<input checked="" type="checkbox"/> 5700.0	<input checked="" type="checkbox"/> 5702.5	<input checked="" type="checkbox"/> 5705.0	<input checked="" type="checkbox"/> 5707.5	<input checked="" type="checkbox"/> 5710.0
<input checked="" type="checkbox"/> 5712.5	<input checked="" type="checkbox"/> 5715.0	<input type="checkbox"/> 5717.5	<input type="checkbox"/> 5720.0	<input type="checkbox"/> 5722.5			

5.7 GHz

<input type="checkbox"/> 5727.5	<input type="checkbox"/> 5730.0	<input type="checkbox"/> 5732.5	<input checked="" type="checkbox"/> 5735.0	<input checked="" type="checkbox"/> 5737.5	<input checked="" type="checkbox"/> 5740.0	<input checked="" type="checkbox"/> 5742.5	<input checked="" type="checkbox"/> 5745.0
<input checked="" type="checkbox"/> 5747.5	<input checked="" type="checkbox"/> 5750.0	<input checked="" type="checkbox"/> 5752.5	<input checked="" type="checkbox"/> 5755.0	<input checked="" type="checkbox"/> 5757.5	<input checked="" type="checkbox"/> 5760.0	<input checked="" type="checkbox"/> 5762.5	<input checked="" type="checkbox"/> 5765.0
<input checked="" type="checkbox"/> 5767.5	<input checked="" type="checkbox"/> 5770.0	<input checked="" type="checkbox"/> 5772.5	<input checked="" type="checkbox"/> 5775.0	<input checked="" type="checkbox"/> 5777.5	<input checked="" type="checkbox"/> 5780.0	<input checked="" type="checkbox"/> 5782.5	<input checked="" type="checkbox"/> 5785.0
<input checked="" type="checkbox"/> 5787.5	<input checked="" type="checkbox"/> 5790.0	<input checked="" type="checkbox"/> 5792.5	<input checked="" type="checkbox"/> 5795.0	<input checked="" type="checkbox"/> 5797.5	<input checked="" type="checkbox"/> 5800.0	<input checked="" type="checkbox"/> 5802.5	<input checked="" type="checkbox"/> 5805.0
<input checked="" type="checkbox"/> 5807.5	<input checked="" type="checkbox"/> 5810.0	<input checked="" type="checkbox"/> 5812.5	<input checked="" type="checkbox"/> 5815.0	<input checked="" type="checkbox"/> 5817.5	<input checked="" type="checkbox"/> 5820.0	<input checked="" type="checkbox"/> 5822.5	<input checked="" type="checkbox"/> 5825.0
<input checked="" type="checkbox"/> 5827.5	<input checked="" type="checkbox"/> 5830.0	<input checked="" type="checkbox"/> 5832.5	<input checked="" type="checkbox"/> 5835.0	<input checked="" type="checkbox"/> 5837.5	<input checked="" type="checkbox"/> 5840.0	<input checked="" type="checkbox"/> 5842.5	<input checked="" type="checkbox"/> 5845.0
<input checked="" type="checkbox"/> 5847.5	<input checked="" type="checkbox"/> 5850.0	<input checked="" type="checkbox"/> 5852.5	<input checked="" type="checkbox"/> 5855.0	<input checked="" type="checkbox"/> 5857.5	<input checked="" type="checkbox"/> 5860.0	<input checked="" type="checkbox"/> 5862.5	<input checked="" type="checkbox"/> 5865.0
<input checked="" type="checkbox"/> 5867.5	<input checked="" type="checkbox"/> 5870.0	<input checked="" type="checkbox"/> 5872.5	<input checked="" type="checkbox"/> 5875.0	<input checked="" type="checkbox"/> 5877.5	<input checked="" type="checkbox"/> 5880.0	<input checked="" type="checkbox"/> 5882.5	<input checked="" type="checkbox"/> 5885.0
<input checked="" type="checkbox"/> 5887.5	<input checked="" type="checkbox"/> 5890.0	<input checked="" type="checkbox"/> 5892.5	<input checked="" type="checkbox"/> 5895.0	<input checked="" type="checkbox"/> 5897.5	<input checked="" type="checkbox"/> 5900.0	<input checked="" type="checkbox"/> 5902.5	<input checked="" type="checkbox"/> 5905.0
<input checked="" type="checkbox"/> 5907.5	<input checked="" type="checkbox"/> 5910.0	<input checked="" type="checkbox"/> 5912.5	<input checked="" type="checkbox"/> 5915.0	<input type="checkbox"/> 5917.5	<input type="checkbox"/> 5920.0	<input type="checkbox"/> 5922.5	

5 MHz only
 ≤ 10 MHz
 Not available in this region

Channel Bandwidth Scan :	<input type="checkbox"/> 5 MHz <input type="checkbox"/> 10 MHz <input checked="" type="checkbox"/> 20 MHz
Cyclic Prefix Scan :	<input checked="" type="checkbox"/> One Sixteenth
AP Selection Method :	<input type="radio"/> Power Level <input checked="" type="radio"/> Optimize for Throughput
Color Code 1 :	254 (0—254) / Priority Primary ▼
Installation Color Code :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled


Additional Color Codes	
Color Code :	0 (0—254) / Priority Primary ▼
	<input type="button" value="Add/Modify Color Code"/> <input type="button" value="Remove Color Code"/>

Additional Color Codes Table	
<u>Color Code</u>	<u>Priority</u>
2	Secondary
3	Tertiary

Power Control	
External Gain Fixed :	23 dB (Range: 0 — +40 dB)

Power Control	
External Gain Fixed :	23 dB (Range: 0 — +40 dB)

Advanced	
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 7-158.
Channel Bandwidth Scan	The channel size used by the radio for RF transmission. <div style="margin-top: 10px;">  <p>Note Selecting multiple channel bandwidths will increase registration and re-registration times.</p> </div>
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. <p>Power Level: AP selection based solely on power level</p> <p><i>or</i></p> <p>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).</p>
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. <p>Color code is not a security feature. Instead, color code is a management</p>

	<p>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).</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The color codes can be disabled, with the exception of the first color code.</p>
Installation Color Code	<p>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.</p>
External Gain	<p>This value represents the antenna gain.</p> <p>For ODUs with integrated antenna, this is set at the correct value in the factory.</p> <p>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.</p>
Large VC data Queue	<p>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.</p>
Receive Quality	<p>To aid in link performance monitoring, the AP and SM now report the</p>

Debug 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 7-161) 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 112](#).

Table 112 PMP 450i AP Radio attributes - 900 MHz

Radio Configuration	
Frequency Carrier :	917.00 ▼
Channel Bandwidth :	10 MHz ▼
Cyclic Prefix :	One Sixteenth ▼
Frame Period :	<input checked="" type="radio"/> 5.0 ms <input type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A												
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled												
Pager Reject Filter :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 collocated 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	
Frame Period	
Color Code	
Subscriber Color Code Rescan (When not on a Primary Color Code)	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
Subscriber Color Code Wait Period for Idle	
Installation Color Code	
Max Range	
Downlink Data	
Contention Slots (a.k.a. Control Slots)	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
Broadcast Repeat Count	
Transmitter Output Power	
External Gain	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
SM Receive Target Level	
Multicast VC Data Rate	
Multicast Repeat Count	
Multicast Downlink CIR	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
Control Message	
Receive Quality Debug	
Pager Reject Filter	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.
Frame Alignment Legacy Mode	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.

Radio page - PTP 450i BHM 5 GHz

The **Radio** page of PTP 450i BHM is explained in [Table 113](#).


Table 113 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 :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 2.5 ms
Color Code :	254 (0—254)
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled OFF ▾															
Frame Alignment Legacy Mode :	Choose Legacy Mode setting from the table below based on collocated radio'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 (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
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 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.
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	<ul style="list-style-type: none"> • PTP 450i modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. <p>The professional installer of the equipment has the responsibility to:</p> <ul style="list-style-type: none"> • 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. <p>Confirm that the power setting is compliant following any reset of the module to factory defaults.</p>
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, 256-QAM) and per channel (polarization).
<div style="display: flex; align-items: flex-start; margin-bottom: 10px;"> <div style="margin-right: 10px;">  </div> <div> <p>Note</p> <p>Due to CPU load, this slightly degrades the packet during per second processing.</p> </div> </div>	
Frame Alignment Legacy Mode	<p>In order to align the frame start of the PTP 100 and PTP 450 systems, the Frame Alignment Legacy Mode has to be selected from following options:</p> <ul style="list-style-type: none"> • OFF • ON (Mode 1) • ON (Mode 2) <p>ON (Mode 1): Selected only if the PTP 100 sync source is the power port and the PTP 100 system is at a release between 12.0 to 13.4.</p> <p>ON (Mode 2): Selected only if the PTP 100 sync source is the power port and the PTP 100 system is at release below 12.0.</p> <p>The Alignment Legacy Mode selection assumes that the PTP 100 remains on a fixed sync source. If autosync is enabled, and the PTP 100 changes sync sources, the PTP 450 BHM's Alignment Legacy Mode setting would have to be changed to match. Therefore it is best to ensure only a single sync source is used on the PTP 100 BHM.</p>

Radio page – PTP 450i BHS 5 GHz

The Radio page of PTP 450i BHS is explained in [Table 114](#).

Table 114 PTP 450i BHS Radio attributes – 5 GHz

Radio Configuration

4.9 GHz

4980.000

5.1 GHz

<input type="checkbox"/> 5152.5	<input type="checkbox"/> 5155.0	<input type="checkbox"/> 5157.5	<input type="checkbox"/> 5160.0	<input type="checkbox"/> 5162.5	<input type="checkbox"/> 5165.0	<input type="checkbox"/> 5167.5
<input type="checkbox"/> 5170.0	<input type="checkbox"/> 5172.5	<input type="checkbox"/> 5175.0	<input type="checkbox"/> 5177.5	<input type="checkbox"/> 5180.0	<input type="checkbox"/> 5182.5	<input type="checkbox"/> 5185.0
<input type="checkbox"/> 5187.5	<input type="checkbox"/> 5190.0	<input type="checkbox"/> 5192.5	<input type="checkbox"/> 5195.0	<input type="checkbox"/> 5197.5	<input type="checkbox"/> 5200.0	<input type="checkbox"/> 5202.5
<input type="checkbox"/> 5205.0	<input type="checkbox"/> 5207.5	<input type="checkbox"/> 5210.0	<input type="checkbox"/> 5212.5	<input type="checkbox"/> 5215.0	<input type="checkbox"/> 5217.5	<input type="checkbox"/> 5220.0
<input type="checkbox"/> 5222.5	<input type="checkbox"/> 5225.0	<input type="checkbox"/> 5227.5	<input type="checkbox"/> 5230.0	<input type="checkbox"/> 5232.5	<input type="checkbox"/> 5235.0	<input type="checkbox"/> 5237.5
<input type="checkbox"/> 5240.0	<input type="checkbox"/> 5242.5	<input type="checkbox"/> 5245.0	<input type="checkbox"/> 5247.5			

5.2 GHz

<input type="checkbox"/> 5252.5	<input type="checkbox"/> 5255.0	<input type="checkbox"/> 5257.5	<input type="checkbox"/> 5260.0	<input type="checkbox"/> 5262.5	<input type="checkbox"/> 5265.0	<input type="checkbox"/> 5267.5
<input type="checkbox"/> 5270.0	<input type="checkbox"/> 5272.5	<input type="checkbox"/> 5275.0	<input type="checkbox"/> 5277.5	<input type="checkbox"/> 5280.0	<input type="checkbox"/> 5282.5	<input type="checkbox"/> 5285.0
<input type="checkbox"/> 5287.5	<input type="checkbox"/> 5290.0	<input type="checkbox"/> 5292.5	<input type="checkbox"/> 5295.0	<input type="checkbox"/> 5297.5	<input type="checkbox"/> 5300.0	<input type="checkbox"/> 5302.5
<input type="checkbox"/> 5305.0	<input type="checkbox"/> 5307.5	<input type="checkbox"/> 5310.0	<input type="checkbox"/> 5312.5	<input type="checkbox"/> 5315.0	<input type="checkbox"/> 5317.5	<input type="checkbox"/> 5320.0
<input type="checkbox"/> 5322.5	<input type="checkbox"/> 5325.0	<input type="checkbox"/> 5327.5	<input type="checkbox"/> 5330.0	<input type="checkbox"/> 5332.5	<input type="checkbox"/> 5335.0	<input type="checkbox"/> 5337.5
<input type="checkbox"/> 5340.0	<input type="checkbox"/> 5342.5	<input type="checkbox"/> 5345.0	<input type="checkbox"/> 5347.5			

5.4 GHz

<input type="checkbox"/> 5472.5	<input type="checkbox"/> 5475.0	<input type="checkbox"/> 5477.5	<input type="checkbox"/> 5480.0	<input type="checkbox"/> 5482.5	<input type="checkbox"/> 5485.0	<input type="checkbox"/> 5487.5
<input checked="" type="checkbox"/> 5490.0	<input checked="" type="checkbox"/> 5492.5	<input checked="" type="checkbox"/> 5495.0	<input checked="" type="checkbox"/> 5497.5	<input checked="" type="checkbox"/> 5500.0	<input checked="" type="checkbox"/> 5502.5	<input checked="" type="checkbox"/> 5505.0
<input checked="" type="checkbox"/> 5507.5	<input checked="" type="checkbox"/> 5510.0	<input checked="" type="checkbox"/> 5512.5	<input checked="" type="checkbox"/> 5515.0	<input checked="" type="checkbox"/> 5517.5	<input checked="" type="checkbox"/> 5520.0	<input checked="" type="checkbox"/> 5522.5
<input checked="" type="checkbox"/> 5525.0	<input checked="" type="checkbox"/> 5527.5	<input checked="" type="checkbox"/> 5530.0	<input checked="" type="checkbox"/> 5532.5	<input checked="" type="checkbox"/> 5535.0	<input checked="" type="checkbox"/> 5537.5	<input checked="" type="checkbox"/> 5540.0
<input checked="" type="checkbox"/> 5542.5	<input checked="" type="checkbox"/> 5545.0	<input checked="" type="checkbox"/> 5547.5	<input checked="" type="checkbox"/> 5550.0	<input checked="" type="checkbox"/> 5552.5	<input checked="" type="checkbox"/> 5555.0	<input checked="" type="checkbox"/> 5557.5
<input checked="" type="checkbox"/> 5560.0	<input checked="" type="checkbox"/> 5562.5	<input checked="" type="checkbox"/> 5565.0	<input checked="" type="checkbox"/> 5567.5	<input checked="" type="checkbox"/> 5570.0	<input checked="" type="checkbox"/> 5572.5	<input checked="" type="checkbox"/> 5575.0
<input checked="" type="checkbox"/> 5577.5	<input checked="" type="checkbox"/> 5580.0	<input checked="" type="checkbox"/> 5582.5	<input checked="" type="checkbox"/> 5585.0	<input checked="" type="checkbox"/> 5587.5	<input checked="" type="checkbox"/> 5590.0	<input checked="" type="checkbox"/> 5592.5
<input checked="" type="checkbox"/> 5595.0	<input checked="" type="checkbox"/> 5597.5	<input checked="" type="checkbox"/> 5600.0	<input checked="" type="checkbox"/> 5602.5	<input checked="" type="checkbox"/> 5605.0	<input checked="" type="checkbox"/> 5607.5	<input checked="" type="checkbox"/> 5610.0
<input checked="" type="checkbox"/> 5612.5	<input checked="" type="checkbox"/> 5615.0	<input checked="" type="checkbox"/> 5617.5	<input checked="" type="checkbox"/> 5620.0	<input checked="" type="checkbox"/> 5622.5	<input checked="" type="checkbox"/> 5625.0	<input checked="" type="checkbox"/> 5627.5
<input checked="" type="checkbox"/> 5630.0	<input checked="" type="checkbox"/> 5632.5	<input checked="" type="checkbox"/> 5635.0	<input checked="" type="checkbox"/> 5637.5	<input checked="" type="checkbox"/> 5640.0	<input checked="" type="checkbox"/> 5642.5	<input checked="" type="checkbox"/> 5645.0
<input checked="" type="checkbox"/> 5647.5	<input checked="" type="checkbox"/> 5650.0	<input checked="" type="checkbox"/> 5652.5	<input checked="" type="checkbox"/> 5655.0	<input checked="" type="checkbox"/> 5657.5	<input checked="" type="checkbox"/> 5660.0	<input checked="" type="checkbox"/> 5662.5
<input checked="" type="checkbox"/> 5665.0	<input checked="" type="checkbox"/> 5667.5	<input checked="" type="checkbox"/> 5670.0	<input checked="" type="checkbox"/> 5672.5	<input checked="" type="checkbox"/> 5675.0	<input checked="" type="checkbox"/> 5677.5	<input checked="" type="checkbox"/> 5680.0
<input checked="" type="checkbox"/> 5682.5	<input checked="" type="checkbox"/> 5685.0	<input checked="" type="checkbox"/> 5687.5	<input checked="" type="checkbox"/> 5690.0	<input checked="" type="checkbox"/> 5692.5	<input checked="" type="checkbox"/> 5695.0	<input checked="" type="checkbox"/> 5697.5
<input checked="" type="checkbox"/> 5700.0	<input checked="" type="checkbox"/> 5702.5	<input checked="" type="checkbox"/> 5705.0	<input checked="" type="checkbox"/> 5707.5	<input checked="" type="checkbox"/> 5710.0	<input checked="" type="checkbox"/> 5712.5	<input checked="" type="checkbox"/> 5715.0
<input type="checkbox"/> 5717.5	<input type="checkbox"/> 5720.0	<input type="checkbox"/> 5722.5				

5.7 GHz

<input type="checkbox"/> 5727.5	<input type="checkbox"/> 5730.0	<input type="checkbox"/> 5732.5	<input checked="" type="checkbox"/> 5735.0	<input checked="" type="checkbox"/> 5737.5	<input checked="" type="checkbox"/> 5740.0	<input checked="" type="checkbox"/> 5742.5
<input checked="" type="checkbox"/> 5745.0	<input checked="" type="checkbox"/> 5747.5	<input checked="" type="checkbox"/> 5750.0	<input checked="" type="checkbox"/> 5752.5	<input checked="" type="checkbox"/> 5755.0	<input checked="" type="checkbox"/> 5757.5	<input checked="" type="checkbox"/> 5760.0
<input checked="" type="checkbox"/> 5762.5	<input checked="" type="checkbox"/> 5765.0	<input checked="" type="checkbox"/> 5767.5	<input checked="" type="checkbox"/> 5770.0	<input checked="" type="checkbox"/> 5772.5	<input checked="" type="checkbox"/> 5775.0	<input checked="" type="checkbox"/> 5777.5
<input checked="" type="checkbox"/> 5780.0	<input checked="" type="checkbox"/> 5782.5	<input checked="" type="checkbox"/> 5785.0	<input checked="" type="checkbox"/> 5787.5	<input checked="" type="checkbox"/> 5790.0	<input checked="" type="checkbox"/> 5792.5	<input checked="" type="checkbox"/> 5795.0
<input checked="" type="checkbox"/> 5797.5	<input checked="" type="checkbox"/> 5800.0	<input checked="" type="checkbox"/> 5802.5	<input checked="" type="checkbox"/> 5805.0	<input checked="" type="checkbox"/> 5807.5	<input checked="" type="checkbox"/> 5810.0	<input checked="" type="checkbox"/> 5812.5
<input checked="" type="checkbox"/> 5815.0	<input checked="" type="checkbox"/> 5817.5	<input checked="" type="checkbox"/> 5820.0	<input checked="" type="checkbox"/> 5822.5	<input checked="" type="checkbox"/> 5825.0	<input checked="" type="checkbox"/> 5827.5	<input checked="" type="checkbox"/> 5830.0
<input checked="" type="checkbox"/> 5832.5	<input checked="" type="checkbox"/> 5835.0	<input checked="" type="checkbox"/> 5837.5	<input checked="" type="checkbox"/> 5840.0	<input checked="" type="checkbox"/> 5842.5	<input checked="" type="checkbox"/> 5845.0	<input checked="" type="checkbox"/> 5847.5
<input checked="" type="checkbox"/> 5850.0	<input checked="" type="checkbox"/> 5852.5	<input checked="" type="checkbox"/> 5855.0	<input checked="" type="checkbox"/> 5857.5	<input checked="" type="checkbox"/> 5860.0	<input checked="" type="checkbox"/> 5862.5	<input checked="" type="checkbox"/> 5865.0
<input checked="" type="checkbox"/> 5867.5	<input checked="" type="checkbox"/> 5870.0	<input checked="" type="checkbox"/> 5872.5	<input checked="" type="checkbox"/> 5875.0	<input checked="" type="checkbox"/> 5877.5	<input checked="" type="checkbox"/> 5880.0	<input checked="" type="checkbox"/> 5882.5
<input checked="" type="checkbox"/> 5885.0	<input checked="" type="checkbox"/> 5887.5	<input checked="" type="checkbox"/> 5890.0	<input checked="" type="checkbox"/> 5892.5	<input checked="" type="checkbox"/> 5895.0	<input checked="" type="checkbox"/> 5897.5	<input checked="" type="checkbox"/> 5900.0
<input checked="" type="checkbox"/> 5902.5	<input checked="" type="checkbox"/> 5905.0	<input checked="" type="checkbox"/> 5907.5	<input checked="" type="checkbox"/> 5910.0	<input checked="" type="checkbox"/> 5912.5	<input checked="" type="checkbox"/> 5915.0	<input type="checkbox"/> 5917.5
<input type="checkbox"/> 5920.0	<input type="checkbox"/> 5922.5					

5 MHz only
≤ 10 MHz
 Not available in this region


Select All Select All 4.9 Select All 5.1 Select All 5.2 Select All 5.4 Select All 5.7

Clear All Restore

Channel Bandwidth Scan :	<input type="checkbox"/> 5 MHz <input type="checkbox"/> 10 MHz <input checked="" type="checkbox"/> 20 MHz
Cyclic Prefix Scan :	<input checked="" type="checkbox"/> One Sixteenth
Color Code :	254 (0—254)
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Power Control	
Transmit Power :	18 dBm (Range: -30 — +27 dBm) (13 dBm V / 13 dBm H)
External Gain :	23 dB (Range: 0 — +40 dB)

Advanced	
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 7-158.
Channel Bandwidth Scan	<p>The channel size used by the radio for RF transmission.</p> <div style="display: flex; align-items: center;">  <p>Note Selecting multiple channel bandwidths will increase registration and re-registration times.</p> </div>
Cyclic Prefix Scan	The cyclic prefix for which BHM scanning is executed.
Color Code	<p>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.</p> <p>The color codes can be disabled, with the exception of the first color code.</p>
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 113 PTP 450i BHM Radio page attributes – 5 GHz on page 7-138
External Gain	
Receive Quality Debug	

PMP/PTP 450 – Configuring radio

Radio page - PMP 450 AP 5 GHz

The **Radio** tab of the AP for 5 GHz is as shown in [Table 115](#).

Table 115 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 :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 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 :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 :	<input checked="" type="radio"/> Allow <input type="radio"/> Deny															
Control Messages :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A															
PMP 430 Interop Mode :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A															
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
PMP 430 SM Registration	
PMP 450/430 Legacy Mode	
Control Messages	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
PMP 430 Interop Mode	
Receive Quality Debug	
Frame Alignment Legacy Mode	

Radio page - PMP 450 AP 3.65 GHz

Table 116 PMP 450 AP Radio attributes - 3.65 GHz

Radio Configuration	
Frequency Carrier :	3650.000 ▾
Channel Bandwidth :	20 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.

Radio page - PMP 450 AP 3.5 GHz

Table 117 PMP 450 AP Radio attributes - 3.5 GHz

Radio Configuration	
Frequency Carrier :	3590.001 ▾
Channel Bandwidth :	10 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.

Radio page - PMP 450 AP 2.4 GHz

Table 118 PMP 450 AP Radio attributes - 2.4 GHz

Radio Configuration	
Frequency Carrier :	2440.0 ▾
Channel Bandwidth :	20 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 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 :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 :	<input type="radio"/> SISO <input checked="" type="radio"/> MIMO-A
Receive Quality Debug :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.

Radio page - PMP 450 SM 5 GHz

Table 119 PMP 450 SM Radio attributes – 5 GHz

Radio Configuration

5.4 GHz

<input type="checkbox"/> 5472.5	<input type="checkbox"/> 5475.0	<input type="checkbox"/> 5477.5	<input checked="" type="checkbox"/> 5480.0	<input checked="" type="checkbox"/> 5482.5	<input checked="" type="checkbox"/> 5485.0	<input checked="" type="checkbox"/> 5487.5
<input checked="" type="checkbox"/> 5490.0	<input checked="" type="checkbox"/> 5492.5	<input checked="" type="checkbox"/> 5495.0	<input checked="" type="checkbox"/> 5497.5	<input checked="" type="checkbox"/> 5500.0	<input checked="" type="checkbox"/> 5502.5	<input checked="" type="checkbox"/> 5505.0
<input checked="" type="checkbox"/> 5507.5	<input checked="" type="checkbox"/> 5510.0	<input checked="" type="checkbox"/> 5512.5	<input checked="" type="checkbox"/> 5515.0	<input checked="" type="checkbox"/> 5517.5	<input checked="" type="checkbox"/> 5520.0	<input checked="" type="checkbox"/> 5522.5
<input checked="" type="checkbox"/> 5525.0	<input checked="" type="checkbox"/> 5527.5	<input checked="" type="checkbox"/> 5530.0	<input checked="" type="checkbox"/> 5532.5	<input checked="" type="checkbox"/> 5535.0	<input checked="" type="checkbox"/> 5537.5	<input checked="" type="checkbox"/> 5540.0
<input checked="" type="checkbox"/> 5542.5	<input checked="" type="checkbox"/> 5545.0	<input checked="" type="checkbox"/> 5547.5	<input checked="" type="checkbox"/> 5550.0	<input checked="" type="checkbox"/> 5552.5	<input checked="" type="checkbox"/> 5555.0	<input checked="" type="checkbox"/> 5557.5
<input checked="" type="checkbox"/> 5560.0	<input checked="" type="checkbox"/> 5562.5	<input checked="" type="checkbox"/> 5565.0	<input checked="" type="checkbox"/> 5567.5	<input checked="" type="checkbox"/> 5570.0	<input checked="" type="checkbox"/> 5572.5	<input checked="" type="checkbox"/> 5575.0
<input checked="" type="checkbox"/> 5577.5	<input checked="" type="checkbox"/> 5580.0	<input checked="" type="checkbox"/> 5582.5	<input checked="" type="checkbox"/> 5585.0	<input checked="" type="checkbox"/> 5587.5	<input checked="" type="checkbox"/> 5590.0	<input type="checkbox"/> 5592.5
<input type="checkbox"/> 5595.0	<input type="checkbox"/> 5597.5	<input type="checkbox"/> 5600.0	<input type="checkbox"/> 5602.5	<input type="checkbox"/> 5605.0	<input type="checkbox"/> 5607.5	<input type="checkbox"/> 5610.0
<input type="checkbox"/> 5612.5	<input type="checkbox"/> 5615.0	<input type="checkbox"/> 5617.5	<input type="checkbox"/> 5620.0	<input type="checkbox"/> 5622.5	<input type="checkbox"/> 5625.0	<input type="checkbox"/> 5627.5
<input type="checkbox"/> 5630.0	<input type="checkbox"/> 5632.5	<input type="checkbox"/> 5635.0	<input type="checkbox"/> 5637.5	<input type="checkbox"/> 5640.0	<input type="checkbox"/> 5642.5	<input type="checkbox"/> 5645.0
<input type="checkbox"/> 5647.5	<input type="checkbox"/> 5650.0	<input type="checkbox"/> 5652.5	<input type="checkbox"/> 5655.0	<input type="checkbox"/> 5657.5	<input type="checkbox"/> 5660.0	<input checked="" type="checkbox"/> 5662.5
<input checked="" type="checkbox"/> 5665.0	<input checked="" type="checkbox"/> 5667.5	<input checked="" type="checkbox"/> 5670.0	<input checked="" type="checkbox"/> 5672.5	<input checked="" type="checkbox"/> 5675.0	<input checked="" type="checkbox"/> 5677.5	<input checked="" type="checkbox"/> 5680.0
<input checked="" type="checkbox"/> 5682.5	<input checked="" type="checkbox"/> 5685.0	<input checked="" type="checkbox"/> 5687.5	<input checked="" type="checkbox"/> 5690.0	<input checked="" type="checkbox"/> 5692.5	<input checked="" type="checkbox"/> 5695.0	<input checked="" type="checkbox"/> 5697.5
<input checked="" type="checkbox"/> 5700.0	<input checked="" type="checkbox"/> 5702.5	<input checked="" type="checkbox"/> 5705.0	<input checked="" type="checkbox"/> 5707.5	<input checked="" type="checkbox"/> 5710.0	<input checked="" type="checkbox"/> 5712.5	<input checked="" type="checkbox"/> 5715.0

Custom Radio Frequency Scan Selection List :

<input type="checkbox"/> 5717.5	<input type="checkbox"/> 5720.0	<input type="checkbox"/> 5722.5
---------------------------------	---------------------------------	---------------------------------

5.7 GHz

<input type="checkbox"/> 5727.5	<input type="checkbox"/> 5730.0	<input type="checkbox"/> 5732.5	<input checked="" type="checkbox"/> 5735.0	<input checked="" type="checkbox"/> 5737.5	<input checked="" type="checkbox"/> 5740.0	<input checked="" type="checkbox"/> 5742.5
<input checked="" type="checkbox"/> 5745.0	<input checked="" type="checkbox"/> 5747.5	<input checked="" type="checkbox"/> 5750.0	<input checked="" type="checkbox"/> 5752.5	<input checked="" type="checkbox"/> 5755.0	<input checked="" type="checkbox"/> 5757.5	<input checked="" type="checkbox"/> 5760.0
<input checked="" type="checkbox"/> 5762.5	<input checked="" type="checkbox"/> 5765.0	<input checked="" type="checkbox"/> 5767.5	<input checked="" type="checkbox"/> 5770.0	<input checked="" type="checkbox"/> 5772.5	<input checked="" type="checkbox"/> 5775.0	<input checked="" type="checkbox"/> 5777.5
<input checked="" type="checkbox"/> 5780.0	<input checked="" type="checkbox"/> 5782.5	<input checked="" type="checkbox"/> 5785.0	<input checked="" type="checkbox"/> 5787.5	<input checked="" type="checkbox"/> 5790.0	<input checked="" type="checkbox"/> 5792.5	<input checked="" type="checkbox"/> 5795.0
<input checked="" type="checkbox"/> 5797.5	<input checked="" type="checkbox"/> 5800.0	<input checked="" type="checkbox"/> 5802.5	<input checked="" type="checkbox"/> 5805.0	<input checked="" type="checkbox"/> 5807.5	<input checked="" type="checkbox"/> 5810.0	<input checked="" type="checkbox"/> 5812.5
<input checked="" type="checkbox"/> 5815.0	<input checked="" type="checkbox"/> 5817.5	<input checked="" type="checkbox"/> 5820.0	<input checked="" type="checkbox"/> 5822.5	<input checked="" type="checkbox"/> 5825.0	<input checked="" type="checkbox"/> 5827.5	<input checked="" type="checkbox"/> 5830.0
<input checked="" type="checkbox"/> 5832.5	<input checked="" type="checkbox"/> 5835.0	<input checked="" type="checkbox"/> 5837.5	<input checked="" type="checkbox"/> 5840.0	<input type="checkbox"/> 5842.5	<input type="checkbox"/> 5845.0	<input type="checkbox"/> 5847.5
<input type="checkbox"/> 5850.0	<input type="checkbox"/> 5852.5	<input type="checkbox"/> 5855.0	<input type="checkbox"/> 5857.5	<input type="checkbox"/> 5860.0	<input type="checkbox"/> 5862.5	<input type="checkbox"/> 5865.0
<input type="checkbox"/> 5867.5	<input type="checkbox"/> 5870.0	<input type="checkbox"/> 5872.5	<input type="checkbox"/> 5875.0	<input type="checkbox"/> 5877.5	<input type="checkbox"/> 5880.0	<input type="checkbox"/> 5882.5
<input type="checkbox"/> 5885.0	<input type="checkbox"/> 5887.5	<input type="checkbox"/> 5890.0	<input type="checkbox"/> 5892.5	<input type="checkbox"/> 5895.0	<input type="checkbox"/> 5897.5	

10 MHz only
Not available in this region

Channel Bandwidth Scan : 10 MHz 20 MHz

Cyclic Prefix Scan : One Sixteenth

AP Selection Method : Power Level Optimize for Throughput

Color Code 1 : (0—254) / Priority

Installation Color Code : Enabled Disabled

Large VC data Q : Enabled Disabled

Additional Color Codes

Color Code : (0—254) / Priority

Additional Color Codes Table

No additional color codes configured

Power Control

External Gain : dB (Range: 0 — +35 dB)

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 7-158.
See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.	

Radio page - PMP 450 SM 3.65 GHz

Table 120 PMP 450 SM Radio attributes – 3.65 GHz

Radio Configuration

3320.123 3333.333 3355.004 3396.500
 3450.000 3496.050 3560.025 3650.000
 3670.000

Custom Radio Frequency Scan Selection List :

5 MHz only
7 MHz only
10 MHz only
 Not available in this region

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 :

5 (0—254) / Priority Primary ▼

Installation Color Code :

Enabled
 Disabled

Large VC data Q :

Enabled
 Disabled

Additional Color Codes

Color Code :

5 (0—254) / Priority Primary ▼

Additional Color Codes Table

Color Code	Priority
5	Primary

Power Control

External Gain :

0 dB (Range: 0 — +70 dB)

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 7-158.

See [Table 110 PMP 450i AP Radio attributes - 5 GHz](#) on page 7-124.

Radio page - PMP 450 SM 3.5 GHz

Table 121 PMP 450 SM Radio attributes – 3.5 GHz

Radio Configuration

The unit is configured for United States, but the network has overridden it to Other ETSI+DFS

<input type="checkbox"/>	3302.500	<input type="checkbox"/>	3302.504	<input type="checkbox"/>	3302.555	<input type="checkbox"/>	3302.600	<input type="checkbox"/>	3302.655
<input type="checkbox"/>	3305.000	<input type="checkbox"/>	3310.000	<input type="checkbox"/>	3315.000	<input type="checkbox"/>	3320.000	<input type="checkbox"/>	3325.000
<input type="checkbox"/>	3330.000	<input type="checkbox"/>	3335.000	<input type="checkbox"/>	3340.000	<input type="checkbox"/>	3345.000	<input type="checkbox"/>	3350.000
<input type="checkbox"/>	3355.000	<input type="checkbox"/>	3360.000	<input type="checkbox"/>	3365.000	<input type="checkbox"/>	3370.000	<input type="checkbox"/>	3375.000
<input type="checkbox"/>	3380.000	<input type="checkbox"/>	3385.000	<input type="checkbox"/>	3390.000	<input type="checkbox"/>	3395.000	<input type="checkbox"/>	3400.000
<input checked="" type="checkbox"/>	3405.000	<input checked="" type="checkbox"/>	3410.000	<input checked="" type="checkbox"/>	3415.000	<input checked="" type="checkbox"/>	3420.000	<input checked="" type="checkbox"/>	3425.000
<input checked="" type="checkbox"/>	3430.000	<input checked="" type="checkbox"/>	3435.000	<input checked="" type="checkbox"/>	3440.000	<input checked="" type="checkbox"/>	3445.000	<input checked="" type="checkbox"/>	3450.000
<input checked="" type="checkbox"/>	3455.000	<input checked="" type="checkbox"/>	3460.000	<input checked="" type="checkbox"/>	3465.000	<input checked="" type="checkbox"/>	3470.000	<input checked="" type="checkbox"/>	3475.000
<input checked="" type="checkbox"/>	3480.000	<input checked="" type="checkbox"/>	3485.000	<input checked="" type="checkbox"/>	3490.000	<input checked="" type="checkbox"/>	3495.000	<input checked="" type="checkbox"/>	3500.000
Custom Radio Frequency Scan Selection List :									
<input checked="" type="checkbox"/>	3505.000	<input checked="" type="checkbox"/>	3510.000	<input checked="" type="checkbox"/>	3515.000	<input checked="" type="checkbox"/>	3520.000	<input checked="" type="checkbox"/>	3525.000
<input checked="" type="checkbox"/>	3530.000	<input checked="" type="checkbox"/>	3535.000	<input checked="" type="checkbox"/>	3540.000	<input checked="" type="checkbox"/>	3545.000	<input checked="" type="checkbox"/>	3550.000
<input checked="" type="checkbox"/>	3555.000	<input checked="" type="checkbox"/>	3560.000	<input checked="" type="checkbox"/>	3565.000	<input checked="" type="checkbox"/>	3570.000	<input checked="" type="checkbox"/>	3575.000
<input checked="" type="checkbox"/>	3580.000	<input checked="" type="checkbox"/>	3585.000	<input checked="" type="checkbox"/>	3590.000	<input checked="" type="checkbox"/>	3595.000	<input type="checkbox"/>	3597.499
<input type="checkbox"/>	3597.500								

5 MHz only
 7 MHz only
 10 MHz only
 Not available in this region

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 : (0—254) / Priority

Installation Color Code : Enabled
 Disabled

Large VC data Q : Enabled
 Disabled

Additional Color Codes

Color Code : (0—254) / Priority

Additional Color Codes Table

No additional color codes configured

Power Control

External Gain : dB (Range: 0 — +70 dB)

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 7-158.

See [Table 110 PMP 450i AP Radio attributes - 5 GHz](#) on page 7-124.

Radio page - PMP 450 SM 2.4 GHz

Table 122 PMP 450 SM Radio attributes – 2.4 GHz

Radio Configuration ☰

	<input checked="" type="checkbox"/> 2402.5 <input checked="" type="checkbox"/> 2405.0 <input checked="" type="checkbox"/> 2407.5 <input checked="" type="checkbox"/> 2410.0 <input checked="" type="checkbox"/> 2412.5 <input checked="" type="checkbox"/> 2415.0 <input checked="" type="checkbox"/> 2417.5 <input checked="" type="checkbox"/> 2420.0 <input checked="" type="checkbox"/> 2422.5 <input checked="" type="checkbox"/> 2425.0 <input checked="" type="checkbox"/> 2427.5 <input checked="" type="checkbox"/> 2430.0 <input checked="" type="checkbox"/> 2432.5 <input checked="" type="checkbox"/> 2435.0 <input checked="" type="checkbox"/> 2437.5 <input checked="" type="checkbox"/> 2440.0 <input checked="" type="checkbox"/> 2442.5 <input checked="" type="checkbox"/> 2445.0 <input checked="" type="checkbox"/> 2447.5 <input checked="" type="checkbox"/> 2450.0 <input checked="" type="checkbox"/> 2452.5 <input checked="" type="checkbox"/> 2455.0 <input checked="" type="checkbox"/> 2457.5 <input checked="" type="checkbox"/> 2460.0 <input checked="" type="checkbox"/> 2462.5 <input checked="" type="checkbox"/> 2465.0 <input checked="" type="checkbox"/> 2467.5 <input checked="" type="checkbox"/> 2470.0 <input checked="" type="checkbox"/> 2472.5 <input checked="" type="checkbox"/> 2475.0 <input type="checkbox"/> 2477.5 <input type="checkbox"/> 2480.0
Custom Radio Frequency Scan Selection List :	5 MHz only 10 MHz only Not available in this region <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Restore"/>
Channel Bandwidth Scan :	<input checked="" type="checkbox"/> 5 MHz <input checked="" type="checkbox"/> 10 MHz <input checked="" type="checkbox"/> 20 MHz
Cyclic Prefix Scan :	<input checked="" type="checkbox"/> One Sixteenth
AP Selection Method :	<input type="radio"/> Power Level <input checked="" type="radio"/> Optimize for Throughput
Color Code 1 :	24 (0—254) / Priority Primary ▼
Installation Color Code :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Additional Color Codes ☰

Color Code :	0 (0—254) / Priority Primary ▼
	<input type="button" value="Add/Modify Color Code"/> <input type="button" value="Remove Color Code"/>

Additional Color Codes Table ☰

Color Code	Priority
1	Primary
2	Secondary
3	Tertiary
11	Primary
22	Secondary
33	Tertiary
111	Primary
222	Secondary
254	Tertiary

Power Control ☰

External Gain :	0 dB (Range: 0 — +35 dB)
-----------------	----------------------------

Advanced ☰

Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 7-158.
See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.	

Radio page - PMP 450 SM 900 MHz

Table 123 PMP 450 SM Radio attributes –900 MHz

Radio Configuration

	<input type="checkbox"/> 904.50 <input type="checkbox"/> 905.00 <input checked="" type="checkbox"/> 905.50 <input checked="" type="checkbox"/> 906.00 <input checked="" type="checkbox"/> 906.50 <input type="checkbox"/> 907.00 <input type="checkbox"/> 907.50 <input type="checkbox"/> 908.00 <input type="checkbox"/> 908.50 <input type="checkbox"/> 909.00 <input type="checkbox"/> 909.50 <input type="checkbox"/> 910.00 <input type="checkbox"/> 910.50 <input type="checkbox"/> 911.00 <input type="checkbox"/> 911.50 <input type="checkbox"/> 912.00 <input type="checkbox"/> 912.50 <input type="checkbox"/> 913.00 <input type="checkbox"/> 913.50 <input type="checkbox"/> 914.00 <input type="checkbox"/> 914.50 <input type="checkbox"/> 915.00 <input type="checkbox"/> 915.50 <input type="checkbox"/> 916.00 <input type="checkbox"/> 916.50 <input checked="" type="checkbox"/> 917.00 <input type="checkbox"/> 917.50 <input type="checkbox"/> 918.00 <input type="checkbox"/> 918.50 <input type="checkbox"/> 919.00 <input type="checkbox"/> 919.50 <input type="checkbox"/> 920.00 <input type="checkbox"/> 920.50 <input type="checkbox"/> 921.00 <input type="checkbox"/> 921.50 <input type="checkbox"/> 922.00 Custom Radio Frequency Scan Selection List : <input type="checkbox"/> 922.50 <input type="checkbox"/> 923.00 <input checked="" type="checkbox"/> 923.50 <input checked="" type="checkbox"/> 924.00 <input checked="" type="checkbox"/> 924.50 <input type="checkbox"/> 924.75 <input type="checkbox"/> 925.00 <input type="checkbox"/> 925.50
	5 MHz only <=7 MHz <= 10 MHz Not available in this region <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Restore"/>
Channel Bandwidth Scan :	<input type="checkbox"/> 5 MHz <input type="checkbox"/> 7 MHz <input checked="" type="checkbox"/> 10 MHz <input type="checkbox"/> 20 MHz
Cyclic Prefix Scan :	<input checked="" type="checkbox"/> One Sixteenth
AP Selection Method :	<input type="radio"/> Power Level <input checked="" type="radio"/> Optimize for Throughput
Color Code 1 :	65 (0—254) / Priority Primary ▼
Installation Color Code :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Additional Color Codes

Color Code :	5 (0—254) / Priority Tertiary ▼
	<input type="button" value="Add/Modify Color Code"/> <input type="button" value="Remove Color Code"/>

Additional Color Codes Table

Color Code	Priority
0	Primary
1	Secondary
5	Tertiary

Power Control

External Gain :	0 dB (Range: 0 — +40 dB)
-----------------	----------------------------

Advanced

Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
-------------------------	--

Attribute	Meaning
Custom Radio Frequency Scan Selection List	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.
Channel Bandwidth	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.

Page 7-154

Scan	
Cyclic Prefix Scan	
AP Selection Method	
Color Code 1	
Installation Color Code	
Large VC data Queue	
Color Code	
External Gain	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124
Receive Quality Debug	See Table 110 PMP 450i AP Radio attributes - 5 GHz on page 7-124.

**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 7-161) and cannot see it in the pull down menu.

Radio page - PTP 450 BHM 5 GHz

Table 124 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled OFF ▾															
Frame Alignment Legacy Mode :	Choose Legacy Mode setting from the table below based on collocated radio's software revision and sync source: <table border="1" style="margin-top: 10px;"> <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
-----------	---------

Refer [Table 113 PTP 450i BHM Radio page attributes – 5 GHz](#) on page 7-138 for all parameters details.

Radio page - PTP 450 BHS 5 GHz

Table 125 PTP 450 BHM Radio attributes –5 GHz

Radio Configuration

5.4 GHz

<input checked="" type="checkbox"/> 5472.5	<input type="checkbox"/> 5475.0	<input type="checkbox"/> 5477.5	<input type="checkbox"/> 5480.0	<input type="checkbox"/> 5482.5	<input type="checkbox"/> 5485.0
<input type="checkbox"/> 5487.5	<input type="checkbox"/> 5490.0	<input type="checkbox"/> 5492.5	<input type="checkbox"/> 5495.0	<input type="checkbox"/> 5497.5	<input type="checkbox"/> 5500.0
<input type="checkbox"/> 5502.5	<input type="checkbox"/> 5505.0	<input type="checkbox"/> 5507.5	<input type="checkbox"/> 5510.0	<input type="checkbox"/> 5512.5	<input type="checkbox"/> 5515.0
<input type="checkbox"/> 5517.5	<input type="checkbox"/> 5520.0	<input type="checkbox"/> 5522.5	<input type="checkbox"/> 5525.0	<input type="checkbox"/> 5527.5	<input type="checkbox"/> 5530.0
<input type="checkbox"/> 5532.5	<input type="checkbox"/> 5535.0	<input type="checkbox"/> 5537.5	<input type="checkbox"/> 5540.0	<input type="checkbox"/> 5542.5	<input type="checkbox"/> 5545.0
<input type="checkbox"/> 5547.5	<input type="checkbox"/> 5550.0	<input type="checkbox"/> 5552.5	<input type="checkbox"/> 5555.0	<input type="checkbox"/> 5557.5	<input type="checkbox"/> 5560.0
<input type="checkbox"/> 5562.5	<input type="checkbox"/> 5565.0	<input type="checkbox"/> 5567.5	<input type="checkbox"/> 5570.0	<input type="checkbox"/> 5572.5	<input type="checkbox"/> 5575.0
<input type="checkbox"/> 5577.5	<input type="checkbox"/> 5580.0	<input type="checkbox"/> 5582.5	<input type="checkbox"/> 5585.0	<input type="checkbox"/> 5587.5	<input type="checkbox"/> 5590.0
<input type="checkbox"/> 5592.5	<input type="checkbox"/> 5595.0	<input checked="" type="checkbox"/> 5597.5	<input type="checkbox"/> 5600.0	<input type="checkbox"/> 5602.5	<input type="checkbox"/> 5605.0
<input type="checkbox"/> 5607.5	<input type="checkbox"/> 5610.0	<input type="checkbox"/> 5612.5	<input type="checkbox"/> 5615.0	<input type="checkbox"/> 5617.5	<input type="checkbox"/> 5620.0
<input type="checkbox"/> 5622.5	<input type="checkbox"/> 5625.0	<input type="checkbox"/> 5627.5	<input type="checkbox"/> 5630.0	<input type="checkbox"/> 5632.5	<input type="checkbox"/> 5635.0
<input type="checkbox"/> 5637.5	<input type="checkbox"/> 5640.0	<input type="checkbox"/> 5642.5	<input type="checkbox"/> 5645.0	<input type="checkbox"/> 5647.5	<input type="checkbox"/> 5650.0
<input checked="" type="checkbox"/> 5652.5	<input type="checkbox"/> 5655.0	<input type="checkbox"/> 5657.5	<input type="checkbox"/> 5660.0	<input type="checkbox"/> 5662.5	<input type="checkbox"/> 5665.0
<input type="checkbox"/> 5667.5	<input type="checkbox"/> 5670.0	<input type="checkbox"/> 5672.5	<input type="checkbox"/> 5675.0	<input type="checkbox"/> 5677.5	<input checked="" type="checkbox"/> 5680.0
<input type="checkbox"/> 5682.5	<input type="checkbox"/> 5685.0	<input type="checkbox"/> 5687.5	<input type="checkbox"/> 5690.0	<input type="checkbox"/> 5692.5	<input type="checkbox"/> 5695.0
<input type="checkbox"/> 5697.5	<input type="checkbox"/> 5700.0	<input type="checkbox"/> 5702.5	<input type="checkbox"/> 5705.0	<input type="checkbox"/> 5707.5	<input type="checkbox"/> 5710.0
<input type="checkbox"/> 5712.5	<input type="checkbox"/> 5715.0	<input type="checkbox"/> 5717.5	<input type="checkbox"/> 5720.0	<input checked="" type="checkbox"/> 5722.5	

Custom Radio Frequency Scan Selection List :

5.7 GHz

<input checked="" type="checkbox"/> 5727.5	<input type="checkbox"/> 5730.0	<input type="checkbox"/> 5732.5	<input type="checkbox"/> 5735.0	<input type="checkbox"/> 5737.5	<input type="checkbox"/> 5740.0
<input type="checkbox"/> 5742.5	<input type="checkbox"/> 5745.0	<input type="checkbox"/> 5747.5	<input type="checkbox"/> 5750.0	<input type="checkbox"/> 5752.5	<input type="checkbox"/> 5755.0
<input type="checkbox"/> 5757.5	<input type="checkbox"/> 5760.0	<input type="checkbox"/> 5762.5	<input type="checkbox"/> 5765.0	<input type="checkbox"/> 5767.5	<input type="checkbox"/> 5770.0
<input type="checkbox"/> 5772.5	<input type="checkbox"/> 5775.0	<input type="checkbox"/> 5777.5	<input type="checkbox"/> 5780.0	<input type="checkbox"/> 5782.5	<input type="checkbox"/> 5785.0
<input type="checkbox"/> 5787.5	<input type="checkbox"/> 5790.0	<input type="checkbox"/> 5792.5	<input type="checkbox"/> 5795.0	<input type="checkbox"/> 5797.5	<input type="checkbox"/> 5800.0
<input type="checkbox"/> 5802.5	<input type="checkbox"/> 5805.0	<input type="checkbox"/> 5807.5	<input type="checkbox"/> 5810.0	<input type="checkbox"/> 5812.5	<input type="checkbox"/> 5815.0
<input type="checkbox"/> 5817.5	<input type="checkbox"/> 5820.0	<input type="checkbox"/> 5822.5	<input type="checkbox"/> 5825.0	<input type="checkbox"/> 5827.5	<input type="checkbox"/> 5830.0
<input type="checkbox"/> 5832.5	<input type="checkbox"/> 5835.0	<input type="checkbox"/> 5837.5	<input type="checkbox"/> 5840.0	<input type="checkbox"/> 5842.5	<input type="checkbox"/> 5845.0
<input type="checkbox"/> 5847.5	<input type="checkbox"/> 5850.0	<input type="checkbox"/> 5852.5	<input type="checkbox"/> 5855.0	<input type="checkbox"/> 5857.5	<input type="checkbox"/> 5860.0
<input type="checkbox"/> 5862.5	<input type="checkbox"/> 5865.0	<input type="checkbox"/> 5867.5	<input type="checkbox"/> 5870.0	<input checked="" type="checkbox"/> 5872.5	<input type="checkbox"/> 5875.0
<input type="checkbox"/> 5877.5	<input type="checkbox"/> 5880.0	<input type="checkbox"/> 5882.5	<input type="checkbox"/> 5885.0	<input type="checkbox"/> 5887.5	<input type="checkbox"/> 5890.0
<input type="checkbox"/> 5892.5	<input type="checkbox"/> 5895.0	<input type="checkbox"/> 5897.5			

≤ 10 MHz
Not available in this region

Select All
Select All 5.4
Select All 5.7
Clear All
Restore

Channel Bandwidth Scan : 10 MHz 20 MHz

Cyclic Prefix Scan : One Sixteenth

Color Code : (0—254)

Large VC data Q : Enabled Disabled

Power Control

Transmit Power : dBm (Range: -30 — +6 dBm) (-3 dBm V / -3 dBm H)

External Gain : dB (Range: 0 — +40 dB)

Advanced

Receive Quality Debug : Enabled Disabled

Attribute	Meaning
Refer Table 114 PTP 450i BHS Radio attributes – 5 GHz on page 7-141 for all parameters details.	

Page 7-157

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

- Actual Multicast CIR honored by the AP = Configured Multicast CINR/ (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 126](#).

Table 126 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 AP. The SM displays the multicast row if it is a PMP 450 platform.

Figure 117 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	nucast pkts	discards	errors	QPSK frgmts	16-QAM frgmts	64-QAM frgmts	256-QAM frgmts	octets	ucast pkts	nucast pkts	discards			errors
Site Name - LUID: 002	018	00	2144887	6558	1121	0	0	5649 2098	3378 1656	2019 1607	1950 1199	2060928	7088	63	0	0	0	3972
Multicast	016	00	NA	NA	NA	NA	NA	NA	NA	NA	NA	0	0	0	0	0	0	NA
Broadcast	012	00	NA	NA	NA	NA	NA	NA	NA	NA	NA	592059	16	8523	0	0	0	NA

The AP and SM display Transmit and Receive Multicast Data Count (under the **Statistics > Scheduler** page), as shown in [Figure 118](#).

Figure 118 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
Overrun 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 127](#).

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 127 PMP/PTP 450 platform AP/SM/BH Custom Frequencies page – 5 GHz

Custom Frequencies Configuration

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

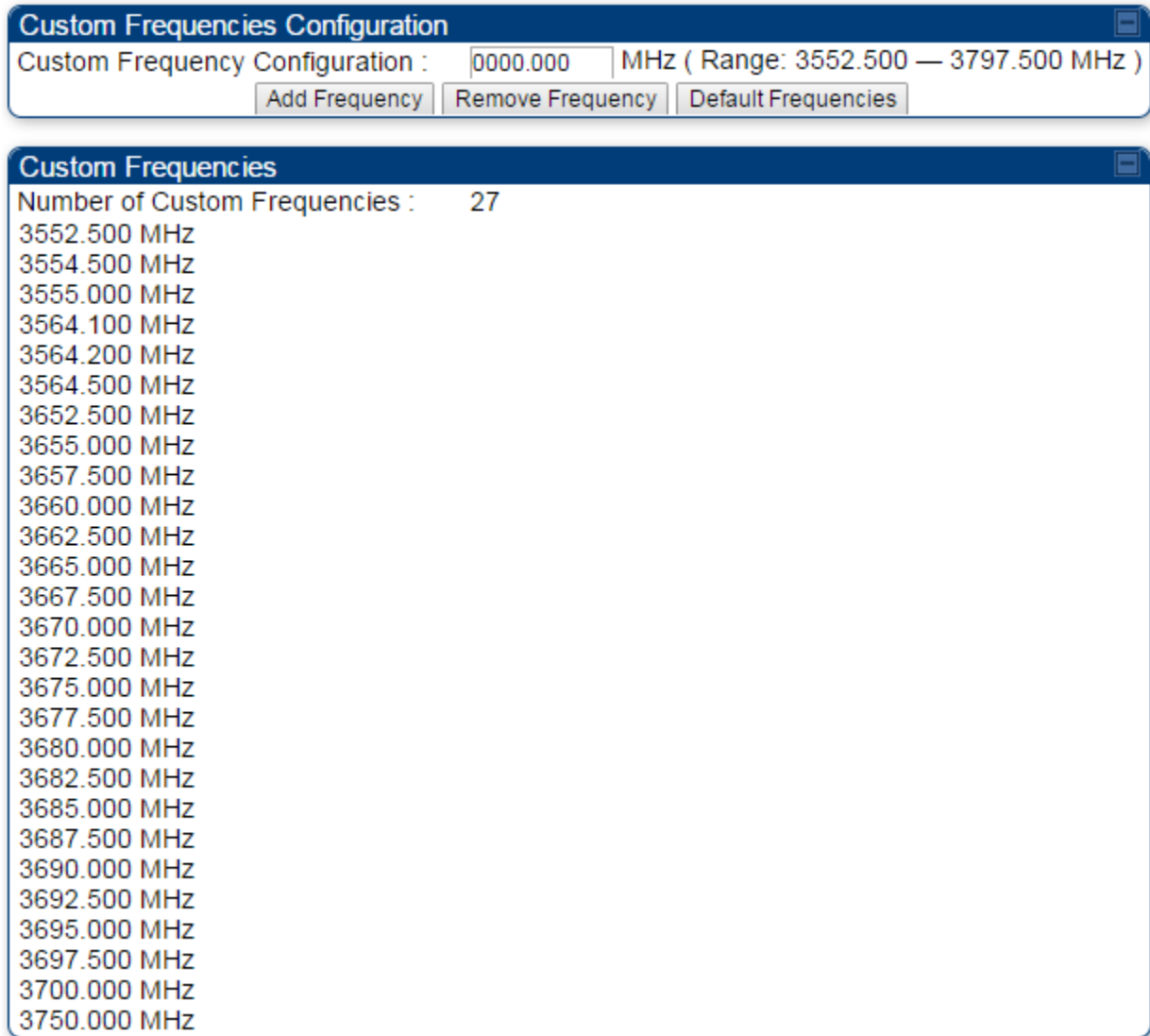
Custom Frequencies

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	<p>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.</p> <p>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.</p>
Custom Frequencies	Displays the complete list of user configured custom frequencies.

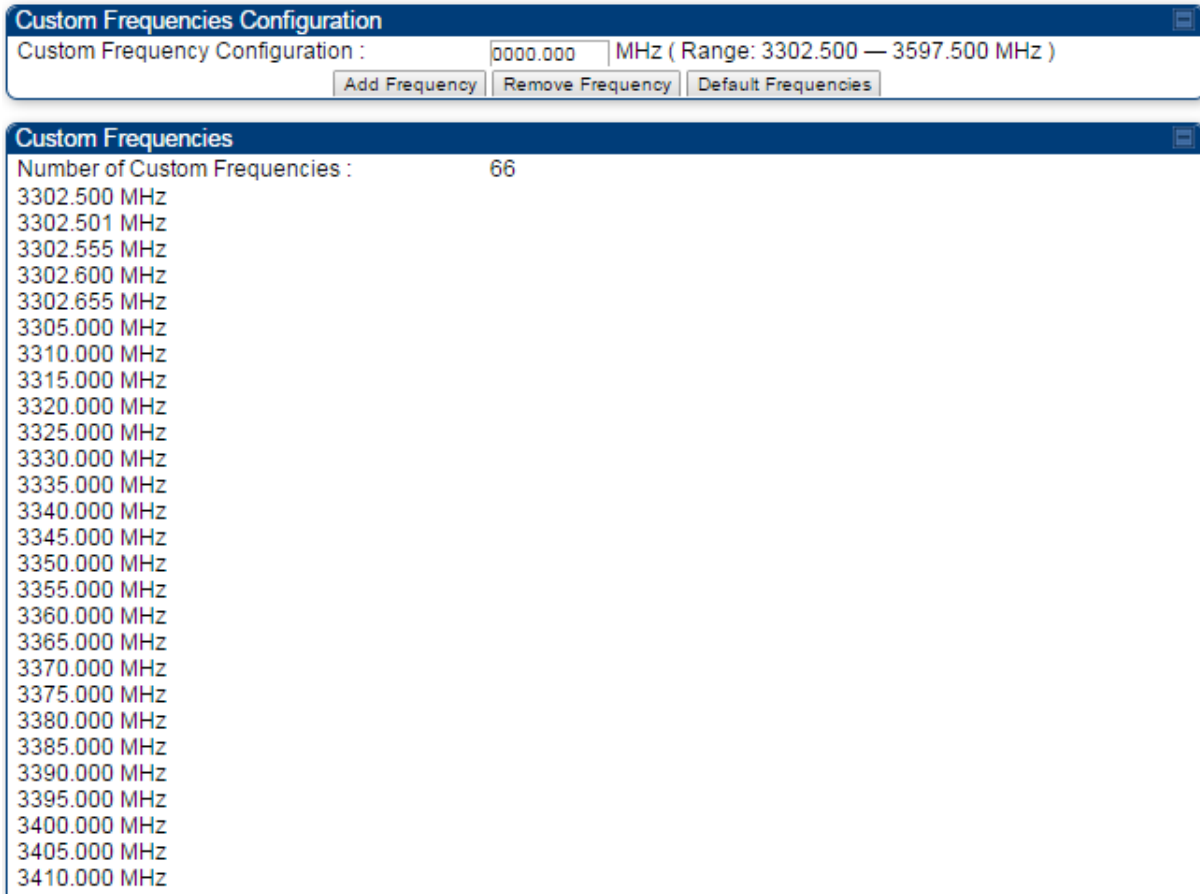
Table 128 PMP/PTP 450 SM/BH Custom Frequencies page – 3.65 GHz



Attribute	Meaning
Custom Frequency Configuration	<p>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.</p> <p>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.</p>
Custom Frequencies	Displays the complete list of user configured custom frequencies.

Table 129 PMP/PTP 450 SM/BH Custom Frequencies page – 3.5 GHz

Attribute	Meaning
Custom Frequency Configuration	<p>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.</p> <p>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.</p>



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 119 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 223](#) on page [10-34](#).

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 in the sector are shown in the table below.

Table 130 Contention slots and number of VCs

Number of VCs	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 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

PMP/PTP 450 platform 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 PMP 450 are shown in [Table 131](#).

Table 131 PMP/PTP 450 platform 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
265-QAM	8X MIMO-B	4X MIMO-A

System Performance

For System Performance details of all the PMP/PTP 450 platform Series products please refer the Link Capacity Planner at:

<https://support.cambiumnetworks.com/files/pmp450>.

Table 132 Co-channel Interference per (CCI) MCS

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

4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	17 dB
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	25 dB
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	33 dB

Table 133 Adjacent Channel Interference (ACI) per MCS

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

Guard Band

No Guard Bands are needed for the 5.4 GHz and 5.8 GHz bands.

Improved PPS performance of PMP 450 and 450i SMs

The PMP 450 platforms Series provides improved packets per second (PPS) performance with regards to the PMP 450. Through hardware and software enhancements, the PPS performance of the PMP 450i AP has been improved to 40000 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.

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 PMP/PTP 450 platform 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 134 LAN1 Network Interface Configuration tab of IP page attributes

LAN1 Network Interface Configuration	
IP Address :	169.254.1.1
Network Accessibility :	<input type="radio"/> Public <input checked="" type="radio"/> Local
Subnet Mask :	255.255.255.0
Gateway IP Address :	169.254.0.0
DHCP state :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DHCP DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically <input type="radio"/> 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 135](#).

Table 135 SNMP page attributes

SNMPv2c Settings	
SNMP Community String 1 :	Canopy
SNMP Community String 1 Permissions :	<input type="radio"/> Read Only <input checked="" type="radio"/> Read / Write
SNMP Community String 2 (Read Only) :	Canopyro

SNMPv3 Settings	
Engine ID :	800000a1030a003ea004be <input type="button" value="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 <input type="radio"/> Enable R/W User Note:Also enable SNMPv2c Permission to be R/W <input checked="" type="radio"/> Disable R/W User
SNMPv3 Read/Write 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 :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> 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 :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Session Status :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Site Information	
Site Information Viewable to Guest Users :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 field allows for a read-only user per device. The default values for the Read-Only users is: <ul style="list-style-type: none"> • 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 : <ul style="list-style-type: none"> • 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	<p>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</p> <ul style="list-style-type: none"> • The network IP address in the form xxx.xxx.xxx.xxx • The CIDR (Classless Interdomain Routing) prefix length in the form /xx <p>For example:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p>
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	<p>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</p> <ul style="list-style-type: none"> • 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.
