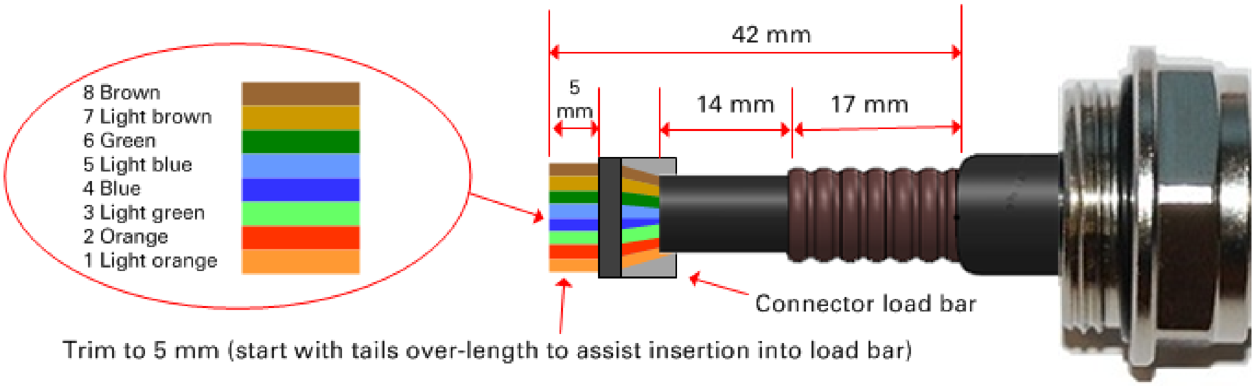
Supplemental installation information

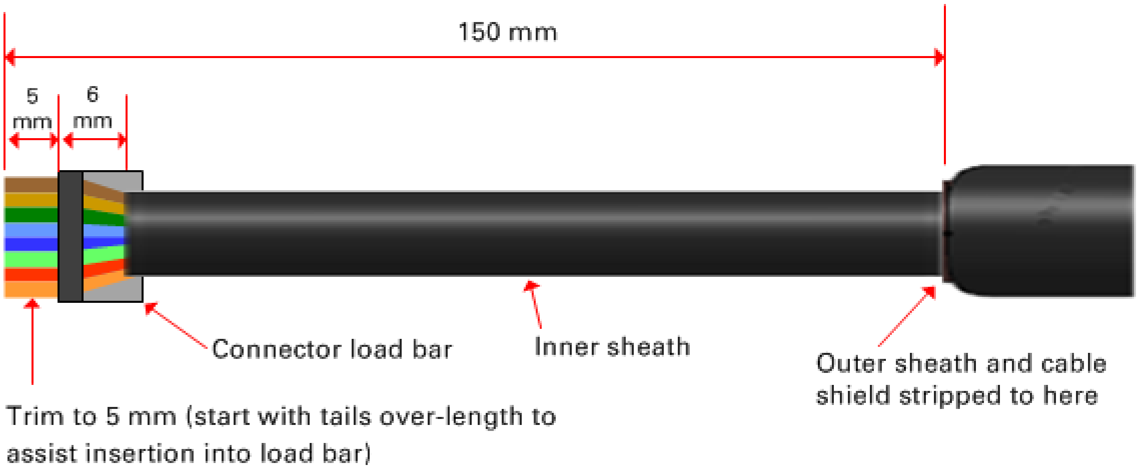
This section contains detailed installation procedures that are not included in the above topics, such as how to strip cables, create grounding points and weatherproof connectors.

Stripping drop cable

When preparing drop cable for connection to the PMP/PTP 450i ODU or LPU, use the following measurements:



When preparing drop cable for connection to the PMP/PTP 450i PSU (without a cable gland), use the following measurements:

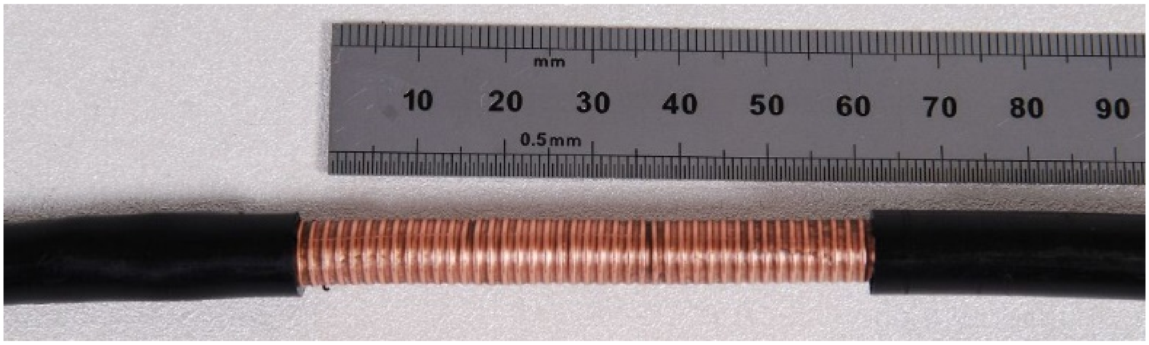

150 mm
5 mm
6 mm
Connector load bar
Inner sheath
Outer sheath and cable shield stripped to here
Trim to 5 mm (start with tails over-length to assist insertion into load bar)

Creating a drop cable grounding point

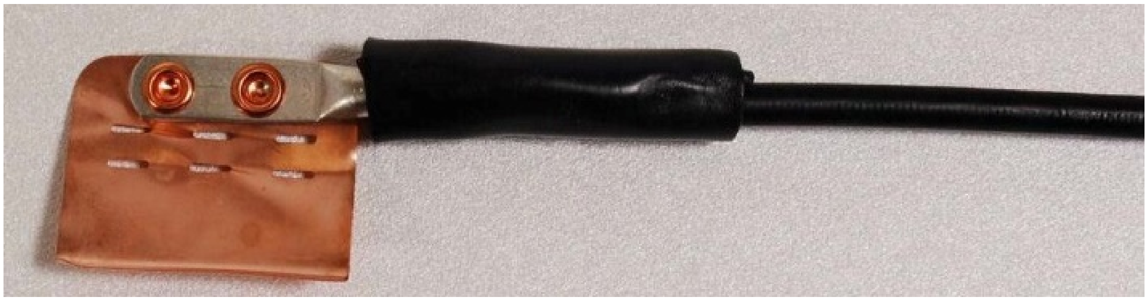
Use this procedure to connect the screen of the main drop cable to the metal of the supporting structure using the cable grounding kit (Cambium part number 01010419001).

To identify suitable grounding points, refer to Drop cable grounding points on page 3-12.

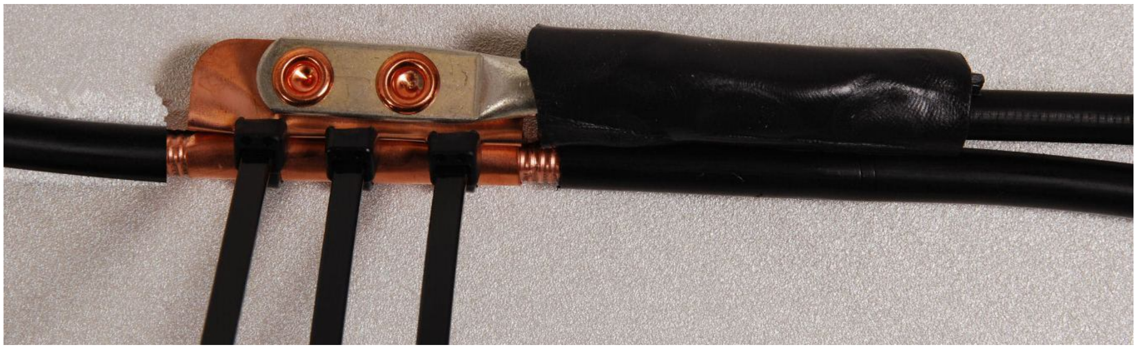
1 Remove 60 mm (2.5 inches) of the drop cable outer sheath.



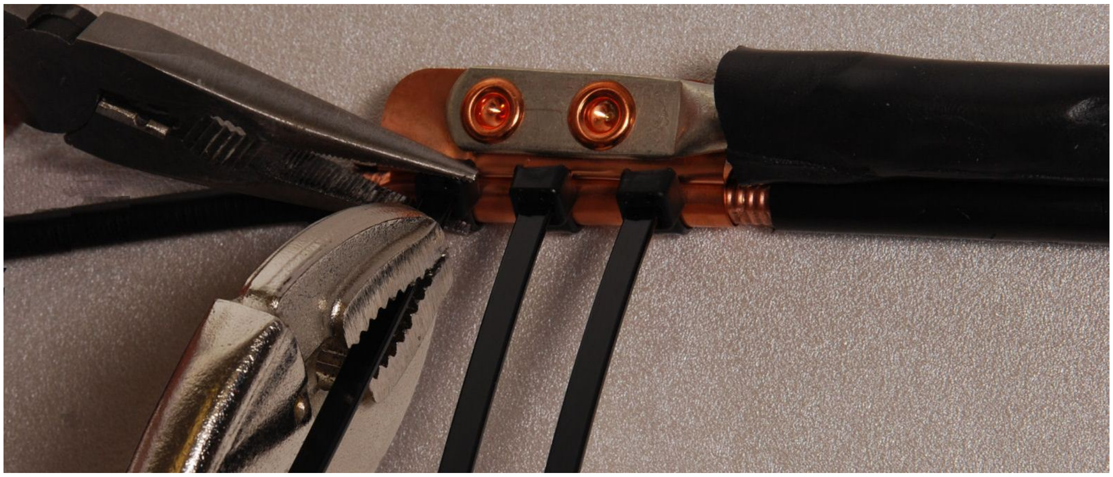
2 Cut 38mm (1.5 inches) of rubber tape (self-amalgamating) and fit to the ground cable lug. Wrap the tape completely around the lug and cable.



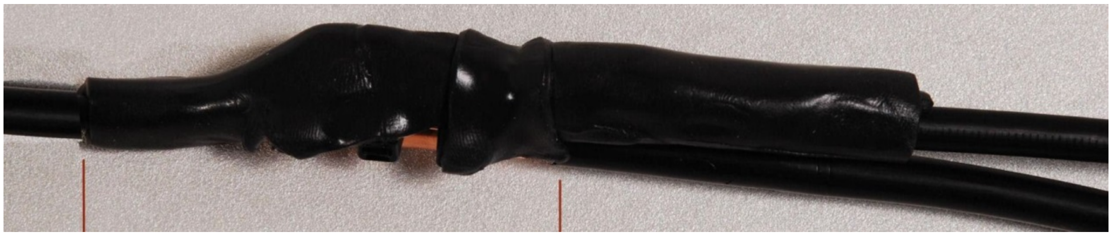
3 Fold the ground wire strap around the drop cable screen and fit cable ties.



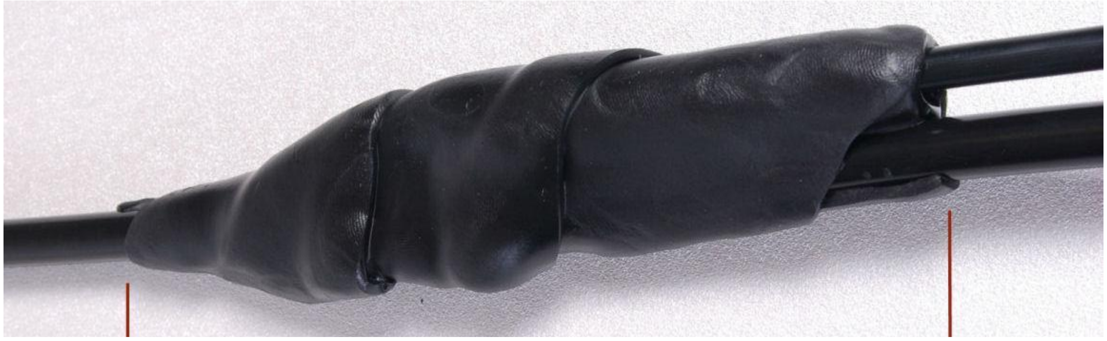
4 Tighten the cable ties with pliers. Cut the surplus from the cable ties.



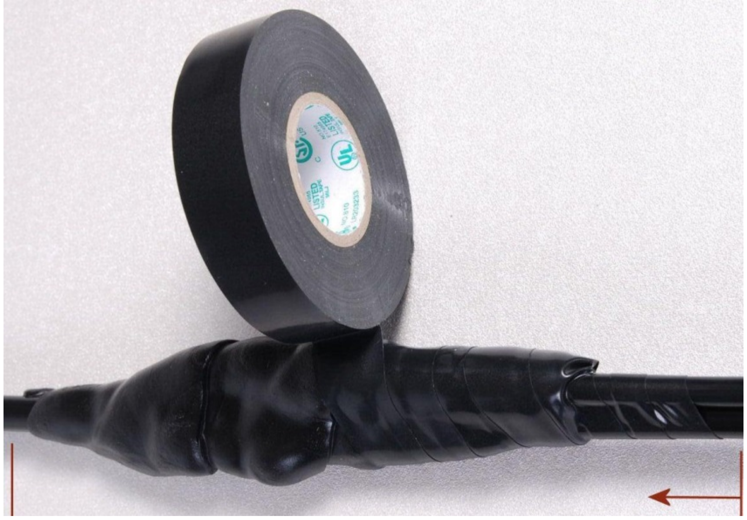
5 Cut a 38mm (1.5 inches) section of self-amalgamating tape and wrap it completely around the joint between the drop and ground cables.



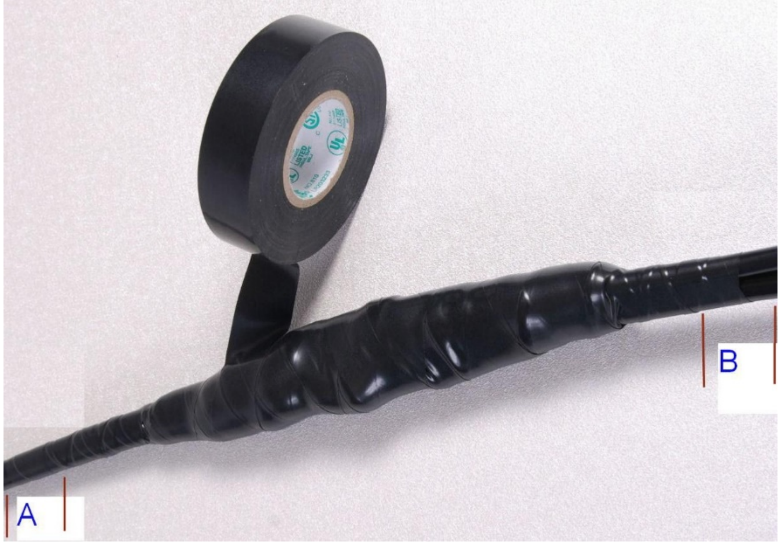
6 Use the remainder of the self-amalgamating tape to wrap the complete assembly. Press the tape edges together so that there are no gaps.



7 Wrap a layer of PVC tape from bottom to top, starting from 25 mm (1 inch) below and finishing 25 mm (1 inch) above the edge of the self-amalgamating tape, overlapping at half width.



8 Repeat with a further four layers of PVC tape, always overlapping at half width. Wrap the layers in alternate directions (top to bottom, then bottom to top). The edges of each layer should be 25mm (1 inch) above (A) and 25 mm (1 inch) below (B) the previous layer.



9 Prepare the metal grounding point of the supporting structure to provide a good electrical contact with the grounding cable clamp. Remove paint, grease or dirt, if present. Apply anti-oxidant compound liberally between the two metals.

10 Clamp the bottom lug of the grounding cable to the supporting structure using site approved methods. Use a two-hole lug secured with fasteners in both holes. This provides better protection than a single-hole lug.

Weatherproofing an N type connector

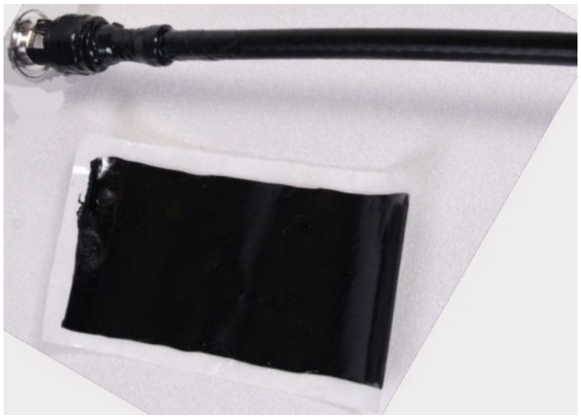
Use this procedure to weatherproof the N type connectors fitted to the connectorized ODU and external antenna (if recommended by the antenna manufacturer).

1 Ensure the connection is tight. A torque wrench should be used if available:

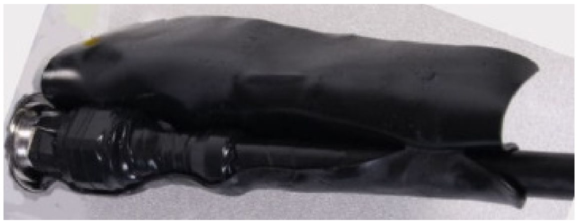
2 Wrap the connection with a layer of 19 mm (0.75 inch) PVC tape, starting 25 mm (1 inch) below the connector body. Overlap the tape to half-width and extend the wrapping to the body of the LPU. Avoid making creases or wrinkles:

3 Smooth the tape edges:

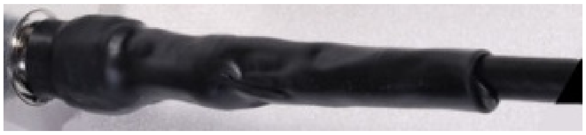
4 Cut a 125mm (5 inches) length of rubber tape (self-amalgamating):



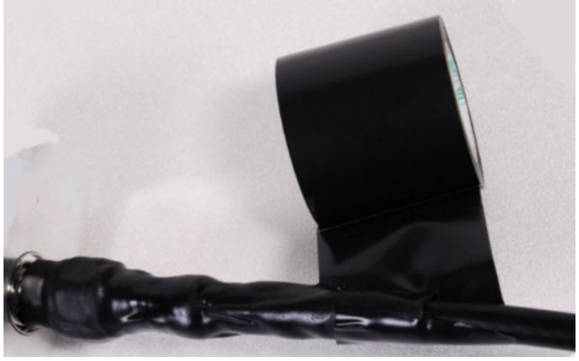
5 Expand the width of the tape by stretching it so that it will wrap completely around the connector and cable:



6 Press the tape edges together so that there are no gaps. The tape should extend 25 mm (1 inch) beyond the PVC tape:



7 Wrap a layer of 50 mm (2 inch) PVC tape from bottom to top, starting from 25 mm (1 inch) below the edge of the self-amalgamating tape, overlapping at half width.



8 Repeat with a further four layers of 19 mm (0.75 inch) PVC tape, always overlapping at half width. Wrap the layers in alternate directions:

- Second layer: top to bottom.
- Third layer: bottom to top.
- Fourth layer: top to bottom.
- Fifth layer: bottom to top.

The bottom edge of each layer should be 25 mm (1 inch) below the previous layer.

9 Check the completed weatherproof connection:

Chapter 7: Configuration

This chapter describes how to use the web interface to configure the PMP/PTP 450i link. This chapter contains the following topics:

Preparing for configuration

This section describes the checks to be performed before proceeding with unit configuration and antenna alignment.

Safety precautions

All national and local safety standards must be followed while configuring the units and aligning the antennas.

Warning

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate RF energy as soon as they are powered up. Respect the safety standards defined in Compliance with safety standards on page 4-22, in particular the minimum separation distances.

Observe the following guidelines:

- Never work in front of the antenna when the ODU is powered.
- Always power down the PSU before connecting or disconnecting the drop cable from the PSU, ODU or LPU.

Regulatory compliance

All applicable radio regulations must be followed while configuring the units and aligning the antennas. For more information, refer to Compliance with radio regulations on page 4-27.

Caution

If the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred before the units are allowed to radiate on site, otherwise the regulations will be infringed.

Attention

Si le concepteur du système a fourni une liste de canaux à interdire pour éviter les radars TDWR, les cannaux concernées doivent être interdits avant que les unités sont autorisées à émettre sur le site, sinon la réglementation peut être enfreinte.

Connecting to the unit

This section describes how to connect the unit to a management PC and power it up.

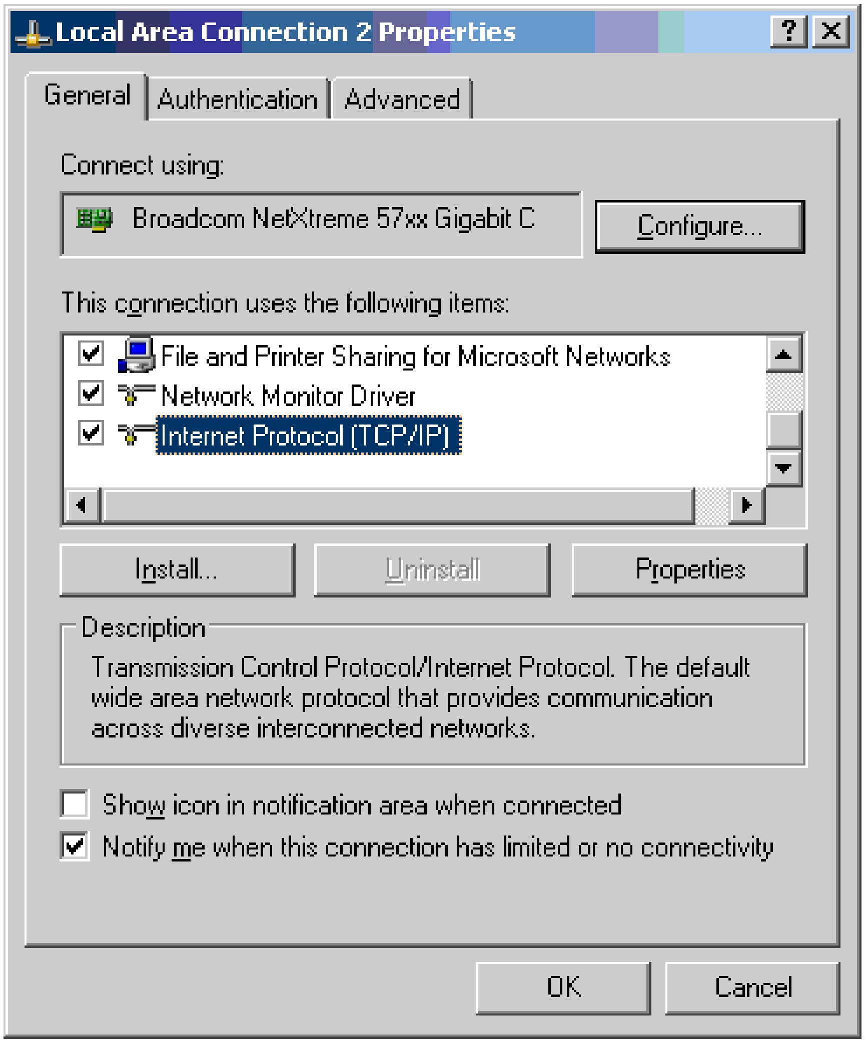
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the PMP/PTP 450i.

Procedure 9 Configuring the management PC

1 Select **Properties** for the Ethernet port. In Windows 7 this is found in **Control Panel > Network and Internet > Network Connections > Local Area Connection.**

2 Select **Internet Protocol (TCP/IP)**:



Connect using:

Broadcom NetXtreme 57xx Gigabit C

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

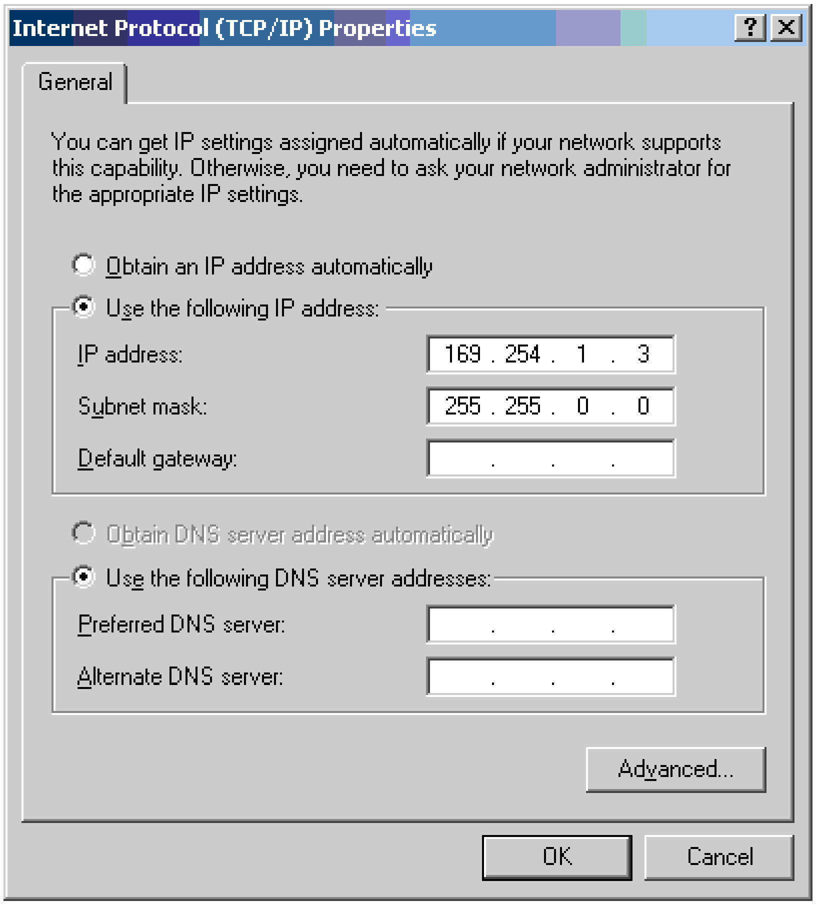
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

3 Click **Properties**.

4 Enter an IP address that is valid for the 169.254.X.X network, avoiding 169.254.0.0 and 169.254.1.1. A good example is 169.254.1.3:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 169 . 254 . 1 . 3

Subnet mask: 255 . 255 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5 Enter a subnet mask of 255.255.0.0. Leave the default gateway blank.

Connecting to the PC and powering up

Use this procedure to connect a management PC and power up the PMP/PTP 450i.

Procedure 10 Connecting to the PC and powering up

1 Check that the ODU and PSU are correctly connected.

2 Connect the PC Ethernet port to the LAN port of the PSU using a standard (not crossed) Ethernet cable.

3 Apply mains or battery power to the PSU. The green Power LED should illuminate continuously.

4 After about several seconds, check that the orange Ethernet LED starts with 10 slow flashes.

5 Check that the Ethernet LED then illuminates continuously.

Using the web interface

This section describes how to log into the PMP/PTP 450i web interface and use its menus.

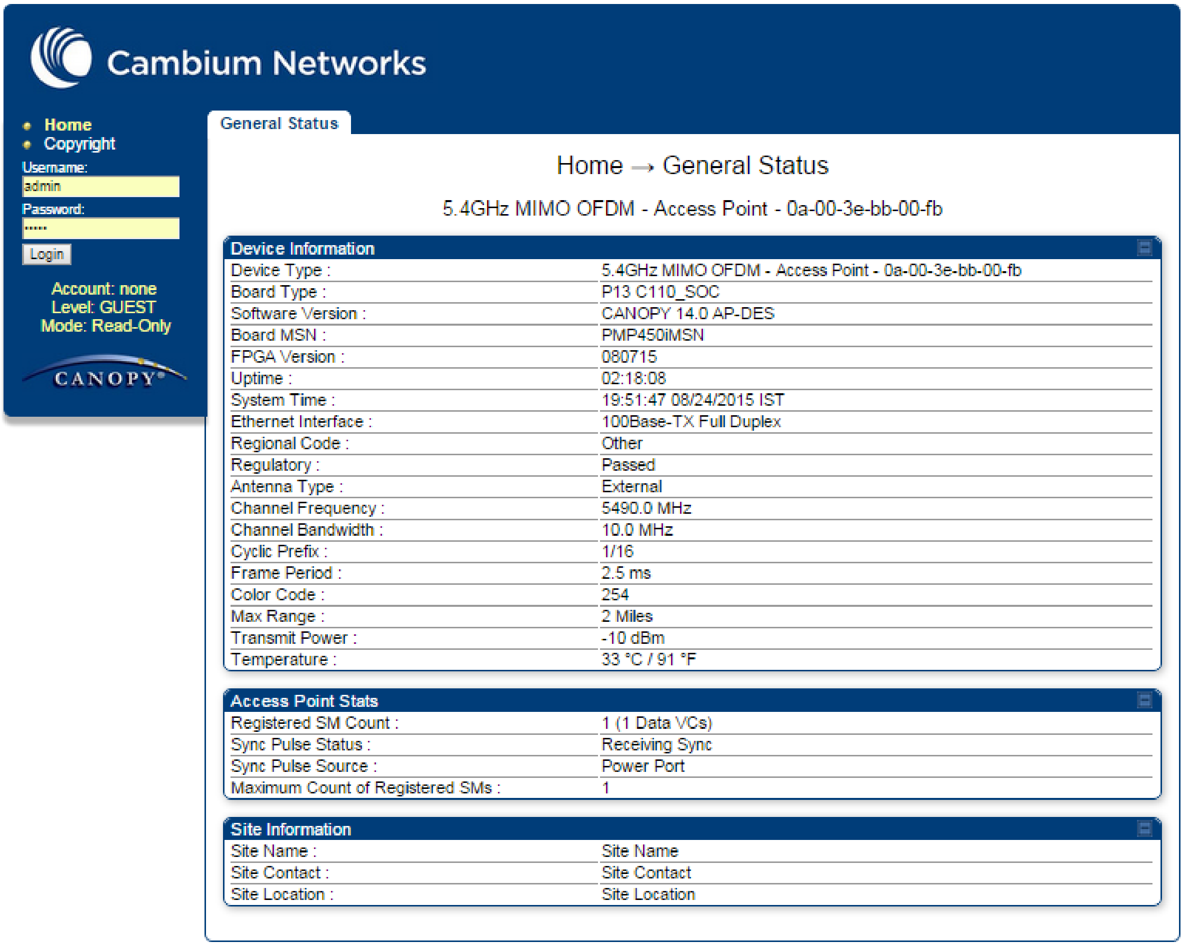
Logging into the web interface

Use this procedure to log into the web interface as a system administrator.

Procedure 11 Logging into the web interface

1 Start the web browser from the management PC.

2 Type the IP address of the unit into the address bar. The factory default IP address is **169.254.1.1**. Press ENTER. The web interface menu and System Summary page are displayed:



Username: admin

Password: •••••

Account: none
Level: GUEST
Mode: Read-Only

Home → General Status

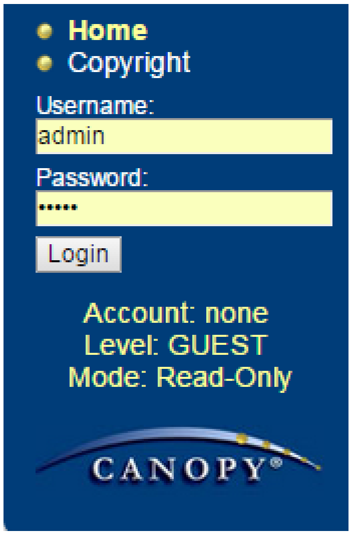
5.4GHz MIMO OFDM - Access Point - 0a-00-3e-bb-00-fb

Device Information	
Device Type :	5.4GHz MIMO OFDM - Access Point - 0a-00-3e-bb-00-fb
Board Type :	P13 C110_SOC
Software Version :	CANOPY 14.0 AP-DES
Board MSN :	PMP450iMSN
FPGA Version :	080715
Uptime :	02:18:08
System Time :	19:51:47 08/24/2015 IST
Ethernet Interface :	100Base-TX Full Duplex
Regional Code :	Other
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	5490.0 MHz
Channel Bandwidth :	10.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Color Code :	254
Max Range :	2 Miles
Transmit Power :	-10 dBm
Temperature :	33 °C / 91 °F

Access Point Stats	
Registered SM Count :	1 (1 Data VCs)
Sync Pulse Status :	Receiving Sync
Sync Pulse Source :	Power Port
Maximum Count of Registered SMs :	1

Site Information	
Site Name :	Site Name
Site Contact :	Site Contact
Site Location :	Site Location

3 On left hand side of home page, the login information is displayed:



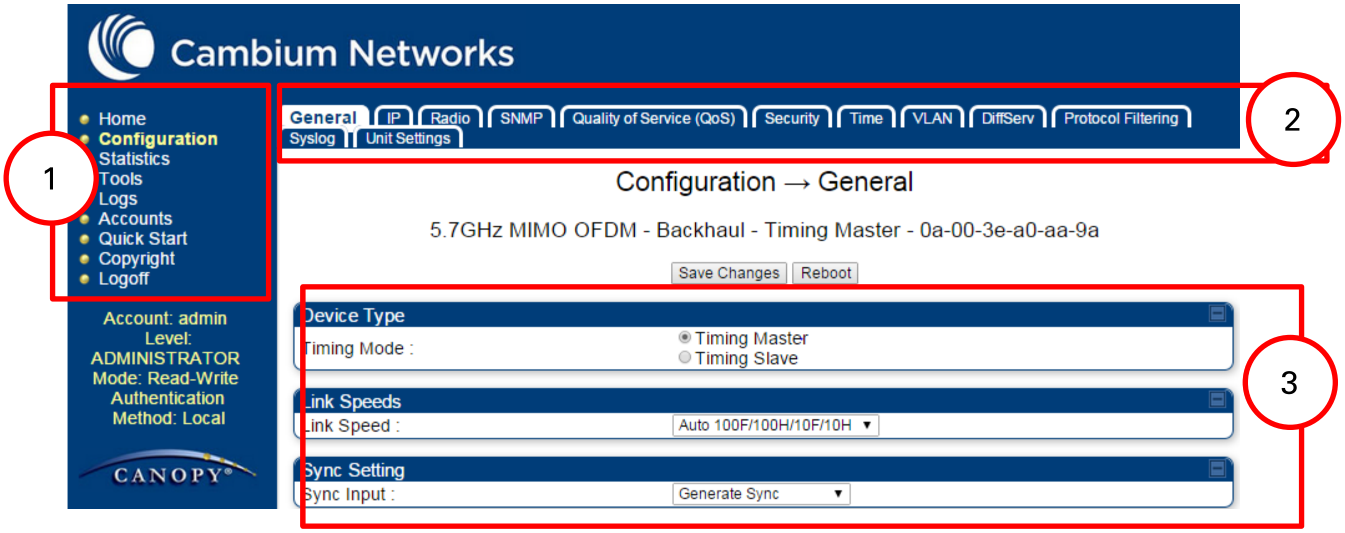
Username:
admin

Password:
•••••

Account: none
Level: GUEST
Mode: Read-Only

4 Enter Username (factory default username is *admin*) and Password (factory default password is *admin*) and click **Login**.

Web GUI



Account: admin
Level:
ADMINISTRATOR
Mode: Read-Write
Authentication
Method: Local

Configuration → General

5.7GHz MIMO OFDM - Backhaul - Timing Master - 0a-00-3e-a0-aa-9a

Device Type

Timing Mode : ● Timing Master ○ Timing Slave

Link Speeds

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

Sync Setting

Sync Input : Generate Sync

Field Name	Description
Main Manu	Click an option in side navigation bar (area marked as “1”). Multiple options in sub-navigation bars appear
Menu Option	Click top sub-navigation bar to choose one configuration page (area marked as “2”)

Parameter	To configure the parameters (e.g. area marked as “3”)
Save Changes	Press "Save Changes" to confirm and save the changes
Reboot	To reboot the ODU

Using the menu options

Use the menu navigation bar in the left panel to navigate to each web page. Some of the menu options are only displayed for specific system configurations. Use Table 54 to locate information about using each web page.

Table 55 Menu options and web pages

Main menu	Menu options	Applicable module	Description
● Home			
	General Status	All	Viewing General Status on page 9-2
	Session Status	AP, BHM	Viewing Session Status on page 9-14
	Event Log	All	Interpreting messages in the Event Log on page 9-19
	Network Infterface	AP, BHM	Viewing the Network Interface on page 9-22
	Layer 2 Neighbors	All	Viewing the Layer 2 Neighbors on page 9-23
● Configuration			
	General	All	General page on page 7-69
	IP	All	Configuring IP and Ethernet interfaces on page 7-25
	Radio	All	Radio configuration page on page 7-116
	SNMP	All	Setting up SNMP agent on page 7-136
	Qaulity of Service (QoS)	All	Configuring quality of service on page 7-153

Main menu	Menu options	Applicable module	Description
	Security	All	Configuring security on page 7-90
	Time	AP, BHM	Time page of AP/BHM on page 7-86
	VLAN	All	VLAN Remarking and Priority bits configuration – AP/SM on page 7-45 VLAN configuration for PTP on page 7-54
	DiffServ	All	IPv4 and IPv6 Prioritization on page 7-61
	Protocol Filtering	All	Filtering protocols and ports on page 7-62
	Syslog	All	Configuring syslog on page 7-141
	Unit Setting	All	Unit Settings page on page 7-82
● Statistics			
	Scheduler	All	Viewing the Scheduler statistics on page 9-24
	Registration Failures	AP, BHM	Viewing list of Registration Failures statistics on page 9-26
	Bridge Control Block	All	Interpreting Bridge Control Block statistics on page 9-49
	Bridging Table	All	Interpreting Bridging Table statistics on page 9-27
	Ethernet	All	Interpreting Ethernet statistics on page 9-29
	Radio	All	Interpreting RF Control Block statistics on page 9-32
	VLAN	All	Interpreting VLAN statistics on page 9-33
	Data VC	All	Interpreting Data VC statistics on page 9-35
	Throughput	AP, BHM	Interpreting Throughput statistics on page 9-37
	Filter	SM	Interpreting Filter statistics on page 9-42

Main menu	Menu options	Applicable module	Description
	ARP	SM	Viewing ARP statistics on page 9-43
	Overload	All	Interpreting Overload statistics on page 9-40
	Syslog Statistics	All	Interpreting syslog statistics on page 9-54
	Translation Table	SM	Interpreting Translation Table statistics on page 9-28
	DHCP Relay	SM	Interpreting DHCP Relay statistics on page 9-41
	NAT Stats	SM	Viewing NAT statistics on page 9-44
	NAT DHCP	SM	Viewing NAT DHCP Statistics on page 9-46
	Pass Through Statistics	AP	Interpreting Pass Through Statistics on page 9-51
	Sync Status	AP	Interpreting Sync Status statistics on page 9-47
	PPPoE	SM	Interpreting PPPoE Statistics for Customer Activities on page 9-48
	SNMPv3 Statistics	All	Interpreting SNMPv3 Statistics on page 9-52
	Frame Utilization		Interpreting SNMPv3 Statistics on page 9-52
● Tools			
	Link Capacity Test	All	Using the Link Capacity Test tool on page 8-19
	Spectrum Analyzer	All	Spectrum Analyzer tool on page 8-3
	Remote Spectrum Analyzer	All	Remote Spectrum Analyzer tool on page 8-10
	AP/BHM Evaluation	SM, BHS	Using AP Evaluation tool on page 8-22 Using BHM Evaluation tool on page 8-26
	Subscriber Configuration	AP	Using the Subscriber Configuration tool on page 8-34

Main menu	Menu options	Applicable module	Description
	OFDM Frame Calculator	AP, BHM	Using the OFDM Frame Calculator tool on page 8-30
	BER results	SM	Using BER Results tool on page 8-38
	Alignment Tool	SM, BHS	Using the Alignment Tool on page 8-13
	Link Status	AP	Using the Link Status tool on page 8-35
	Sessions	AP	Using the Sessions tool on page 8-39
● Logs			
● Accounts			
	Change User Setting		Changing a User Setting on page 7-92
	Add user		Adding a User for Access to a module on page 7-91
	Delete User		Deleting a User from Access to a module on page 7-92
	User		Users account on page 7-93
● Quick Start			
	Quick Start	AP, BHM	Quick link setup on page 7-12
	Region Settings	AP, BHM	Quick link setup on page 7-12
	Radio Carrier Frequency	AP, BHM	Quick link setup on page 7-12
	Synchronization	AP, BHM	Quick link setup on page 7-12
	LAN IP Address	AP, BHM	Quick link setup on page 7-12
	Review and Save Configuration	AP, BHM	Quick link setup on page 7-12
● PDA			
	Quick Status	SM	The PDA web-page includes 320 x 240 pixel formatted displays of information important to installation
	Spectrum Results (PDA)	SM	

Main menu	Menu options	Applicable module	Description
	Information	SM	and alignment for installers using legacy PDA devices. All device web pages are compatible with touch devices such as smart phones and tablets.
	BHM Evaluation	SM	
	AIM	SM	
● Copyright			
	Copyright Notices	All	The Copyright web-page displays pertinent device copyright information.
● Logoff		All	

Quick link setup

This section describes how to use the Quick Start Wizard to complete the essential system configuration tasks that must be performed on a PTP/PMP configuration.

Note

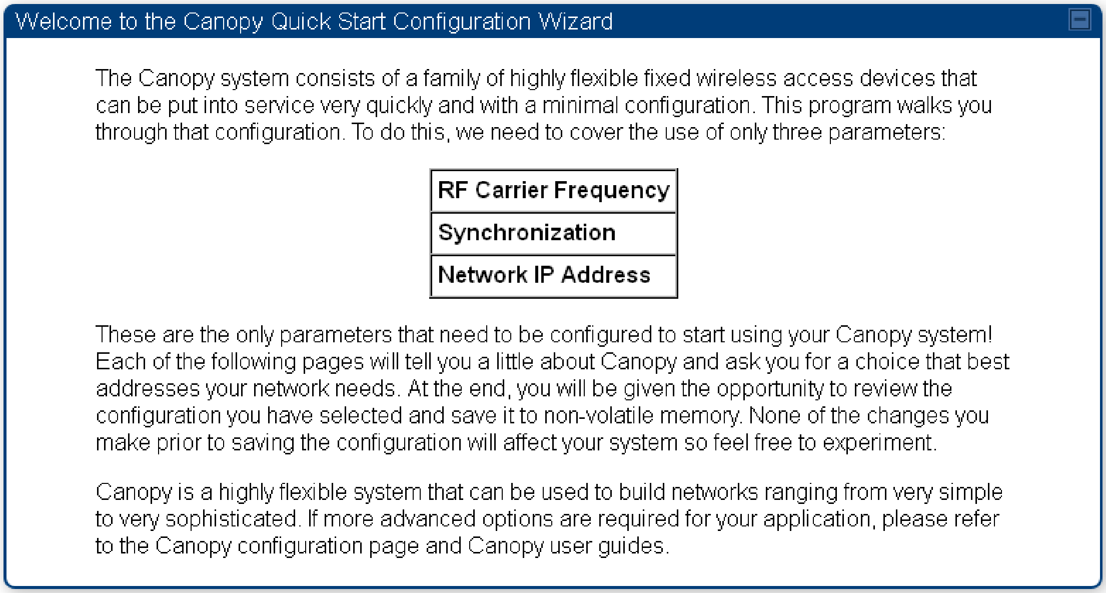
If the IP address of the AP or BHM is not known, See Radio recovery mode – Radio Recovery Console / Default Mode (fka Default Plug)on page 1-16.

Initiating Quick Start Wizard

Appplicable products	PMP :	☑	AP	PTP:	☑	BHM

To start with Quick Start Wizard: after logging into the web management interface click the **Quick Start** button on the left side of main menu bar. The AP/BHM responds by opening the Quick Start page.

Figure 51 Disarm Installation page (top and bottom of page shown)



Welcome to the Canopy Quick Start Configuration Wizard

The Canopy system consists of a family of highly flexible fixed wireless access devices that can be put into service very quickly and with a minimal configuration. This program walks you through that configuration. To do this, we need to cover the use of only three parameters:

RF Carrier Frequency
Synchronization
Network IP Address

These are the only parameters that need to be configured to start using your Canopy system! Each of the following pages will tell you a little about Canopy and ask you for a choice that best addresses your network needs. At the end, you will be given the opportunity to review the configuration you have selected and save it to non-volatile memory. None of the changes you make prior to saving the configuration will affect your system so feel free to experiment.

Canopy is a highly flexible system that can be used to build networks ranging from very simple to very sophisticated. If more advanced options are required for your application, please refer to the Canopy configuration page and Canopy user guides.

Quick Start is a wizard that helps you to perform a basic configuration that places an AP/BHM into service. Only the following parameters must be configured:

- Region Code
- RF Carrier Frequency
- Synchronization
- LAN (Network) IP Address

In each Quick Start page, you can

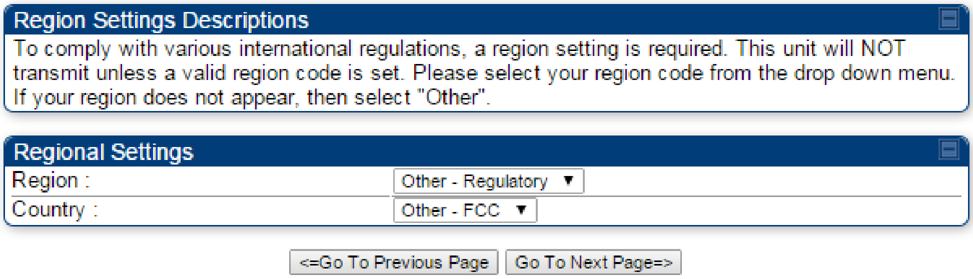
- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Procedure 12 Quick start wizard

1 At the bottom of the Quick Start tab, click the **Go To Next Page** button.

2 From the pull-down menu, select the region in which the AP will operate.

Figure 52 Regional Settings tab of AP/BHM



Region Settings Descriptions

To comply with various international regulations, a region setting is required. This unit will NOT transmit unless a valid region code is set. Please select your region code from the drop down menu. If your region does not appear, then select "Other".

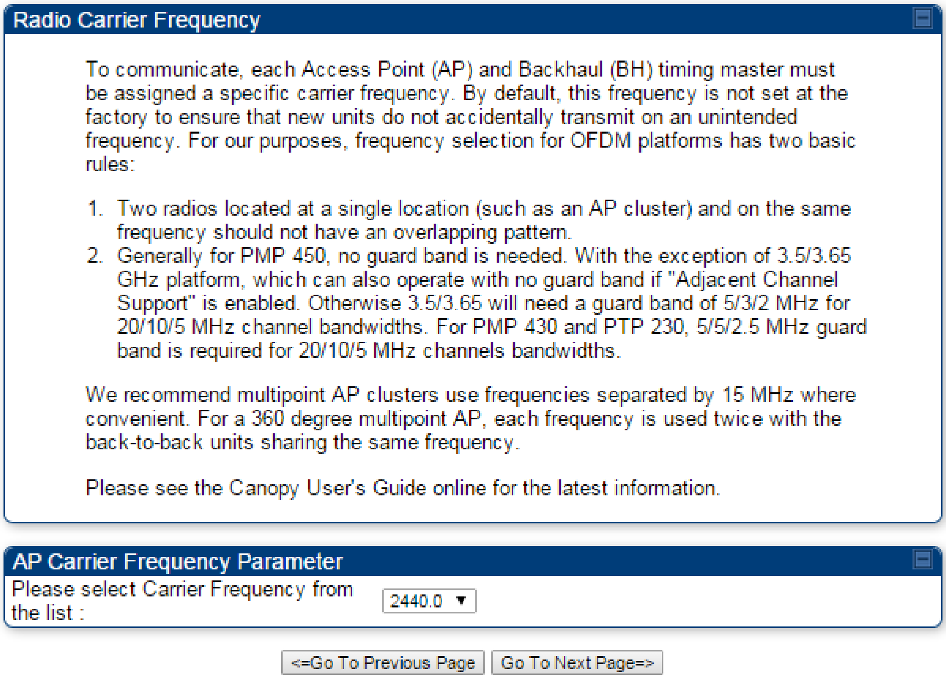
Regional Settings

Region :	Other - Regulatory ▼
Country :	Other - FCC ▼

3 Click the **Go To Next Page** button.

4 From the pull-down menu, select a frequency for the test.

Figure 53 Radio Carrier Frequency tab of AP/BHM



Radio Carrier Frequency

To communicate, each Access Point (AP) and Backhaul (BH) timing master must be assigned a specific carrier frequency. By default, this frequency is not set at the factory to ensure that new units do not accidentally transmit on an unintended frequency. For our purposes, frequency selection for OFDM platforms has two basic rules:

1. Two radios located at a single location (such as an AP cluster) and on the same frequency should not have an overlapping pattern.
2. Generally for PMP 450, no guard band is needed. With the exception of 3.5/3.65 GHz platform, which can also operate with no guard band if "Adjacent Channel Support" is enabled. Otherwise 3.5/3.65 will need a guard band of 5/3/2 MHz for 20/10/5 MHz channel bandwidths. For PMP 430 and PTP 230, 5/5/2.5 MHz guard band is required for 20/10/5 MHz channels bandwidths.

We recommend multipoint AP clusters use frequencies separated by 15 MHz where convenient. For a 360 degree multipoint AP, each frequency is used twice with the back-to-back units sharing the same frequency.

Please see the Canopy User's Guide online for the latest information.

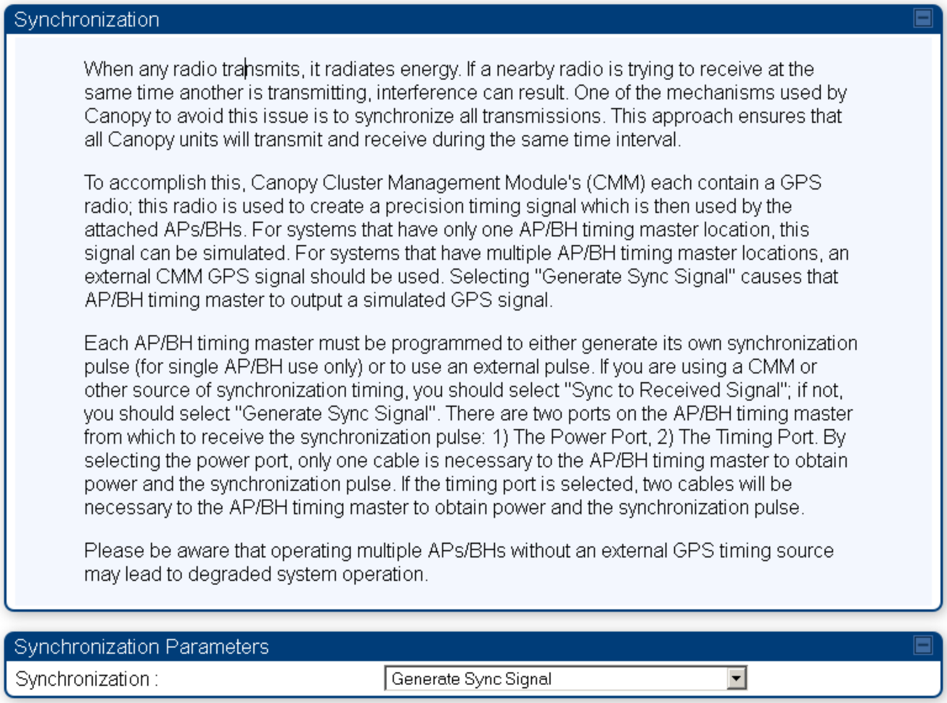
AP Carrier Frequency Parameter

Please select Carrier Frequency from the list :	2440.0 ▼

5 Click the **Go To Next Page** button.

6 At the bottom of this tab, select **Generate Sync Signal**.

Figure 54 Synchronization tab of AP/BHM



Synchronization

When any radio transmits, it radiates energy. If a nearby radio is trying to receive at the same time another is transmitting, interference can result. One of the mechanisms used by Canopy to avoid this issue is to synchronize all transmissions. This approach ensures that all Canopy units will transmit and receive during the same time interval.

To accomplish this, Canopy Cluster Management Module's (CMM) each contain a GPS radio; this radio is used to create a precision timing signal which is then used by the attached APs/BHs. For systems that have only one AP/BH timing master location, this signal can be simulated. For systems that have multiple AP/BH timing master locations, an external CMM GPS signal should be used. Selecting "Generate Sync Signal" causes that AP/BH timing master to output a simulated GPS signal.

Each AP/BH timing master must be programmed to either generate its own synchronization pulse (for single AP/BH use only) or to use an external pulse. If you are using a CMM or other source of synchronization timing, you should select "Sync to Received Signal"; if not, you should select "Generate Sync Signal". There are two ports on the AP/BH timing master from which to receive the synchronization pulse: 1) The Power Port, 2) The Timing Port. By selecting the power port, only one cable is necessary to the AP/BH timing master to obtain power and the synchronization pulse. If the timing port is selected, two cables will be necessary to the AP/BH timing master to obtain power and the synchronization pulse.

Please be aware that operating multiple APs/BHs without an external GPS timing source may lead to degraded system operation.

Synchronization Parameters

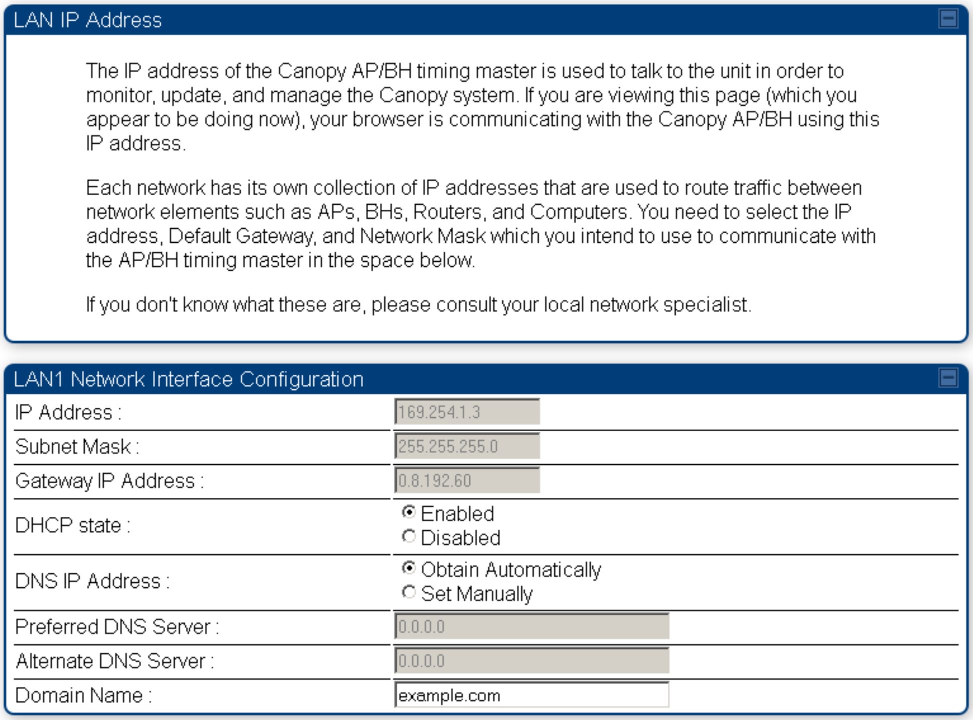
Synchronization : Generate Sync Signal

7 Click the **Go To Next Page** button.

8 At the bottom of the IP address configuration tab, either

- specify an **IP Address**, a **Subnet Mask**, and a **Gateway IP Address** for management of the AP and leave the **DHCP state** set to **Disabled.**
- set the **DHCP state** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server (DNS).

Figure 55 LAN IP Address tab of the AP/BHM



LAN IP Address

The IP address of the Canopy AP/BH timing master is used to talk to the unit in order to monitor, update, and manage the Canopy system. If you are viewing this page (which you appear to be doing now), your browser is communicating with the Canopy AP/BH using this IP address.

Each network has its own collection of IP addresses that are used to route traffic between network elements such as APs, BHs, Routers, and Computers. You need to select the IP address, Default Gateway, and Network Mask which you intend to use to communicate with the AP/BH timing master in the space below.

If you don't know what these are, please consult your local network specialist.

LAN1 Network Interface Configuration

IP Address :	169.254.1.3
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.8.192.60
DHCP state :	● Enabled ○ Disabled
DNS IP Address :	● Obtain Automatically ○ Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

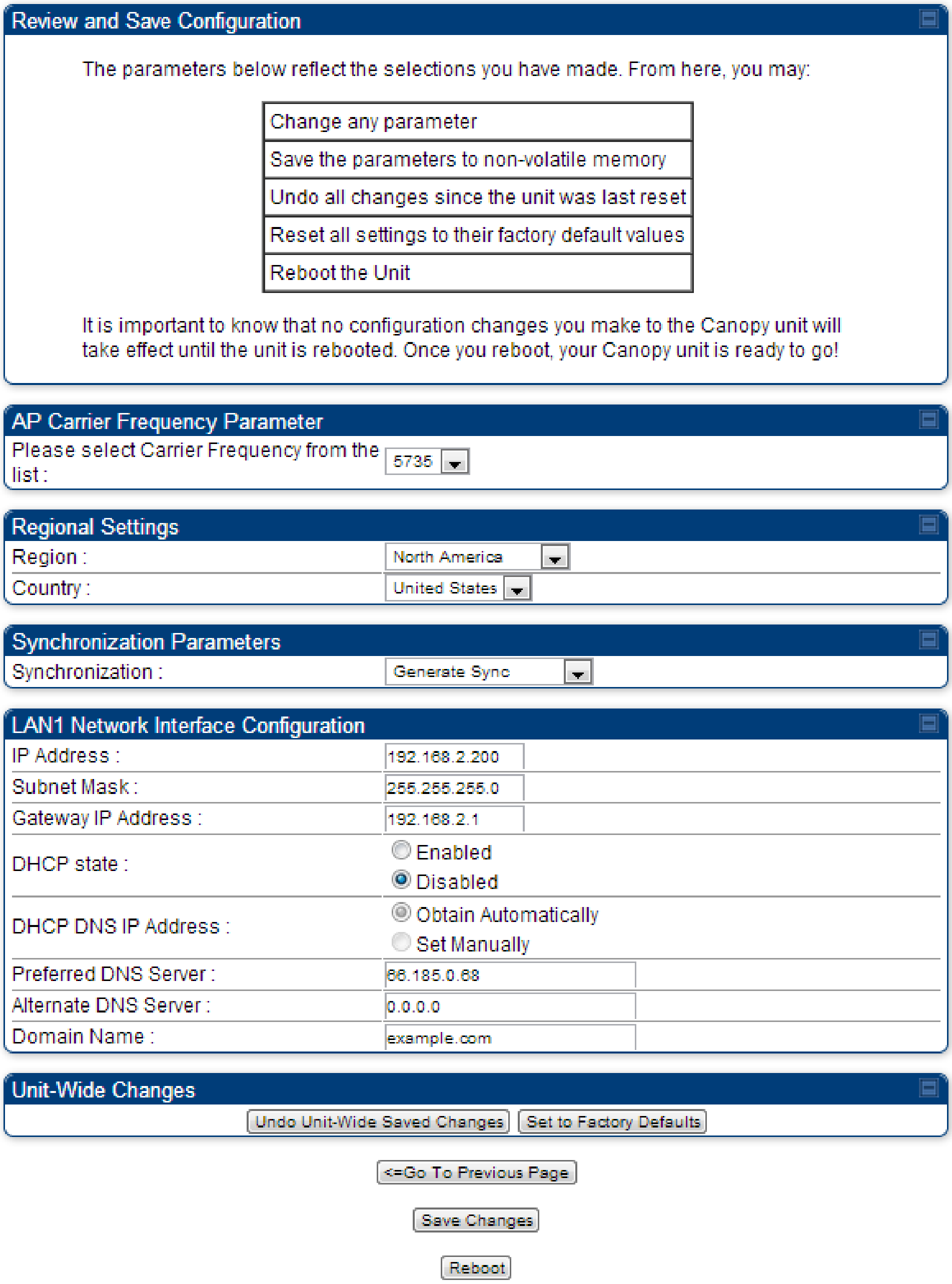
Note

Cambium encourages you to experiment with the interface. Unless you save a configuration and reboot the AP after you save the configuration, none of the changes are affected.

9 Click the **Go To Next Page =>** button.

10 Ensure that the initial parameters for the AP are set as you intended.

Figure 56 Review and Save Configuration tab of the AP/BHM



Review and Save Configuration

The parameters below reflect the selections you have made. From here, you may:

Change any parameter
Save the parameters to non-volatile memory
Undo all changes since the unit was last reset
Reset all settings to their factory default values
Reboot the Unit

It is important to know that no configuration changes you make to the Canopy unit will take effect until the unit is rebooted. Once you reboot, your Canopy unit is ready to go!

AP Carrier Frequency Parameter

Please select Carrier Frequency from the list :	5735

Regional Settings

Region :	North America
Country :	United States

Synchronization Parameters

Synchronization :	Generate Sync

LAN1 Network Interface Configuration

IP Address :	192.168.2.200
Subnet Mask :	255.255.255.0
Gateway IP Address :	192.168.2.1
DHCP state :	○ Enabled ● Disabled
DHCP DNS IP Address :	● Obtain Automatically ○ Set Manually
Preferred DNS Server :	66.185.0.68
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

Unit-Wide Changes

11 Click the **Save Changes** button.

12 Click the **Reboot** button.
RESULT: The AP responds with the message **Reboot Has Been Initiated...**

13 Wait until the indicator LEDs are not red.

14 Trigger your browser to refresh the page until the AP redisplays the General Status tab.

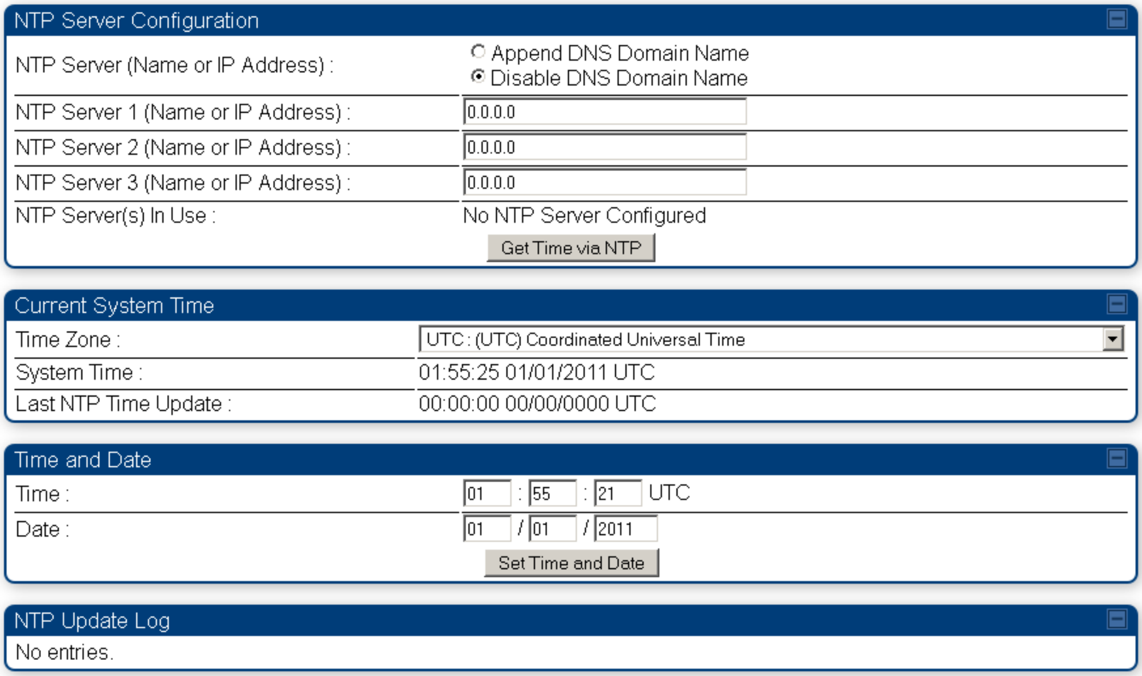
15 Wait until the red indicator LEDs are not lit.

Configuring time settings

Appplicable products	PMP :	☑	AP	PTP:	☑	BHM

To proceed with the test setup, click the **Configuration** link on the left side of the General Status page. When the AP responds by opening the Configuration page to the General page, click the Time tab.

Figure 57 Time tab of the AP/BHM



NTP Server Configuration

NTP Server (Name or IP Address) :	○ Append DNS Domain Name ● Disable DNS Domain Name
NTP Server 1 (Name or IP Address) :	0.0.0.0
NTP Server 2 (Name or IP Address) :	0.0.0.0
NTP Server 3 (Name or IP Address) :	0.0.0.0
NTP Server(s) In Use :	No NTP Server Configured

Current System Time

Time Zone :	UTC : (UTC) Coordinated Universal Time
System Time :	01:55:25 01/01/2011 UTC
Last NTP Time Update :	00:00:00 00/00/0000 UTC

Time and Date

Time :	01 : 55 : 21 UTC
Date :	01 / 01 / 2011

NTP Update Log

No entries.

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 you 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:

- A connected CMM4 passes time and date (GPS time and date, if received).
- A separate NTP server is addressable from the AP/BHM.

If the AP/BHM should obtain time and date from a CMM4, or a separate NTP server, enter the IP address 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 through NTP**.

If you enter a time and date, the format for entry is

Figure 58 Time and date entry formats

Time : *hh* / *mm* / *ss*

Date : *MM* / *dd* / *yyyy*

where

hh represents the two-digit hour in the range 00 to 24
mm represents the two-digit minute
ss represents the two-digit second
MM represents the two-digit month
dd represents the two-digit day
yyyy represents the four-digit year

Proceed with the time setup as follows.

Procedure 13 Entering AP/BHM time setup information

1 Enter the appropriate information in the format shown above.

2 Then click the **Set Time and Date** button.

Note
The time displayed at the top of this page is static unless your browser is set to automatically refresh

Powering the SM/BHS for test

Procedure 14 Powering the SM/BHS for test

1 In one hand, securely hold the top (larger shell) of the SM/BHS. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.

2 Plug one end of a CAT 5 Ethernet cable into the SM PSU port

3 Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply

4 Roughly aim the SM/BHS toward the AP/BHM

5 Plug the power supply into an electrical outlet

Warning
From this point until you remove power from the AP/BHM, stay at least as far from the AP/BHM as the minimum separation distance specified in Calculated distances and power compliance margins.

6 Repeat the foregoing steps for each SM/BHS that you wish to include in the test.

Viewing the Session Status of the AP/BHM to determine test registration

Once the SMs/BHS under test are powered on, return to the computing device to determine if the SM/BHS units have registered to the AP/BHM.

Note

In order for accurate power level readings to be displayed, traffic must be present on the radio link.

The Session Status tab provides information about each SM/BHS that has registered to the AP/BHM. This information is useful for managing and troubleshooting a system.
All information that you have entered in the **Site Name** field of the SM/BHS displays in the Session Status tab of the linked AP/BHM.

The Session Status tab also includes the current active values on each SM(or BHS) (LUID) for MIR, and VLAN, as well as the source of these values (representing the SM/BHS itself, Authentication Server, or the AP/BHM and cap, if any—for example, APCAP as shown above).. As an SM/BHS registers to the AP/BHM, the configuration source that this page displays for the associated LUID may change. After registration, however, the displayed source is stable and can be trusted.

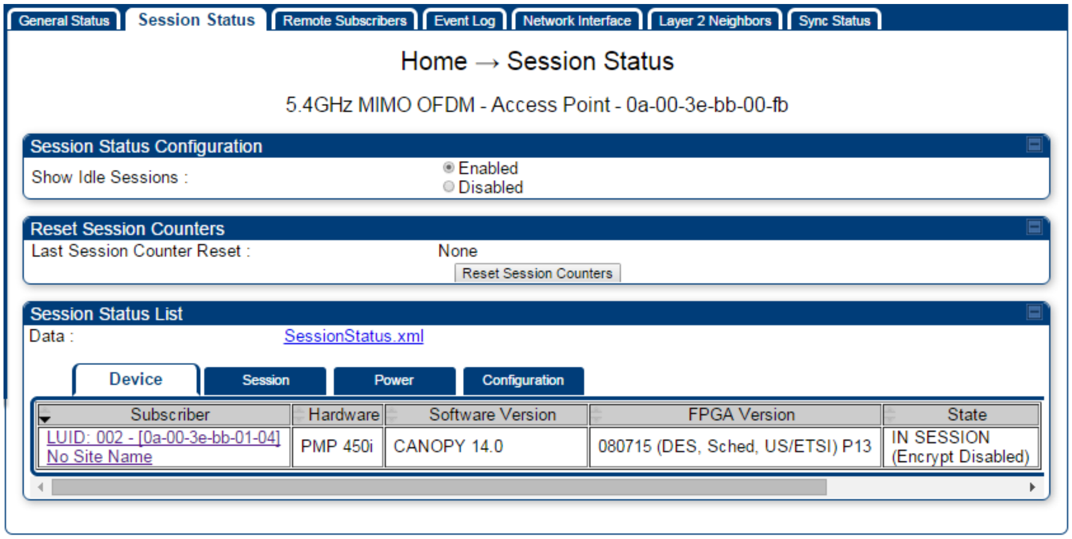
Idle subscribers may be included or removed from the session status display by enabling or disabling, respectively, the **Show Idle Sessions** parameter. Enabling or disabling this parameter only affects the GUI display of subscribers, not the registration status.

The SessionStatus.xml hyperlink allows user to export session status page from web management interface of AP/BHM. The session status page will be exported in xml file.

Procedure 15 Viewing the AP Session Status page

1 On the AP web management GUI, navigate to **Home, Session Status**:

Figure 59 Session Status tab of AP



Home → Session Status

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

Session Status Configuration

Show Idle Sessions : ● Enabled ○ Disabled

Reset Session Counters

Last Session Counter Reset : None

Session Status List

Data : SessionStatus.xml

Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-bb-01-04] No Site Name	PMP 450i	CANOPY 14.0	080715 (DES, Sched, US/ETSI) P13	IN SESSION (Encrypt Disabled)

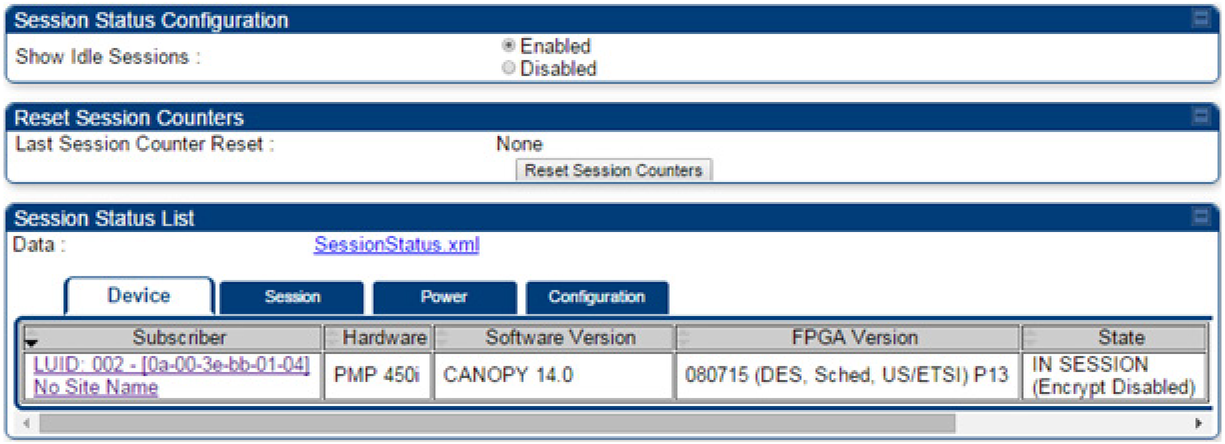
Note

Session status page for BHM is same as AP.

2 Verify that for each SM (or BHS) MAC address (printed on the SM/BHS housing) the AP/BHM has established a registered session by verifying the “State” status of each entry.

The Session Status page of the AP/BHM is explained in Table 55.

Table 56 Session Status Attributes – AP/BHM



Session Status Configuration

Show Idle Sessions : ● Enabled ○ Disabled

Reset Session Counters

Last Session Counter Reset : None

Session Status List

Data : SessionStatus.xml

Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-bb-01-04] No Site Name	PMP 450i	CANOPY 14.0	080715 (DES, Sched, US/ETSI) P13	IN SESSION (Encrypt Disabled)

Attribute	Meaning
LUID	This field displays the LUID (logical unit Identifier) of the SM/BHS. As each SM/BHS registers to the AP/BHM, the system assigns a LUID of 2 or a higher unique number to the SM/BHS. If an SM/BHS loses registration with the AP/BHM and then regains registration, the SM/BHS will retain the same LUID. **Note** The LUID associated is lost when a power cycle of the AP/BHM occurs. Both the LUID and the MAC are hot links to open the interface to the SM/BHS. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
MAC	This field displays the MAC address (or electronic serial number) of the SM/BHS. Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
State	This field displays the current status of the SM/BHS as either • **IN SESSION** to indicate that the SM/BHS is currently registered to the AP/BHM. • **IDLE** to indicate that the SM/BHS was registered to the AP/BHM at one time, but now is not. This field also indicates whether the encryption scheme in the module is enabled.
Site Name	This field indicates the name of the SM/BHS. You can assign or change this name on the Configuration web page of the SM/BHS. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Software Version	This field displays the software release that operates on the SM/BHS, the release date and time of the software.
FPGA Version	This field displays the version of FPGA that runs on the SM/BHS.
Session Timeout	This field displays the timeout in seconds for management sessions via HTTP, ftp access to the SM/BHS. 0 indicates that no limit is imposed.
AirDelay	This field displays the distance of the SM from the AP/BHM. To derive the distance in meters, multiply the displayed number by 0.3048. At close distances, the value in this field is unreliable.
Session Count	This field displays how many times the AP/BHM has granted registration to the SM/BHS. Typically, this is the sum of Reg Count and Re-Reg

	Count. However, the result of internal calculation may display here as a value that slightly differs from the sum
Reg Count	When a SM/BHS makes a registration request, the AP/BHM checks its local database to see whether it considers the SM/BHS to be already registered. If the AP/BHM concludes that the SM/BHS is not currently in session, then the request increments the value of this field.
Re-Reg Count	When an SM/BHS makes a registration request, the AP/BHM checks its local database to see whether it considers the SM/BHS to be already registered. If the AP/BHM concludes that the SM/BHS is not, then the request increments the value of this field. Typically, a **Re-Reg Count** is the case where the SM/BHS attempts to register for having lost communication with the AP/BHM and the AP/BHM has not yet observed the link to the SM/BHS as being out of session. Then the AP/BHM again grants the registration to the SM/BHS and increments the re-registration count. If the number of sessions is significantly greater than the number for other SMs/BHS, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).
Session Uptime	Once an SM/BHS successfully registers to an AP/BHM, this timer is started. If a session drops or is interrupted, this timer is reactivated once re-registration is complete.
Power Level	This field indicates the AP's/BHM's combined receive power level for the listed SM/BHS.
Signal Strength Ratio	This field displays the ratio of the Vertical path received signal power to the Horizontal path received signal power. This ratio can be useful for determining multipathing conditions (high vertical to horizontal ratio).
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor.
Sustained Uplink Data Rate	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified rate at which each SM/BHS registered to this AP/BHM is replenished with credits for transmission. The configuration source of the value is indicated in parentheses. The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Uplink Burst Allocation	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified maximum amount of data that each SM/BHS is allowed to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. The configuration source of the value is indicated in

	parentheses. The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Sustained Downlink Data Rate	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified the rate at which the AP/BHM should be replenished with credits (tokens) for transmission to each of the SMs/BHS's in its sector. The configuration source of the value is indicated in parentheses. The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Downlink Burst Allocation	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the maximum amount of data to allow the AP/BHM to transmit to any registered SM/BHS before the AP/BHM is replenished with transmission credits at the **Sustained Downlink Data Rate**. The configuration source of the value is indicated in parentheses. The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Max Burst Uplink Rate	The data rate at which an SM/BHS is allowed to burst (until burst allocation limit is reached) before being recharged at the **Sustained Uplink Data Rate** with credits to transit more. When set to 0 (default), the burst rate is unlimited. The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Max Burst Downlink Rate	The data rate at which an SM/BHS is allowed to burst (until burst allocation limit is reached) before being recharged at the **Sustained Downlink Data Rate** with credits to transit more. When set to 0 (default), the burst rate is unlimited. The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Low Priority Uplink CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Low Priority Downlink CIR	This field indicates the minimum rate at which low priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
High Uplink CIR	This field indicates the minimum rate at which high priority traffic is sent

	over the uplink (unless CIR is oversubscribed or RF link quality is degraded). The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
High Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). The AP/BHM will display one of denotations for configuration source. See Table 56 on page 7-24.
Rate	This field displays whether the high-priority channel is enabled in the SM and the status of rate adapt. For example, if "8X/4X" is listed, the radio is capable of operating at 8X but is currently operating at 4X, due to RF conditions. This field also states whether it is MIMO-A or MIMO-B radio e.g. "8X/8X MIMO-B"indicates MIMO-B and "8X/4X MIMO-A" indicates MIMO-A.

Table 57 Session Status > Configuration CIR configuration denotations

Attribute	Meaning
(SM)	QoS/VLAN parameters are derived from the SM's/BHS's settings
(APCAP)	QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps)
(D)	QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server.
(AAA)	QoS/VLAN parameters are retrieved from the RADIUS server
(BAM)	QoS/VLAN parameters are retrieved from a WM BAM server

Configuring IP and Ethernet interfaces

This task consists of the following sections:

Configuring the IP interface

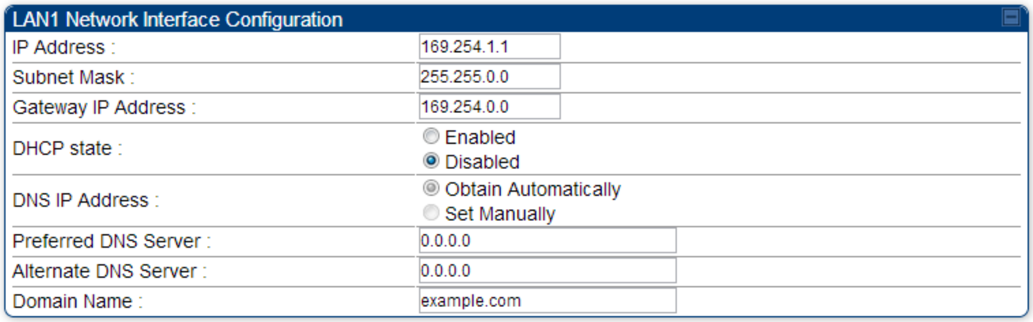
The IP interface allows users to connect to the PMP/PTP 450i web interface, either from a locally connected computer or from a management network.

Appplicable products **PMP :** ☑ AP ☑ SM **PTP:** ☑ BHM ☑ BMS

To configure the IP interface, follow these instructions:

Procedure 16 Configuring the AP/BHM IP interface

1 Select menu option **Configuration** > **IP**. The LAN configuration page is displayed:



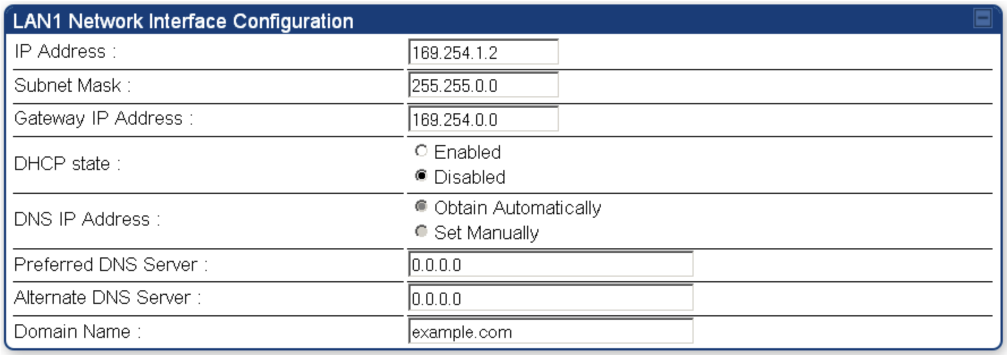
LAN1 Network Interface Configuration

IP Address :	169.254.1.1
Subnet Mask :	255.255.0.0
Gateway IP Address :	169.254.0.0
DHCP state :	○ Enabled ● Disabled
DNS IP Address :	● Obtain Automatically ○ Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

2 Update IP Address, Subnet Mask and Gateway IP Address to meet network requirements (as specified by the network administrator).

3 Review the other IP interface attributes and update them, if necessary (see Table 57 IP interface attributes).

4 Click **Save.** “Reboot Required” message is displayed:



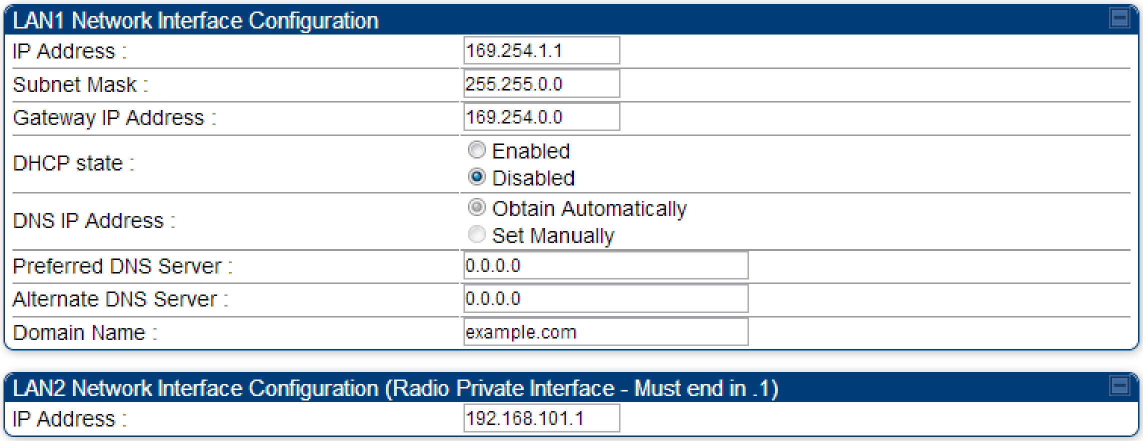
LAN1 Network Interface Configuration

IP Address :	169.254.1.2
Subnet Mask :	255.255.0.0
Gateway IP Address :	169.254.0.0
DHCP state :	○ Enabled ● Disabled
DNS IP Address :	● Obtain Automatically ○ Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

5 Click **Reboot.**

The IP page of AP/SM/BHM/BHS is explained in Table 57.

Table 58 IP interface attributes



LAN1 Network Interface Configuration

IP Address :	169.254.1.1
Subnet Mask :	255.255.0.0
Gateway IP Address :	169.254.0.0
DHCP state :	○ Enabled ● Disabled
DNS IP Address :	● Obtain Automatically ○ Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

LAN2 Network Interface Configuration (Radio Private Interface - Must end in .1)

IP Address :	192.168.101.1

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.
Subnet Mask	Defines the address range of the connected IP network.
	The IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
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. 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 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.
LAN2 Network Interface Configuration (Radio Private Interface) – IP Address	It is recommended not to change this parameter from the default AP/BHM private IP address of 192.168.101.1. A /24 CIDR subnet is used to communicate with each of the SMs/BHS that are registered. The AP/BHM uses a combination of the private IP and the LUID (logical unit ID) of the SM/BHS. It is only displayed for AP and BHM.

Table 59 SM/BHS private IP and LUID

SM/BHS	LUID	Private IP
First SM/BHS registered	2	192.168.101.2
Second SM/BHS registered	3	192.168.101.3

NAT, DHCP Server, DHCP Client and DMZ

Appplicable products	**PMP :**	☑ SM

The system provides NAT (Network Address Translation) for SMs in the following combinations of NAT and DHCP (Dynamic Host Configuration Protocol):

- NAT Disabled
- NAT with DHCP Client (**DHCP** selected as the **Connection Type** of the WAN interface) and DHCP Server
- NAT with DHCP Client(**DHCP** selected as the **Connection Type** of the WAN interface)
- NAT with DHCP Server
- NAT without DHCP

NAT

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.

In the Cambium system, NAT supports many protocols, including HTTP, ICMP (Internet Control Message Protocols), and FTP (File Transfer Protocol). For virtual private network (VPN) implementation, L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) and PPTP (Point to Point Tunneling Protocol) are supported.

Note

When NAT is enabled, a reduction in throughput is introduced in the system (due to processing overhead).

DHCP

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 SM provides the following:

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

DMZ

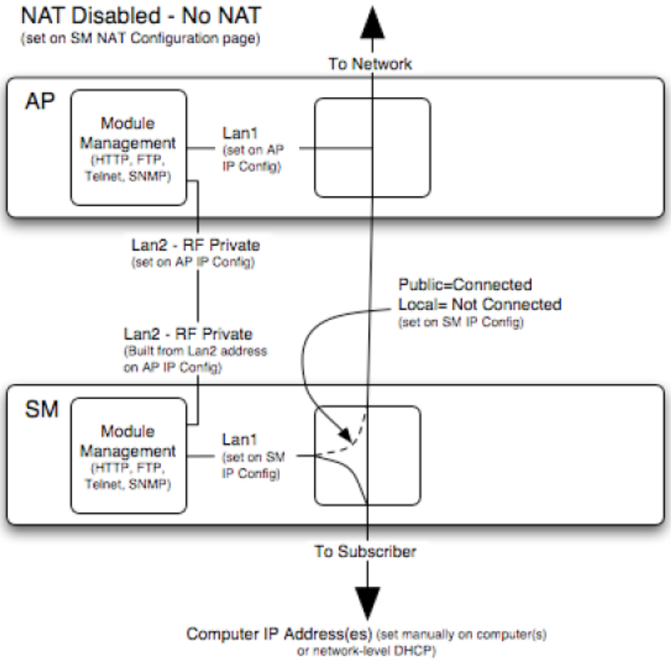
In conjunction with the NAT features, a DMZ (Demilitarized Zone) allows the allotment of one IP address behind the SM for a device to logically exist outside the firewall and receive network traffic. The first three octets of this IP address must be identical to the first three octets of the NAT private IP address.

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

NAT Disabled

The NAT Disabled implementation is illustrated in Figure 60.

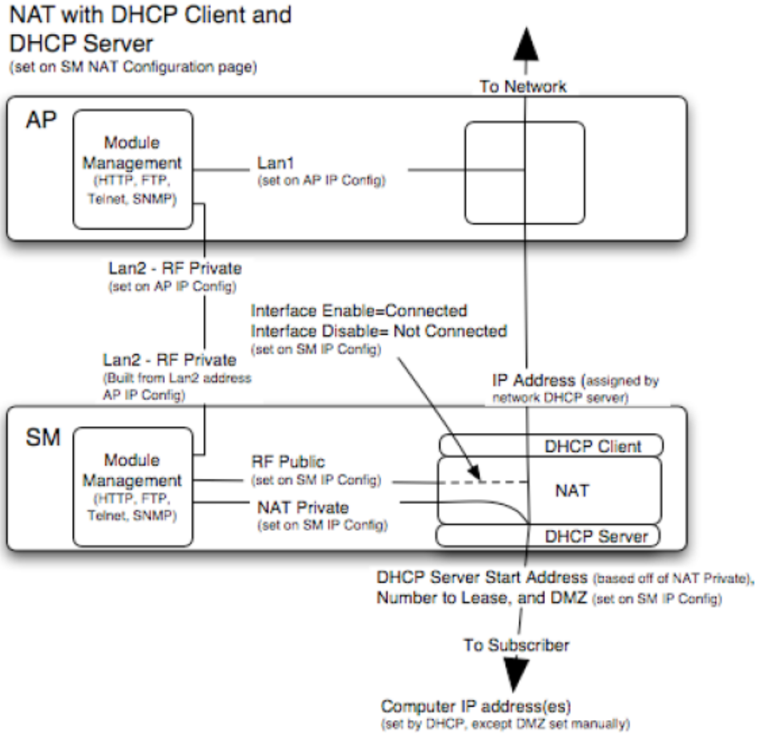
Figure 60 NAT disabled implementation



NAT with DHCP Client and DHCP Server

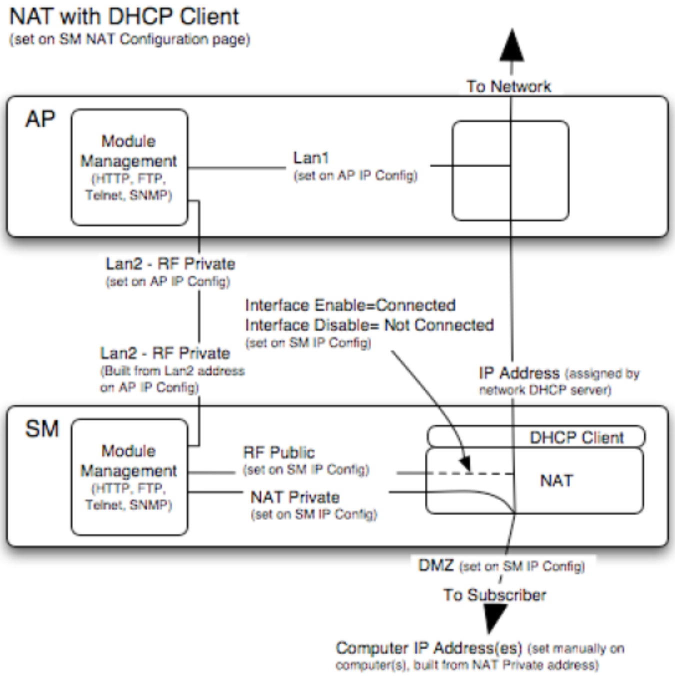
The NAT with DHCP Client and DHCP server is illustrated in Figure 61.

Figure 61 NAT with DHCP client and DHCP server implementation



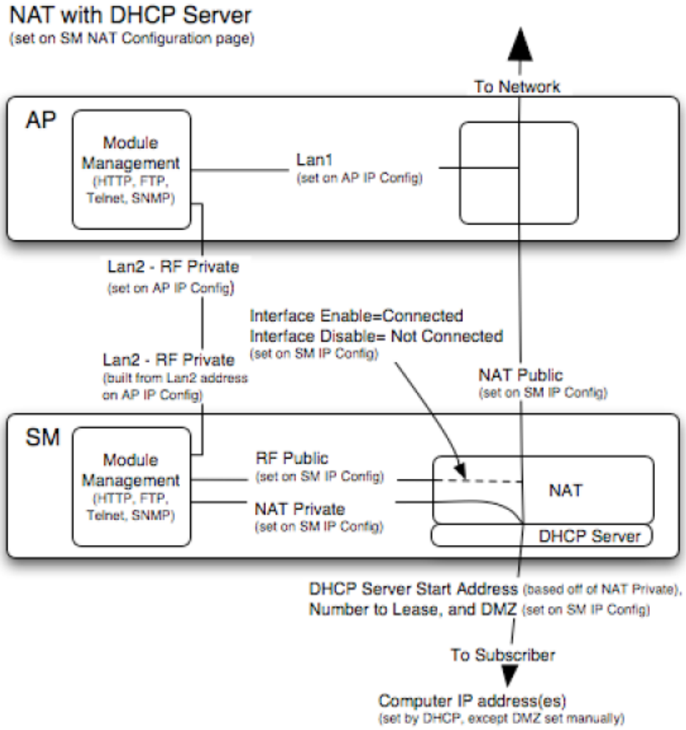
NAT with DHCP Client

Figure 62 NAT with DHCP client implementation



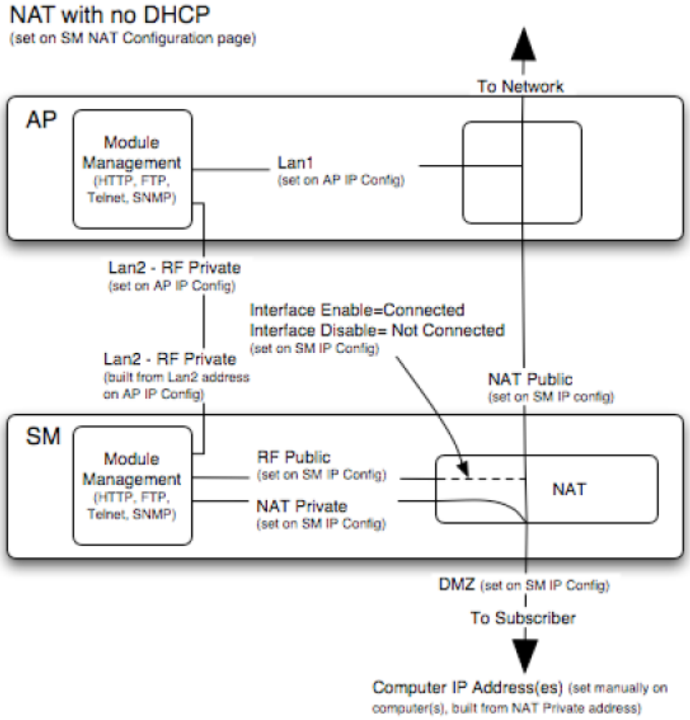
NAT with DHCP Server

Figure 63 NAT with DHCP server implementation



NAT without DHCP

Figure 64 NAT without DHCP implementation


NAT with no DHCP
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(built from Lan2 address on AP IP Config)
NAT Public
(set on SM IP config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

NAT and VPNs

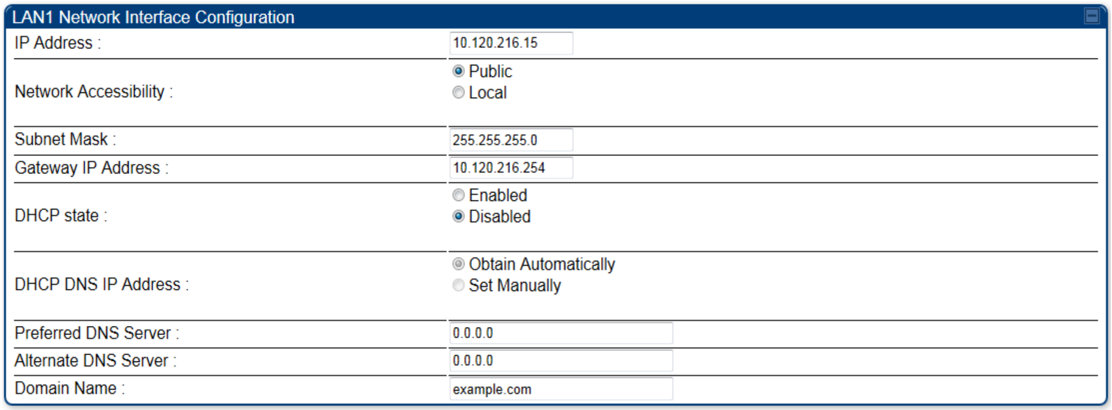
VPN technology provides the benefits of a private network during communication over a public network. One typical use of a VPN is to connect employees remotely (who are at home or in a different city), with their corporate network through a public Internet. Any of several VPN implementation schemes is 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 59.

Table 60 IP attributes - SM with NAT disabled



LAN1 Network Interface Configuration

IP Address :	10.120.216.15
Network Accessibility :	● Public ○ Local
Subnet Mask :	255.255.255.0
Gateway IP Address :	10.120.216.254
DHCP state :	○ Enabled ● Disabled
DHCP DNS IP Address :	● Obtain Automatically ○ Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

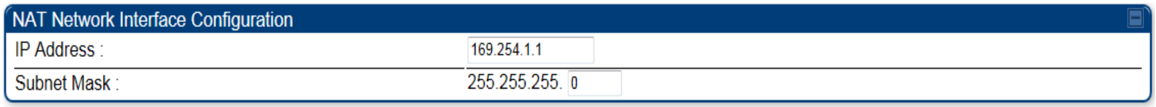
Attribute	**Meaning**
IP Address	Enter the non-routable IP address to associate with the Ethernet connection on this SM. (The default IP address from the factory is 169.254.1.1.) If you forget this parameter, you must both: • physically access the module. • use recovery mode to access the module configuration parameters at 169.254.1.1. See Radio recovery mode – Radio Recovery Console / Default Mode (fka Default Plug)on page 1-16 **Note** 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.
Network Accessibility	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**).
Subnet Mask	Enter an appropriate subnet mask for the SM to communicate on the network. The default subnet mask is 255.255.0.0.
Gateway IP Address	Enter the appropriate gateway for the SM to communicate with the network. The default gateway is 169.254.0.0.
DHCP state	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. In this tab, DHCP State is settable only if the **Network Accessibility**

	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 60.

Table 61 IP attributes - SM with NAT enabled



NAT Network Interface Configuration

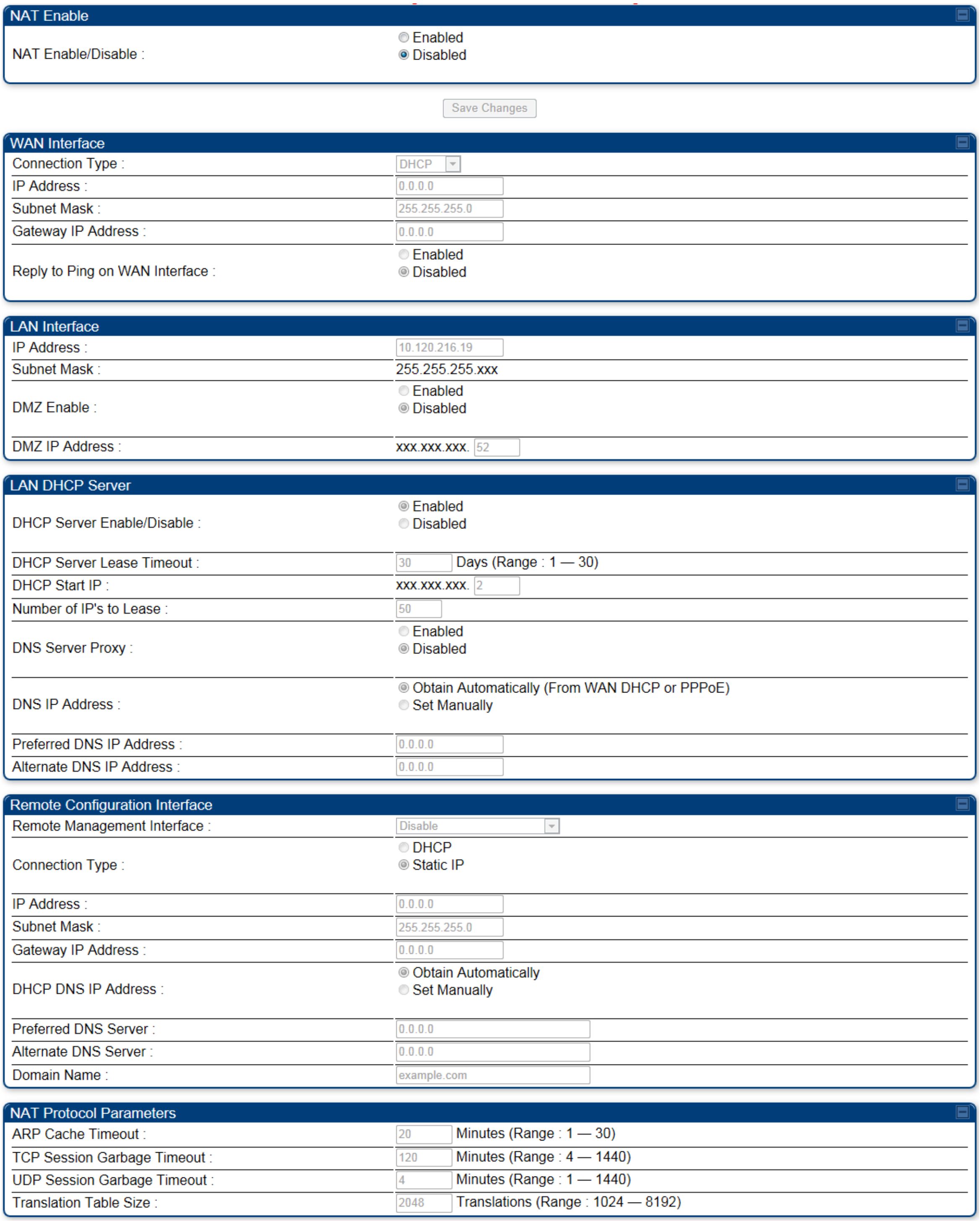
IP Address :	169.254.1.1
Subnet Mask :	255.255.255. 0

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 61.

Table 62 NAT attributes - SM with NAT disabled



NAT Enable

NAT Enable/Disable :	○ Enabled ● Disabled

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 :	○ Enabled ● Disabled

LAN Interface

IP Address :	10.120.216.19
Subnet Mask :	255.255.255.xxx
DMZ Enable :	○ Enabled ● Disabled
DMZ IP Address :	xxx.xxx.xxx. 52

LAN DHCP Server

DHCP Server Enable/Disable :	● Enabled ○ 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 :	○ Enabled ● Disabled
DNS IP Address :	● Obtain Automatically (From WAN DHCP or PPPoE) ○ 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 :	○ DHCP ● 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 :	● Obtain Automatically ○ 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	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. 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.
IP Address	This field displays the IP address for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.
Subnet Mask	This field displays the subnet mask for the SM. DHCP Server *will not* automatically assign this address when NAT is disabled.
Gateway IP Address	This field displays the gateway IP address for the SM. DHCP Server *will not* 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 configurabled:

WAN Inter face > Connection Type, IP Address, Subnet Mask, Gateway IP address

LAN Interface > IP Address

LAN DHCP Server > DHCP Server Enebale/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

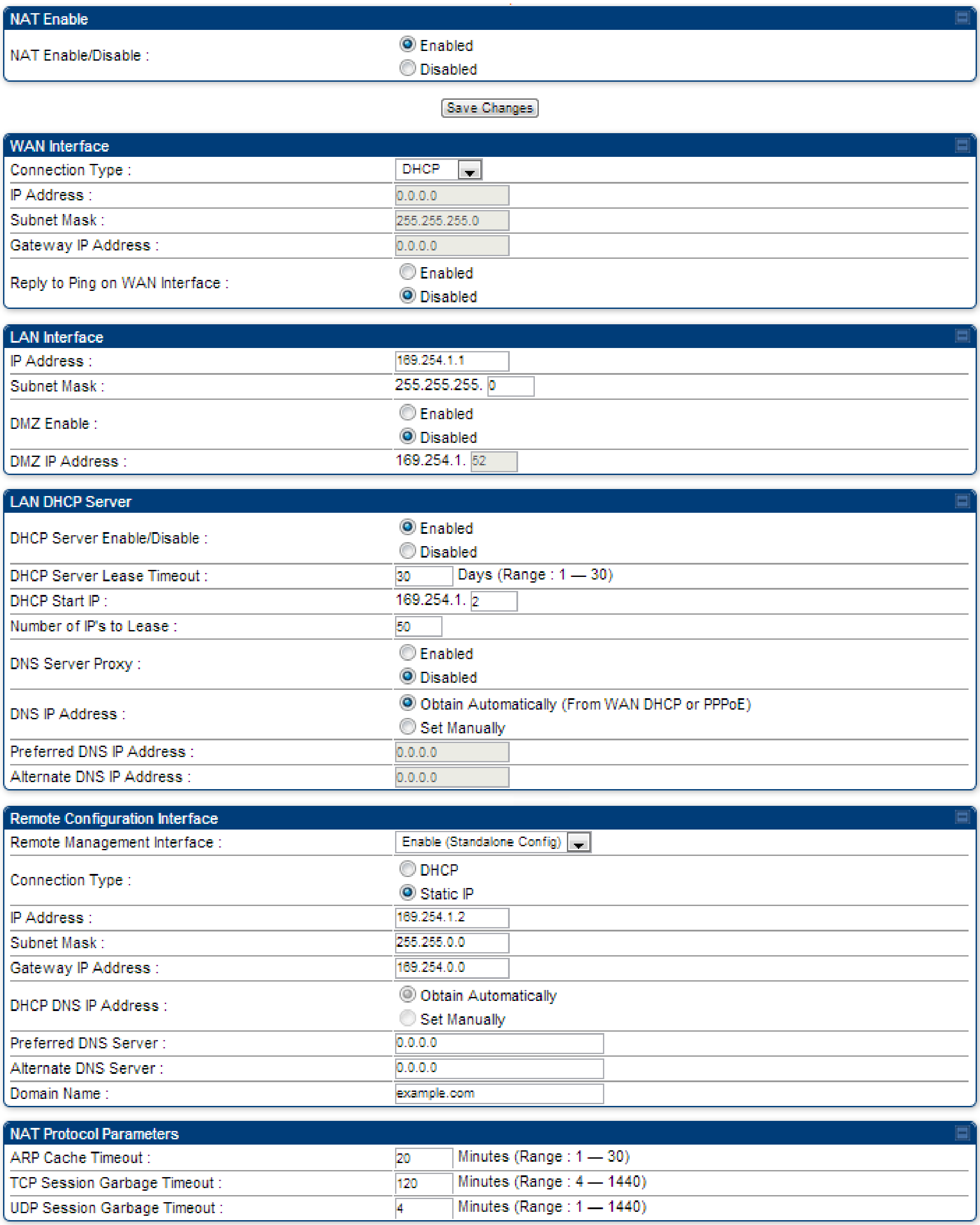
Remote Management Interface > Remote Management Interface, IP address, Subnet Mask, DHCP DNS IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name

NAT Protocol Parameters > ARP Cache Timout, 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 62.

Table 63 NAT attributes - SM with NAT enabled



NAT Enable

NAT Enable/Disable :	● Enabled ○ Disabled

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 :	○ Enabled ● Disabled

LAN Interface

IP Address :	169.254.1.1
Subnet Mask :	255.255.255. 0
DMZ Enable :	○ Enabled ● Disabled
DMZ IP Address :	169.254.1. 52

LAN DHCP Server

DHCP Server Enable/Disable :	● Enabled ○ 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 :	○ Enabled ● Disabled
DNS IP Address :	● Obtain Automatically (From WAN DHCP or PPPoE) ○ 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 :	○ DHCP ● 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 :	● Obtain Automatically ○ 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

	(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. 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.
WAN Interface	The WAN interface is the RF-side address for transport traffic.
Connection Type	This parameter may be set to **Static IP**—when this is the selection, all three parameters (**IP Address**, **Subnet Mask**, and **Gateway IP Address**) must be properly populated. **DHCP**—when this is the selection, the information from the DHCP server configures the interface. **PPPoE**—when this is the selection, the information from the PPPoE server configures the interface.
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 *does not* 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	Select either **Enabled** or **Disabled**. **Enable** to: • 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). **Disable** to: • 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	Select either: **Obtain Automatically** to allow the system to set the IP address of the DNS server *or* **Set Manually** to enable yourself to set both a preferred and an alternate DNS IP address.
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	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) **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. **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. **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). **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). **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 is consumed by the device's network stack for management.
Connection Type	This parameter can be set to: **Static IP**—when this is the selection, all three parameters (**IP Address**, **Subnet Mask**, and **Gateway IP Address**) must be properly populated. **DHCP**—when this is the selection, the information from the DHCP server configures the interface.
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	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. 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.
DHCP DNS IP Address	Select either: **Obtain Automatically** to allow the system to set the IP address of the DNS server. *or* **Set Manually** to enable yourself to set both a preferred and an alternate DNS IP address.
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.

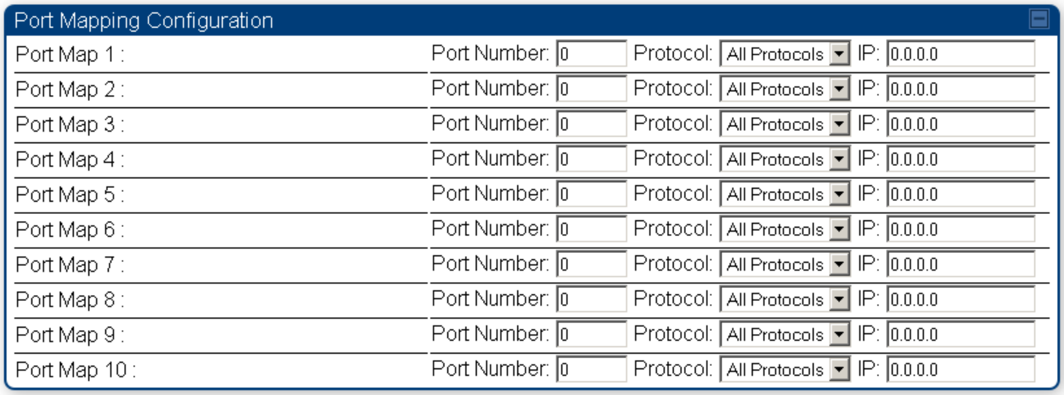
Table 64 SM DNS Options with NAT Enabled

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 64.

Table 65 NAT Port Mapping attributes - SM



Port Mapping Configuration

Port Map 1 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 2 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 3 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 4 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 5 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 6 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 7 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 8 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 9 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0
Port Map 10 :	Port Number: 0	Protocol: All Protocols	IP: 0.0.0.0

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

Appplicable 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

Appplicable 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 65. AP does not support VLAN ID remarking.

Table 66 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.

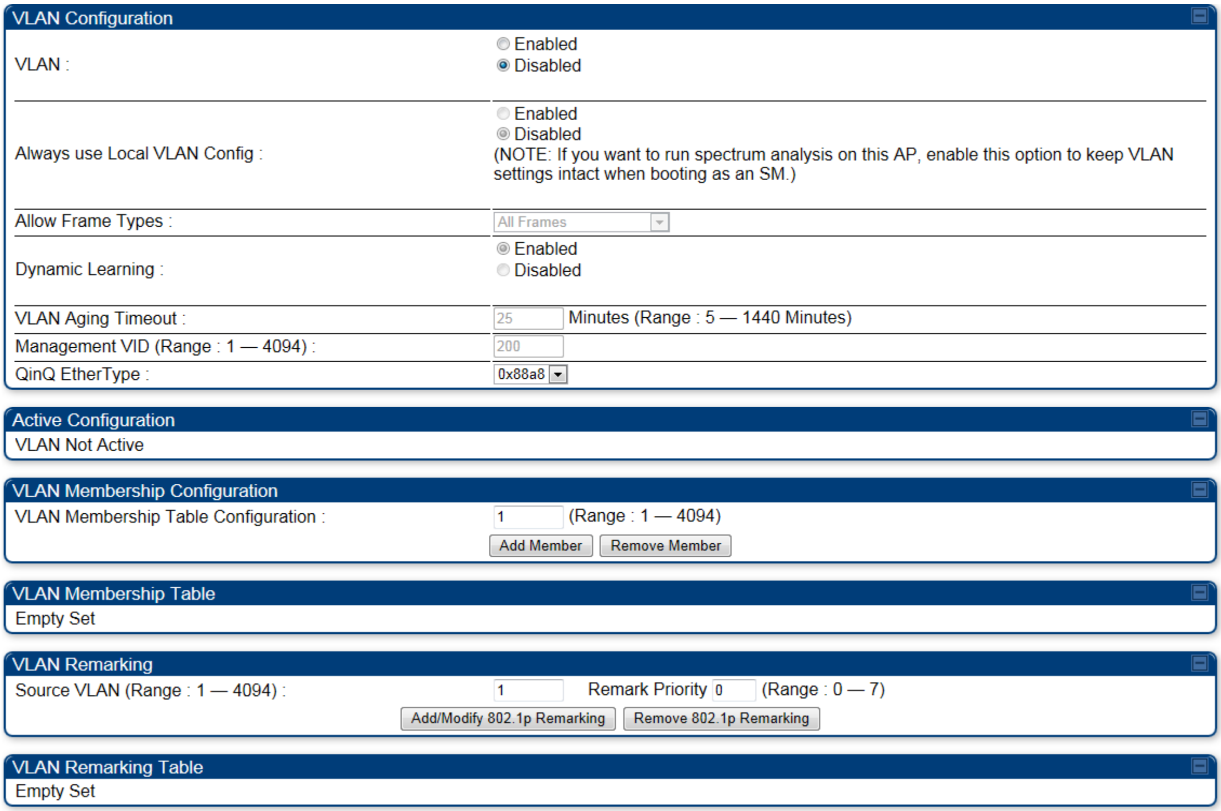
Management VID

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 66.

Table 67 AP/BHM VLAN tab attributes



VLAN Configuration

VLAN :	○ Enabled ● Disabled
Always use Local VLAN Config :	○ Enabled ● Disabled (NOTE: If you want to run spectrum analysis on this AP, enable this option to keep VLAN settings intact when booting as an SM.)
Allow Frame Types :	All Frames
Dynamic Learning :	● Enabled ○ Disabled
VLAN Aging Timeout :	25 Minutes (Range : 5 — 1440 Minutes)
Management VID (Range : 1 — 4094) :	200
QinQ EtherType :	0x88a8

Active Configuration

VLAN Not Active

VLAN Membership Configuration

VLAN Membership Table Configuration :	1 (Range : 1 — 4094)

VLAN Membership Table

Empty Set

VLAN Remarking

Source VLAN (Range : 1 — 4094) :	1 Remark Priority 0 (Range : 0 — 7)

VLAN Remarking Table

Empty Set

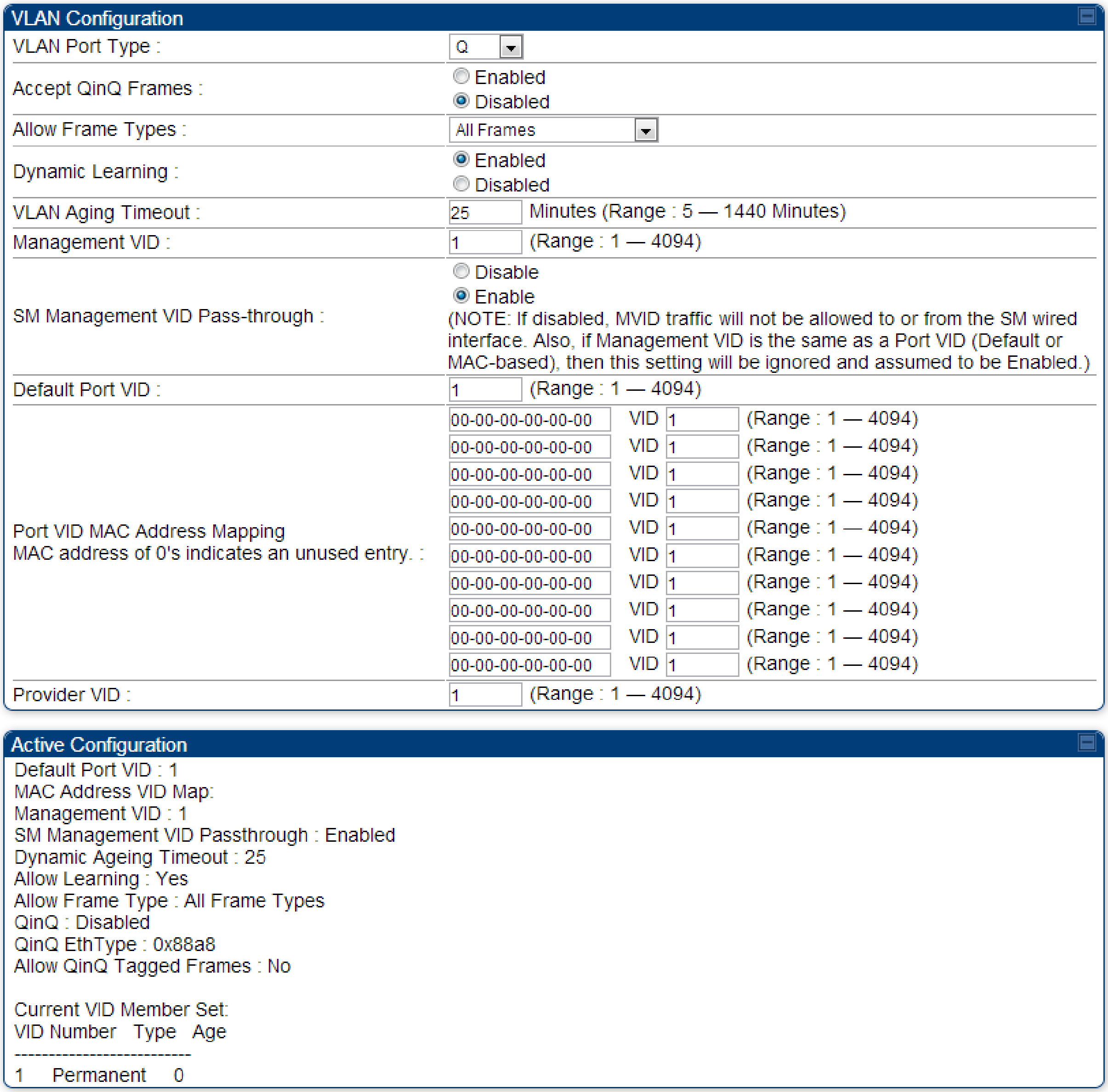
<table>
<tr><th>Attribute</th><th>Meaning</th></tr>
<tr><td>VLAN</td><td>Specify whether VLAN functionality for the AP and all linked SMs must (<b>Enabled</b>) or may not (<b>Disabled</b>) be allowed. The default value is <b>Disabled</b>.</td></tr>
<tr><td>Always use Local VLAN Config</td><td>Enable 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,</td></tr>
<tr><td>Allow Frame Types</td><td>Select the type of arriving frames that the AP must tag, using the VID that is stored in the <b>Untagged Ingress VID</b> parameter. The default value is <b>All Frames</b>.</td></tr>
<tr><td>Dynamic Learning</td><td>Specify whether the AP must (<b>Enabled</b>) or not (<b>Disabled</b>) 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 <b>Enabled</b>.</td></tr>
<tr><td>VLAN Aging Timeout</td><td>Specify how long the AP must keep dynamically learned VIDs. The range of values is 5 to <i>1440</i> (minutes). The default value is <i>25</i> (minutes).
<b>Note</b>
VIDs that you enter for the Management VID and VLAN Membership parameters do not time out.</td></tr>
<tr><td>Management VID</td><td>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 <b>1</b>.</td></tr>
<tr><td>QinQ EtherType</td><td>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:
<b>Table 68</b> Q-in-Q Ethernet frame
<table>
<tr><td>Ethernet Header</td><td>S-VLAN EthType 0x88a8</td><td>C-VLAN EthType 0x8100</td><td>IP Data EthType 0x0800</td></tr>
</table>
The 802.1ad S-VLAN is the outer VLAN that is configurable on the <b>Configuration &gt; VLAN</b> 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.</td></tr>
</table>

	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 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.

VLAN page of SM

The **VLAN** tab of SM/BHS is explained in Table 68.

Table 69 SM VLAN attributes



VLAN Configuration

VLAN Port Type :	Q
Accept QinQ Frames :	○ Enabled ● Disabled
Allow Frame Types :	All Frames
Dynamic Learning :	● Enabled ○ Disabled
VLAN Aging Timeout :	25 Minutes (Range : 5 — 1440 Minutes)
Management VID :	1 (Range : 1 — 4094)
SM Management VID Pass-through :	○ Disable ● Enable (NOTE: If disabled, MVID traffic will not be 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 will be ignored and assumed to be Enabled.)
Default Port VID :	1 (Range : 1 — 4094)
Port VID MAC Address Mapping MAC address of 0's indicates an unused entry. :	00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094) 00-00-00-00-00-00 VID 1 (Range : 1 — 4094)
Provider VID :	1 (Range : 1 — 4094)

Active Configuration

```
Default Port VID : 1
MAC Address VID Map:
Management VID : 1
SM Management VID Passthrough : Enabled
Dynamic Ageing Timeout : 25
Allow Learning : Yes
Allow Frame Type : All Frame Types
QinQ : Disabled
QinQ EthType : 0x88a8
Allow QinQ Tagged Frames : No

Current VID Member Set:
VID Number   Type   Age
--------------------------
1     Permanent     0
```

Attribute	Meaning
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 SM/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.
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). **Note** VIDs that you enter for the Untagged Ingress VID and Management VID parameters do not time out.
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

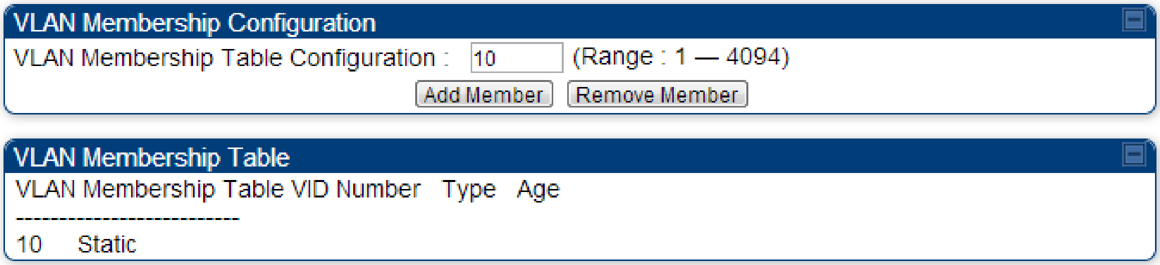
	corresponding VID is used for that frame's Q-tag (Q port) or C-tag (Q-in-Q port). If there is no match, then the Default Port VID is used. This table is also used in the downstream direction for removal of the tag based on the destination MAC address so that an untagged (for Q port) or Q-Tagged (for 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.
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	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: **Permanent**—This indicates that the module was assigned the VID number through direct configuration by the operator. **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.
Active Configuration, Current VID Member Set, Age	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: **Permanent** type - Number never times out and this is indicated by the digit 0. **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. **Note** Values in this Active Configuration block can differ from attempted values in configurations: The AP can override the value that the SM has configured for SM Management VID Pass-Through.

VLAN Membership tab of SM

The **Configuration > VLAN > VLAN Membership** tab is explained in Table 69.

Table 70 SM VLAN Membership attributes



VLAN Membership Table Configuration : 10 (Range : 1 — 4094)

```
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.

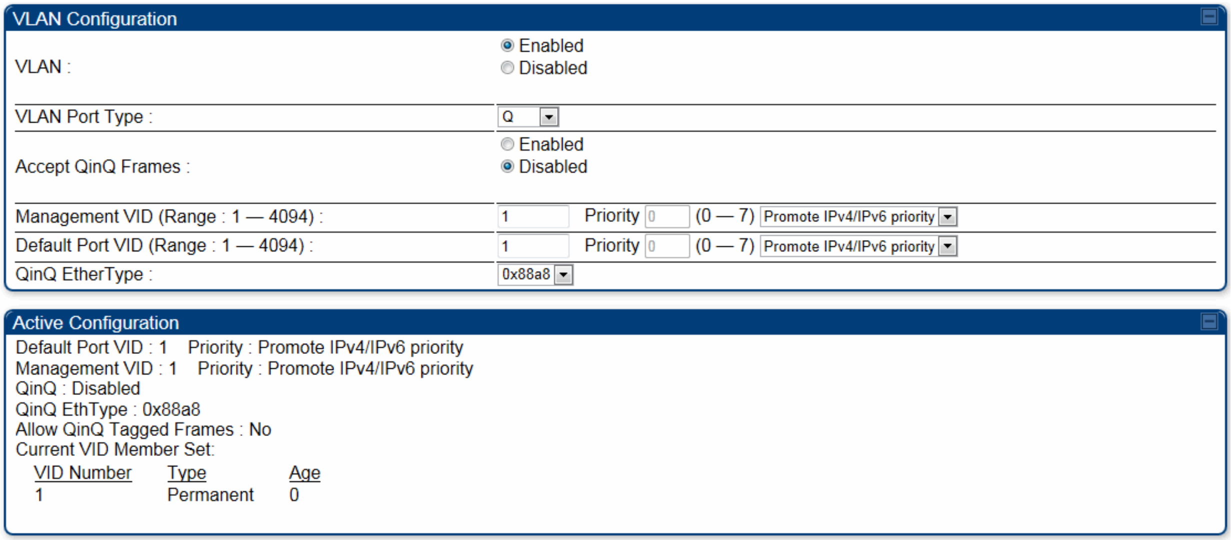
VLAN configuration for PTP

Appplicable products	**PTP:** ☑ BHM ☑ BMS

VLAN page of BHM

The VLAN tab of BHS is explained in Table 70.

Table 71 BHM VLAN page attributes



VLAN Configuration

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

Active 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

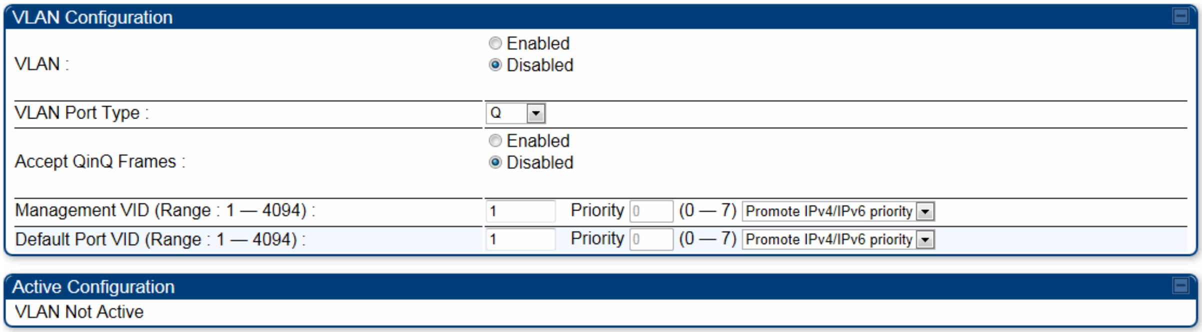
Attribute	Meaning
VLAN	Specify whether VLAN functionality for the BHM and all linked BHS must be (**Enabled**) or may not (**Disabled**) be allowed. The default value is **Disabled**.
VLAN Port Type	By default this is Q, indicating that it is to operate in the existing manner. The other option is Q-in-Q, 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

<table>
<tr>
<td></td>
<td>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:
<table>
<tr><td>Ethernet Header</td><td>S-VLAN EthType 0x88a8</td><td>C-VLAN EthType 0x8100</td><td>IP Data EthType 0x0800</td></tr>
</table>
The 802.1ad S-VLAN is the outer VLAN that is configurable on the <b>Configuration > VLAN</b> 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.</td>
</tr>
<tr>
<td>VLAN Not Active</td>
<td>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.</td>
</tr>
</table>

VLAN page of BHS

The VLAN tab of BHS is explained in Table 71.

Table 72 BHS VLAN page attributes



VLAN Configuration

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

Active Configuration

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

Appplicable products	**PMP :**	☑ 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.

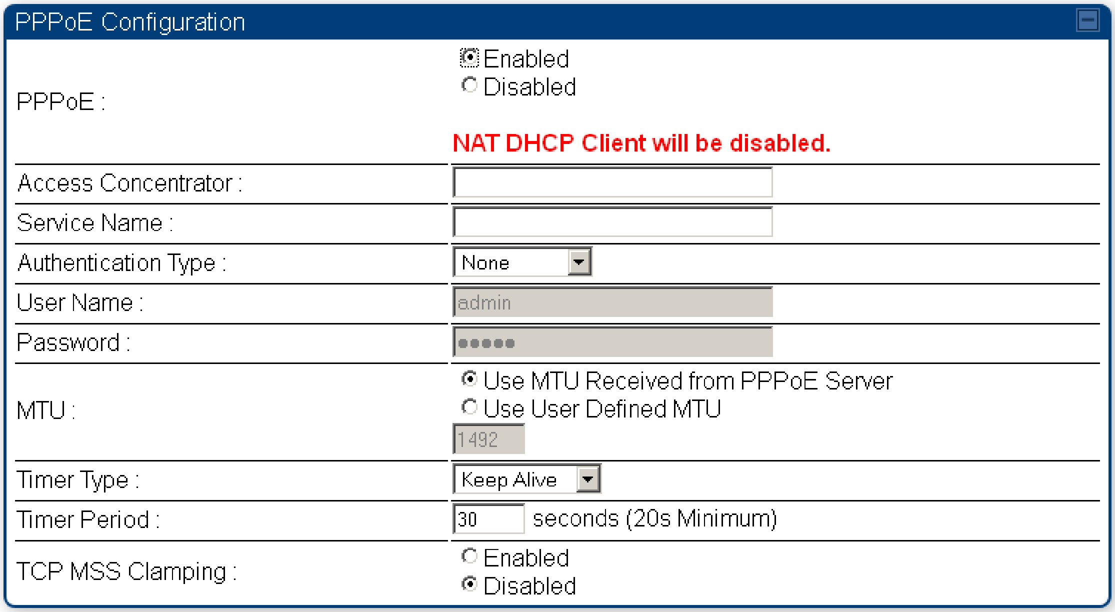
In order to enable PPPoE, NAT MUST be enabled on the SM and Translation Bridging MUST be disabled on the AP. These items is strictly enforced for you when you are trying to enable PPPoE. A message will indicate any prerequisites not being met. Also, the NAT Public IP DHCP client cannot be enabled, because 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 72.

Table 73 SM PPPoE attributes



PPPoE Configuration

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	**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. **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.
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

Appplicable products	PMP :	☑	AP	☑	SM	PTP:	☑	BHM	☑	BMS

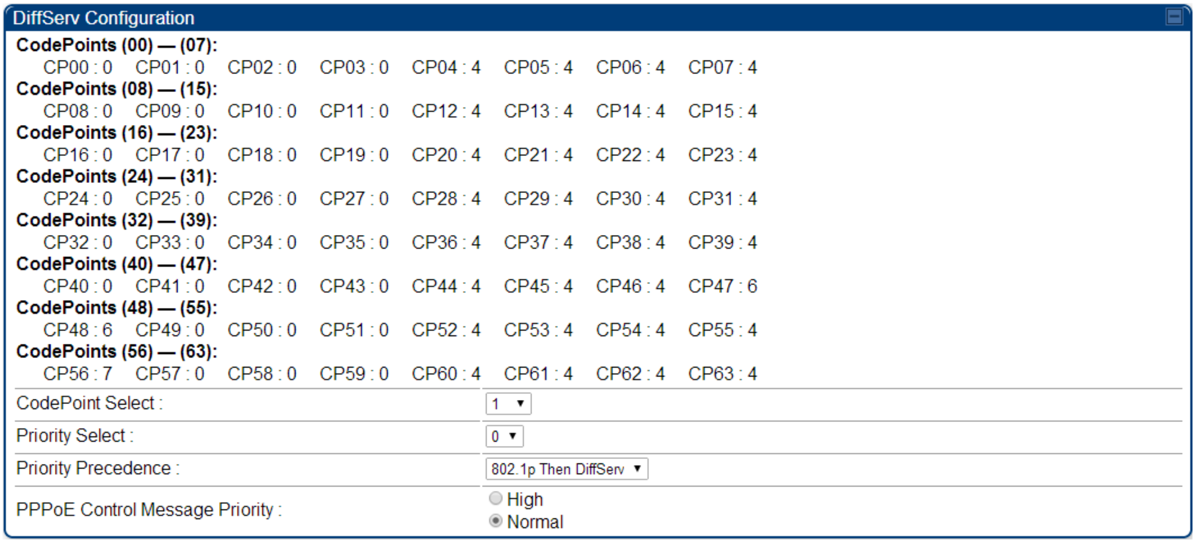
IPv4 and IPv6 Prioritization

PMP/PTP 450i 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 74 DiffServ attributes – AP/BHM



DiffServ Configuration

CodePoints (00) — (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4
CodePoints (08) — (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4
CodePoints (16) — (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4
CodePoints (24) — (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4
CodePoints (32) — (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4
CodePoints (40) — (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 6
CodePoints (48) — (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4
CodePoints (56) — (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4

CodePoint Select :	1 ▾
Priority Select :	0 ▾
Priority Precedence :	802.1p Then DiffServ ▾
PPPoE Control Message Priority :	○ High ● Normal

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.

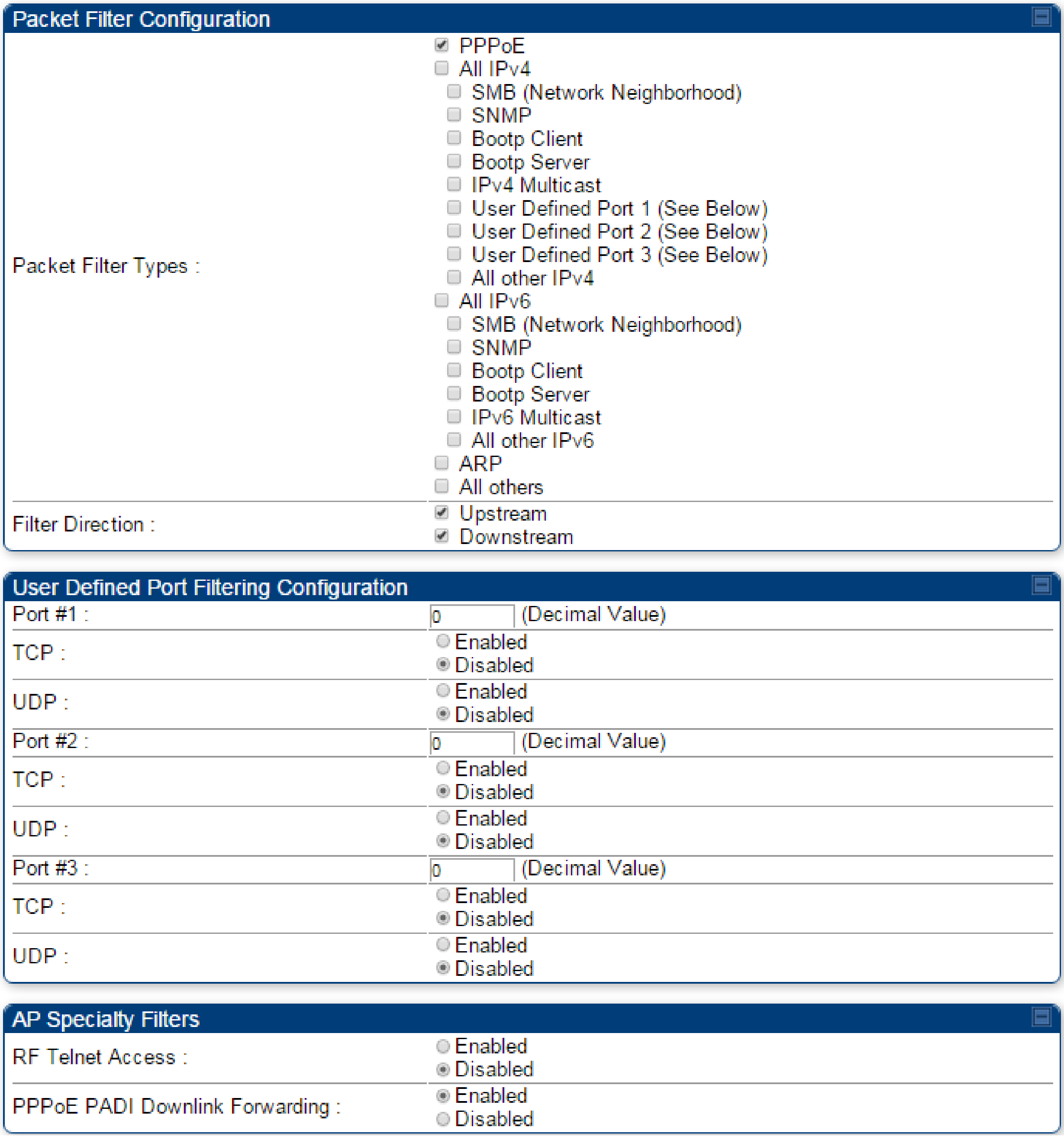
IPv4 and IPv6 Filtering

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 75 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 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #2 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #3 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled

AP Specialty Filters

RF Telnet Access :	○ Enabled ● Disabled
PPPoE PADI Downlink Forwarding :	● Enabled ○ Disabled

Attribute	Meaning
Packet Filter Types	For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. To filter packets in any of the user-defined ports, you must do all of the following: - Check the box for **User Defined Port** ***n*** **(See Below)** in the **Packet Filter Types** section of this tab.

	• 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 7-65
- Upgrading to a new software version on page 7-65

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

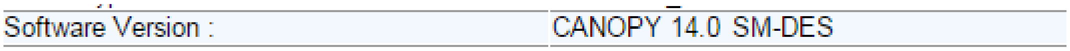
Checking the installed software version

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):



Software Version : CANOPY 14.0 SM-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 450i 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 7-65.

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 vai 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.

Configuring General and Unit Settings

General page

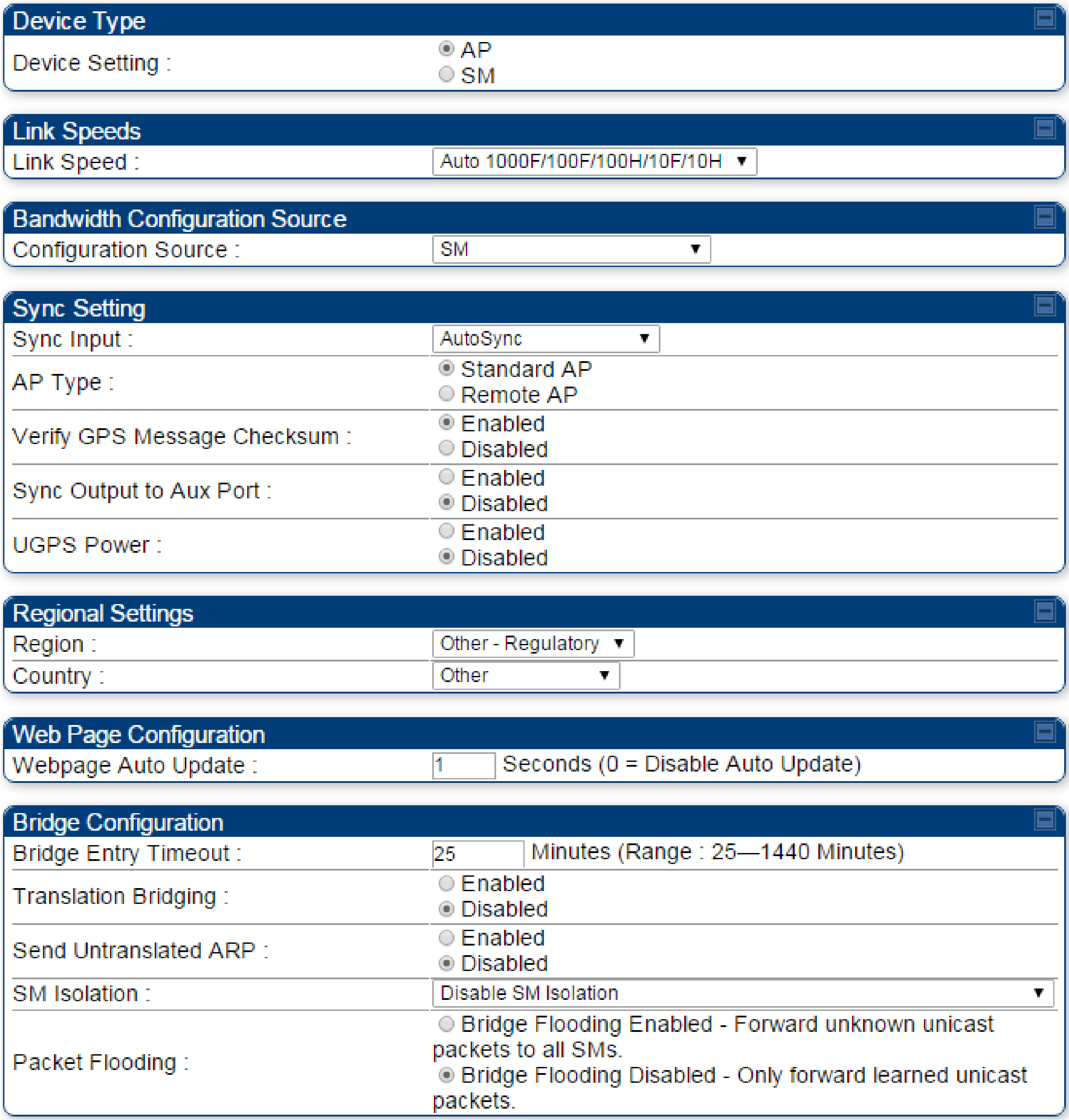
The **Configuration > General** page of the AP/BMH or BHM/BHS contains many of the configurable parameters that define how the ratio’s operate in sector or backhaul.

Appplicable products	**PMP :**	☑	AP	☑	SM	**PTP:**	☑	BHM	☑	BMS

General page of AP

The General page of AP is explained in Table 75.

Table 76 General page attributes - AP



Device Type

Device Setting :	● AP ○ SM

Link Speeds

Link Speed :	Auto 1000F/100F/100H/10F/10H ▼

Bandwidth Configuration Source

Configuration Source :	SM ▼

Sync Setting

Sync Input :	AutoSync ▼
AP Type :	● Standard AP ○ Remote AP
Verify GPS Message Checksum :	● Enabled ○ Disabled
Sync Output to Aux Port :	○ Enabled ● Disabled
UGPS Power :	○ Enabled ● Disabled

Regional Settings

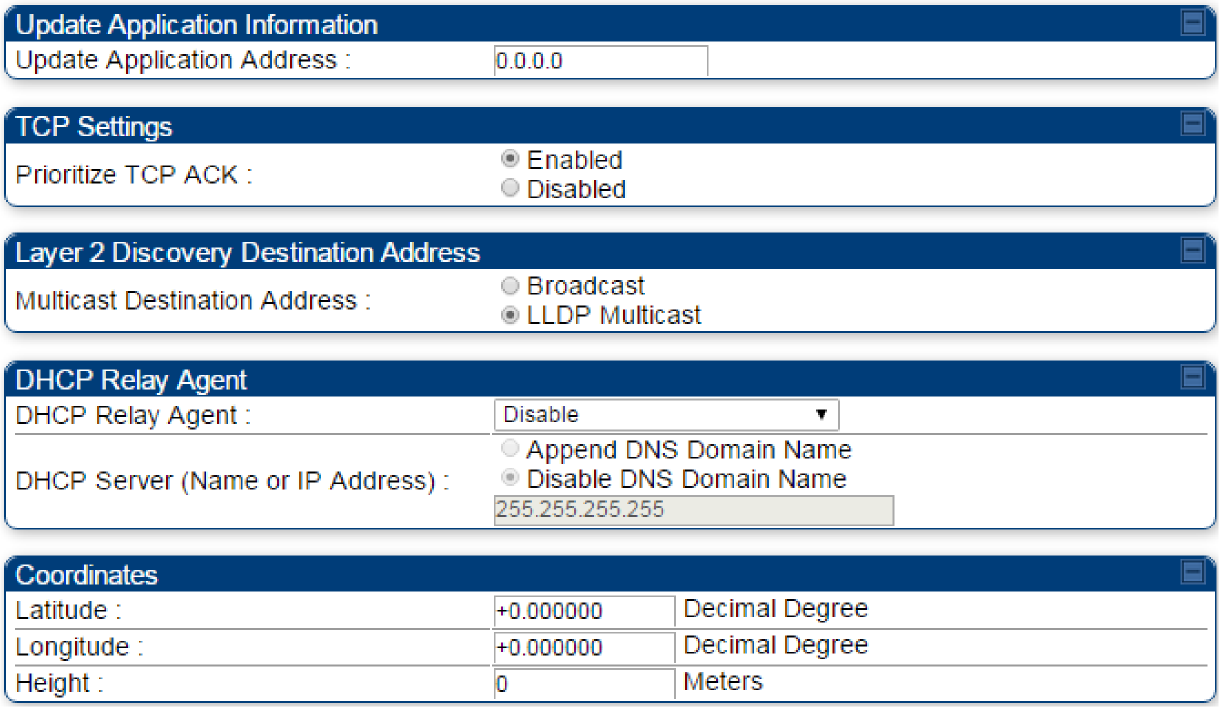
Region :	Other - Regulatory ▼
Country :	Other ▼

Web Page Configuration

Webpage Auto Update :	1 Seconds (0 = Disable Auto Update)

Bridge Configuration

Bridge Entry Timeout :	25 Minutes (Range : 25—1440 Minutes)
Translation Bridging :	○ Enabled ● Disabled
Send Untranslated ARP :	○ Enabled ● Disabled
SM Isolation :	Disable SM Isolation ▼
Packet Flooding :	○ Bridge Flooding Enabled - Forward unknown unicast packets to all SMs. ● Bridge Flooding Disabled - Only forward learned unicast packets.



Update Application Information

Update Application Address : 0.0.0.0

TCP Settings

Prioritize TCP ACK : ● Enabled ○ Disabled

Layer 2 Discovery Destination Address

Multicast Destination Address : ○ Broadcast ● LLDP Multicast

DHCP Relay Agent

DHCP Relay Agent : Disable

DHCP Server (Name or IP Address) : ○ Append DNS Domain Name ● Disable DNS Domain Name 255.255.255.255

Coordinates

Latitude : +0.000000 Decimal Degree

Longitude : +0.000000 Decimal Degree

Height : 0 Meters

Attribute	Meaning
Device Setting	Allows the Spectrum Analyzer to be run directly from AP now.
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: **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: • 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 7-158.
Sync Input	See Synchronization on page 7-88
AP Type	**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. **Remote AP**: The Autosync mechanism will source GPS synchronization from the AP's RJ-11 port or from the device on-board GPS module.
Region	From the drop-down list, select the region in which the radio is operating.

Country	From the drop-down list, select the country in which the radio is operating. 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). 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. Country Code settings affect the radios in the following ways: • 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 For more information on how transmit power limiting and DFS is implemented for each country, see the *PMP 450 Planning Guide*.
Webpage Auto Update	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.
Bridge Entry Timeout	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. **Caution** An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.
Translation Bridging	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: Not more than 10 IP devices at any time are valid to send data to the AP from behind the SM. AP populates the Translation Table tab of its Statistics web page, displaying the MAC address and IP address of all the valid connected devices. 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. If 10 are connected and another attempts to connect:

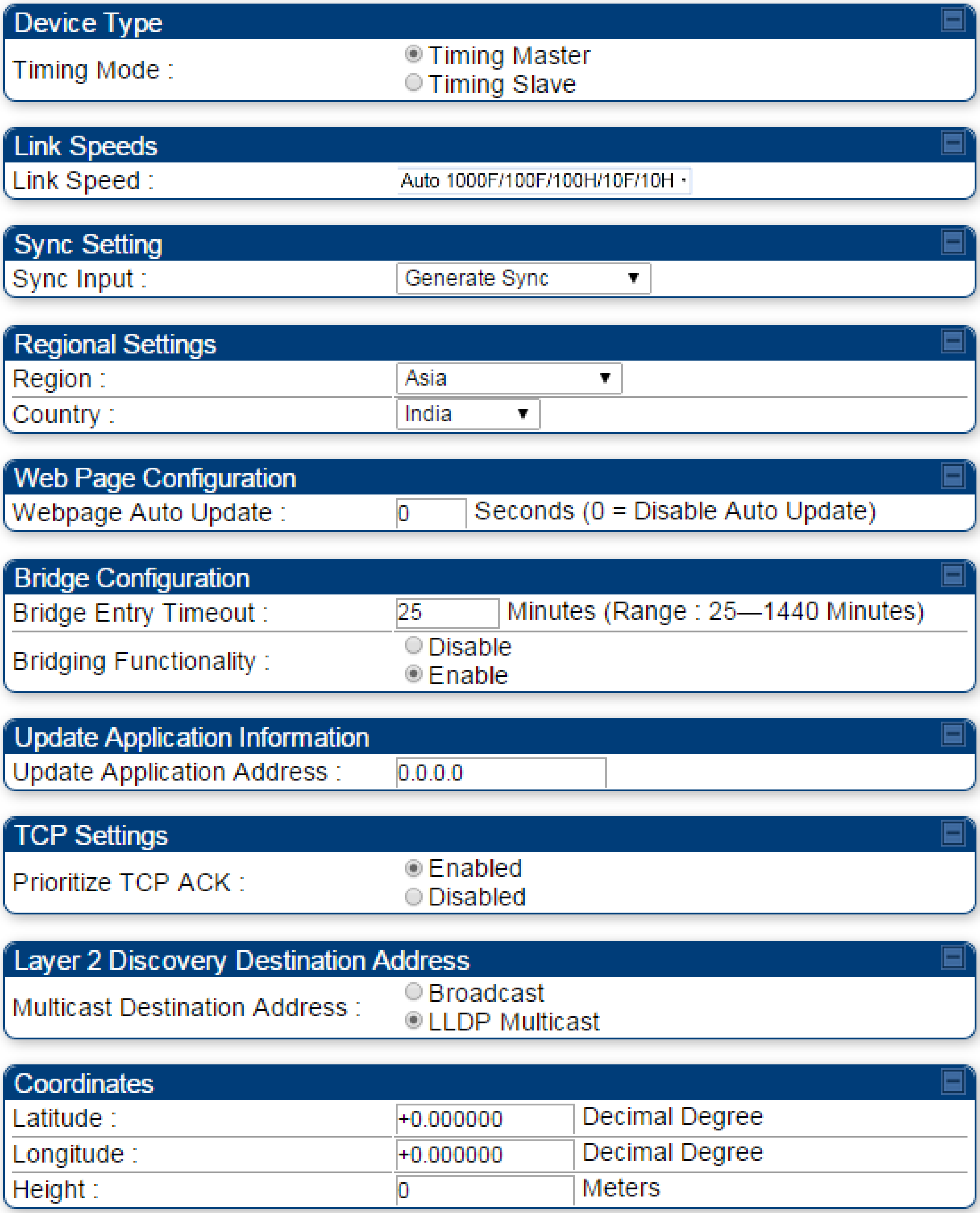
	If no Translation Table entry is older than 255 minutes, the attempt is ignored. If an entry is older than 255 minutes, the oldest entry is removed and the attempt is successful. the Send Untranslated ARP parameter in the General tab of the Configuration page can be: Disabled, so that the AP overwrites the MAC address in Address Resolution Protocol (ARP) packets before forwarding them. Enabled, so that the AP forwards ARP packets regardless of whether it has overwritten the MAC address. 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).
Send Untranslated ARP	If the **Translation Bridging** parameter is set to **Enabled**, then the **Send Untranslated ARP** parameter can be: **Disabled -** so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them. **Enabled -** so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address. If the **Translation Bridging** parameter is set to **Disabled**, then the **Send Untranslated ARP** parameter has no effect.
SM Isolation	Prevent or allow SM-to-SM communication by selecting from the following drop-down menu items: **Disable SM Isolation** (the default selection). This allows full communication between SMs. **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication. **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.
Packet Flooding	**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. **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.
Update Application	Enter the address of the server to access for software updates on this AP

Address	and registered SMs.
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	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: **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. **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. 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.
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 *Decimal Degree* while the Height is calculated in *Meters.*

General page of BHM

The General page of BHM is explained in Table 76.

Table 77 General page attributes - BHM



Device Type

Timing Mode : ● Timing Master ○ 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 : ○ Disable ● Enable

Update Application Information

Update Application Address : 0.0.0.0

TCP Settings

Prioritize TCP ACK : ● Enabled ○ Disabled

Layer 2 Discovery Destination Address

Multicast Destination Address : ○ Broadcast ● LLDP Multicast

Coordinates

Latitude : +0.000000 Decimal Degree

Longitude : +0.000000 Decimal Degree

Height : 0 Meters

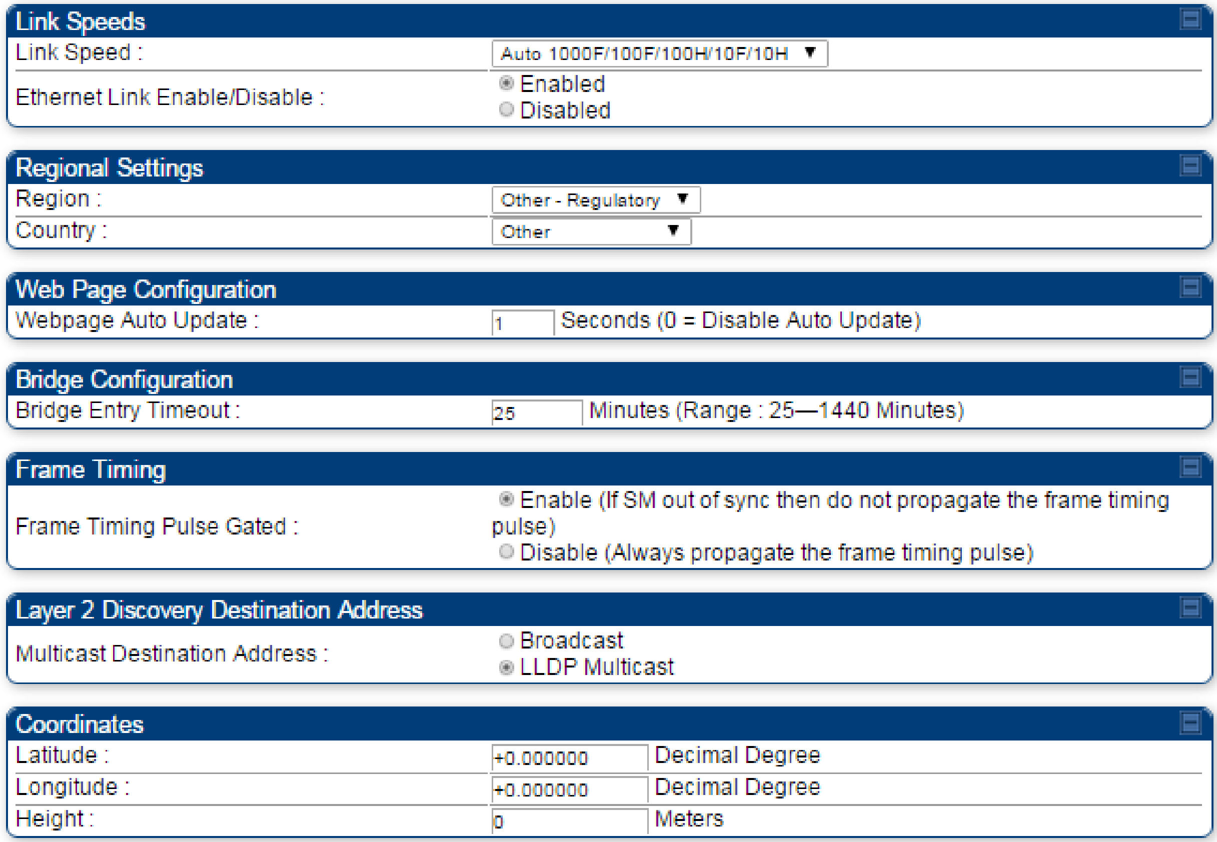
Attribute	Meaning
Timing Mode	Allows the user to choose the mode between Timing Master and Timing Slave.

Link Speed	See Table 75 General page attributes - AP on page 7-70
Sync Input	See Synchronization on page 7-88
Region	See Table 75 General page attributes - AP on page 7-70
Country	
Webpage Auto Update	
Bridge Entry Timeout	
Bridging Functionality	Select whether you want bridge table filtering active (**Enable**) or not (**Disable**) on this BH. **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. **Enable**: Allows user to enable bridge functionality. **Note** 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.
Prioritize TCP ACK	See Table 75 General page attributes - AP on page 7-70
Multicast Destination Address	
Latitude Longitude Height	

General page of SM

The General page of SM is explained in Table 77.

Table 78 General page attributes – SM



Link Speeds

Link Speed :	Auto 1000F/100F/100H/10F/10H ▼
Ethernet Link Enable/Disable :	● Enabled ○ Disabled

Regional Settings

Region :	Other - Regulatory ▼
Country :	Other ▼

Web Page Configuration

Webpage Auto Update :	1 Seconds (0 = Disable Auto Update)

Bridge Configuration

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

Frame Timing

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

Layer 2 Discovery Destination Address

Multicast Destination Address :	○ Broadcast ● LLDP Multicast

Coordinates

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

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	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: The subscriber is delinquent with payment(s). You suspect that the subscriber is sending or flooding undesired broadcast packets into the network, such as when • a virus is present in the subscriber's computing device. • the subscriber's home router is improperly configured.

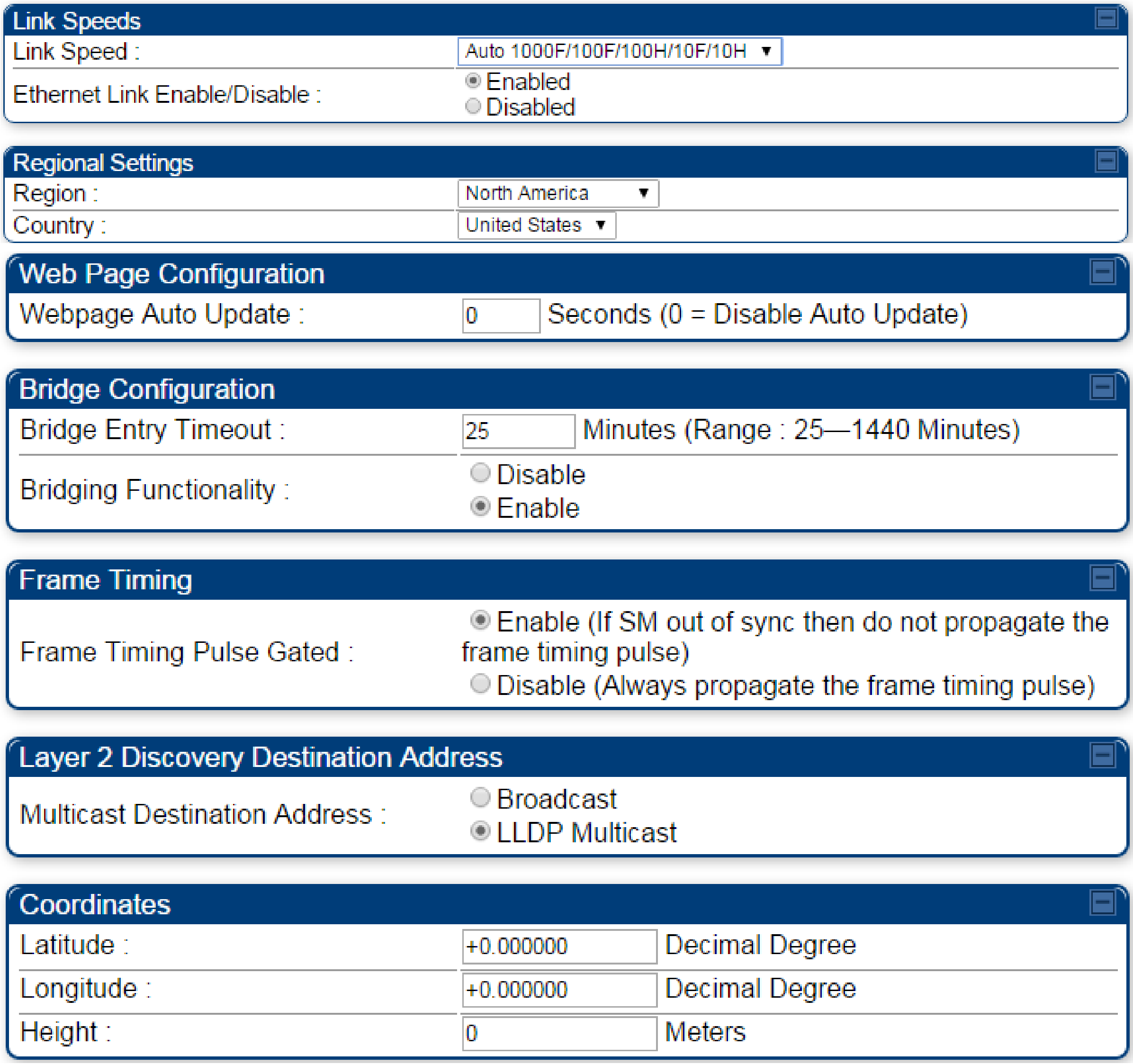
Region	This parameter allows you to set the region in which the radio will operate. The SM radio automatically inherits the Region type of the master. This behavior ignores the value of the **Region** parameter in the SM, even when the value is **None**. Nevertheless, since future system software releases 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.
Country	This parameter allows you to set the country in which the radio will operate. 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. 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.
Webpage Auto Update	See Table 75 General page attributes - AP on page 7-70
Bridge Entry Timeout	Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the 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. **Caution** This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is *25* (minutes). An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.
Frame Timing Pulse Gated	If this SM extends the sync pulse to a BH master or an AP, select either **Enable**—If this SM loses sync from the AP, then *do not* propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync. **Disable**—If this SM loses sync from the AP, then propagate the sync 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 of BHS

The General page of BHS is explained in Table 78.

Table 79 General page attributes – BHS



Link Speeds

Link Speed :	Auto 1000F/100F/100H/10F/10H ▼
Ethernet Link Enable/Disable :	● Enabled ○ 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 :	○ Disable ● Enable

Frame Timing

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

Layer 2 Discovery Destination Address

Multicast Destination Address :	○ Broadcast ● LLDP Multicast

Coordinates

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

Attribute	Meaning
Timing Mode	Allows the user to choose the mode between Timing Master and Timing Slave.
Link Speed	From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all BHMs and BHSs in the operator network.
Region	This parameter allows you to set the region in which the radio will operate. The BHS radio automatically inherits the Region type of the master. This behavior ignores the value of the **Region** parameter in the BHS, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter must be always set to the value that corresponds to the local region.
Country	This parameter allows you to set the country in which the radio will operate. The BHS radio automatically inherits the Country Code type of the master. This behavior ignores the value of the **Country** parameter in the BHS, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter must be always set to the value that corresponds to the local region. PMP/PTP 450i 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.
Webpage Auto Update	See Table 75 General page attributes - AP on page 7-70
Bridge Entry Timeout	Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the BHM encounters no activity with the BHS (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout must be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network. ⚠ **Caution** This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is *25* (minutes). An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end

	users.
Bridging Functionality	See Table 76 General page attributes - BHM on page 7-75
Frame Timing Pulse Gated	If this BHS extends the sync pulse to a BH master or an BHM, select either **Enable**—If this BHS loses sync from the BHM, then *do not* propagate a sync pulse to the BH timing master or other BHM. This setting prevents interference in the event that the BHS loses sync. **Disable**—If this BHS loses sync from the BHM, then propagate the sync pulse to the BH timing master or other BHM.
Multicast Destination Address	See Table 75 General page attributes - AP on page 7-70
Latitude Longitude Height	See Table 76 General page attributes - BHM on page 7-75

Unit Settings page

Appplicable products	**PMP :**	☑	AP	☑	SM	**PTP:**	☑	BHM	☑	BMS

The **Unit Settings** page of the PMP/PTP 450i 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 Pannel setting is applicable for SM only.

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

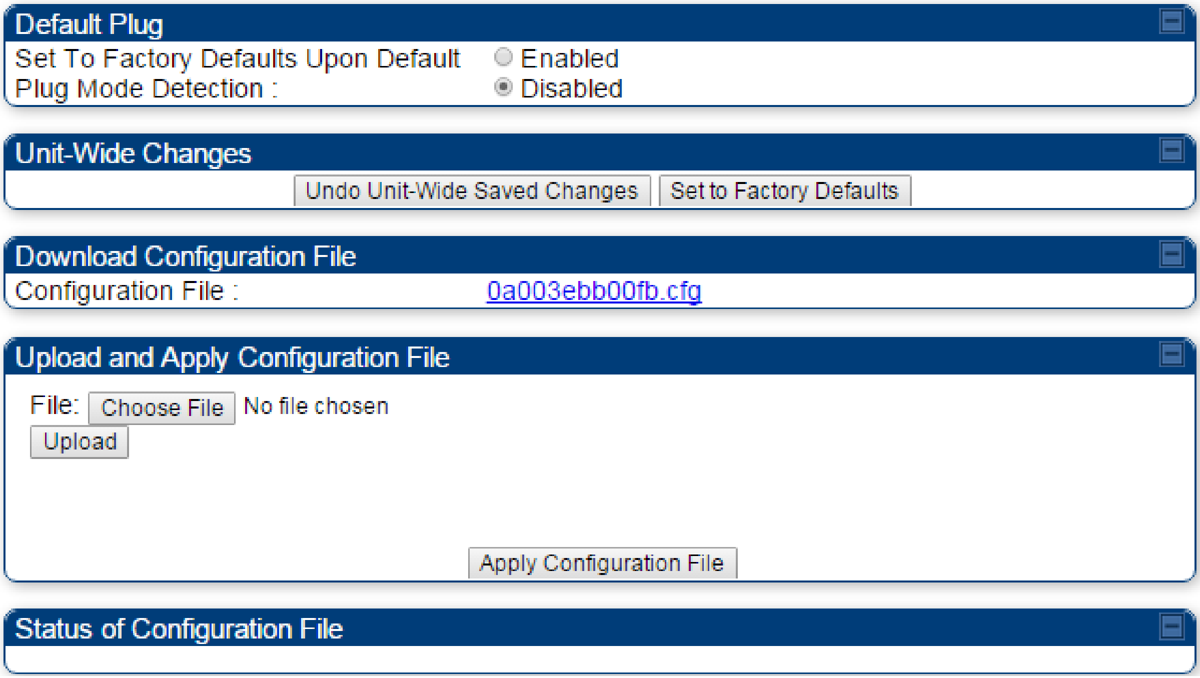
The PMP/PTP 450i also supports import and export of configuration from the AP/BHM/SM/BHS as a text file. The configuration file is in JSON format. The logged in user must be an ADMINISTRATOR in order to export or import the configuration file.

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 7-173.

Unit Settings page of AP/BHM

The Unit Setting page of AP/BHM is explained in Table 79.

Table 80 Unit Settings attributes – AP/BHM


Default Plug
Unit-Wide Changes
Undo Unit-Wide Saved Changes
Set to Factory Defaults
Download Configuration File
Upload and Apply Configuration File
Choose File
Upload
Apply Configuration File
Status of Configuration File

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

Configuration File : 0a003ebb00fb.cfg

File: No file chosen

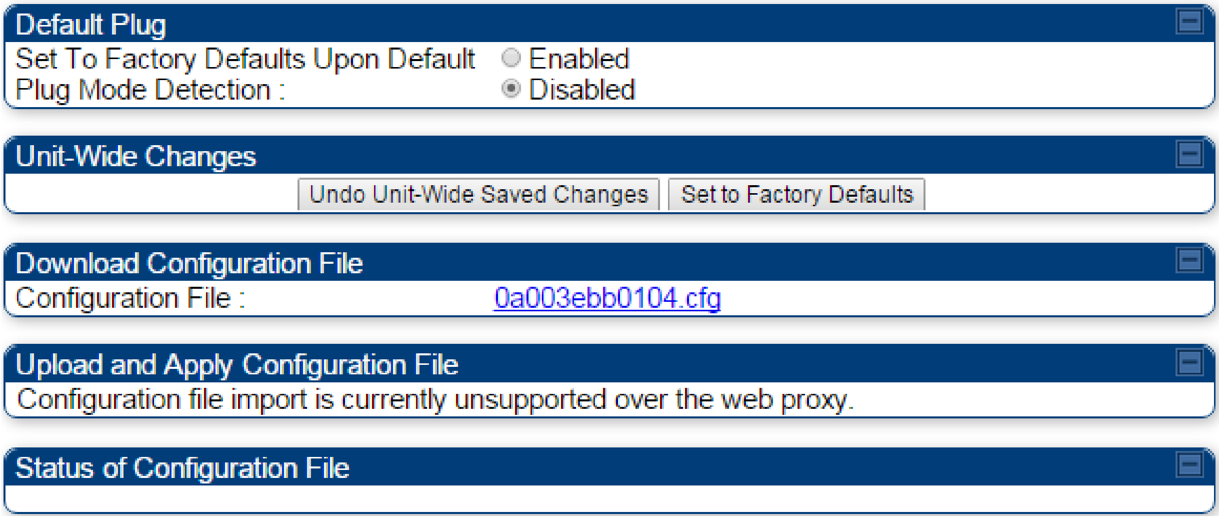
Attribute	Meaning
Set to Factory Defaults Upon Default Mode Detection	If **Enabled** is checked, then the default mode functions is enabled. When the module is rebooted with Default mode enabled, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. A subscriber, technician, or other person who gains physical access to the module and uses an override *cannot* see or learn the settings that were previously configured in it. If **Disabled** is checked, then the default mode functions is disabled. See Radio recovery mode – Radio Recovery Console / Default Mode (fka Default Plug) on page 1-16 **Caution** When **Set to Factory Defaults Upon Default Mode** is set to **Enable**, the radio does not select all of the frequencies for Radio Frequency Scan Selection List. It needs to be selected manually.
Undo Unit-Wide Saved Changes	When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.
Set to Factory	When you click this button, *all configurable parameters on all tabs* are

Defaults	reset to the factory settings. **Note** This can be reverted by selecting "Undo Unit-Wide Saved Changes", *before* rebooting the radio, though this is not recommended.
Configuration File	This allows to download the configuration file of the radio. This configuration file contains the complete configuration including all the default values. The configuration file is highlighted as downloadable link and the naming convention is “<mac address of AP>.cfg”.
Apply Configuration File	This allows to import and apply configuration to the AP. **Chose File**: Select the file to upload the configuration. The configuration file is named as “<file name>.cfg”. **Upload**: Import the configuration to the AP. **Apply Configuration File**: Apply the imported configuration file to the AP. The imported configuration file may either contain a full device configuration or a partial device configuration. If a partial configuration file is imported, only the items contained in the file will be updated, the rest of the device configuration parameters will remain the same. Operators may also include a special flag in the configure file to instruct the device to first revert to factory defaults then to apply the imported configuration.
Status of Configuration file	This section shows the results of the upload.

Unit Settings page of SM/BHS

The Unit Settings page of SM/BHS is explained in Table 80.

Table 81 SM Unit Settings attributes



Default Plug

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

Unit-Wide Changes

Download Configuration File

Configuration File : 0a003ebb0104.cfg

Upload and Apply Configuration File

Configuration file import is currently unsupported over the web proxy.

Status of Configuration File

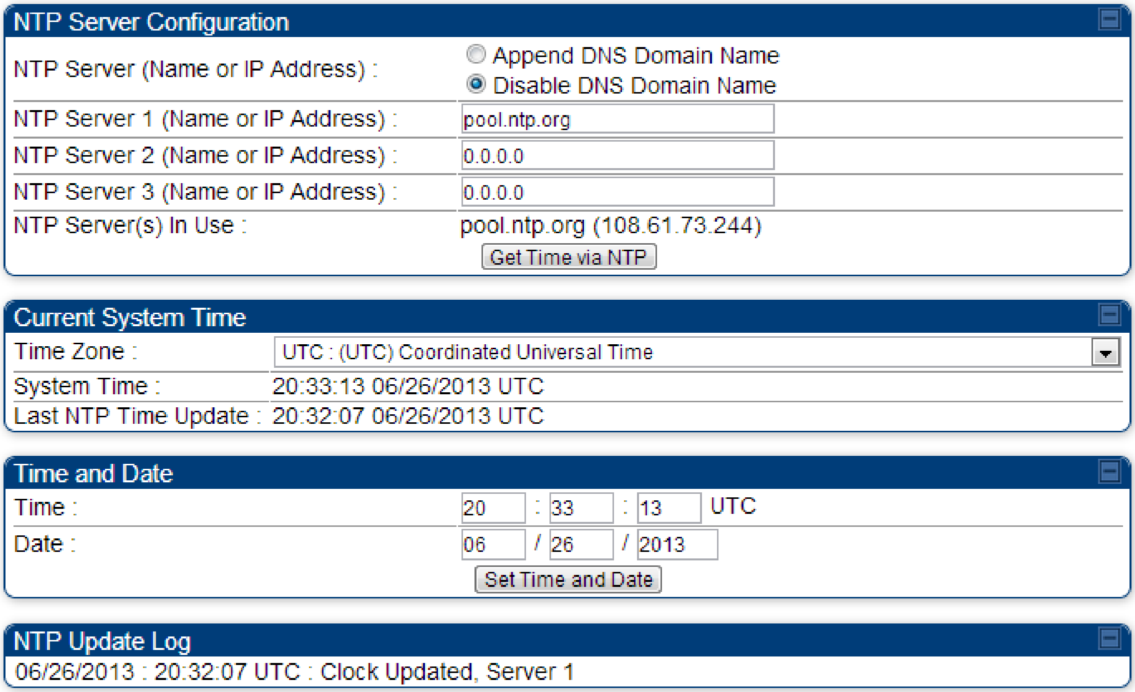
Attribute	Meaning
Set to Factory Defaults Upon Default Plug Detection	See Table 79 Unit Settings attributes – AP/BHM on page 7-83
Undo Unit-Wide Saved Changes	See Table 79 Unit Settings attributes – AP/BHM on page 7-83
Set to Factory Defaults	
Configuration File	
Status of Configuration file	

Time page of AP/BHM

Appplicable products	PMP : ☑ AP	PTP: ☑ BHM

The Time page of AP/BHM is explained in Table 81.

Table 82 AP 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) : pool.ntp.org

NTP Server 2 (Name or IP Address) : 0.0.0.0

NTP Server 3 (Name or IP Address) : 0.0.0.0

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

Current System Time

Time Zone : UTC : (UTC) Coordinated Universal Time

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) NTP Server 2 (Name or IP Address) NTP Server 3 (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: • 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.

Synchronization

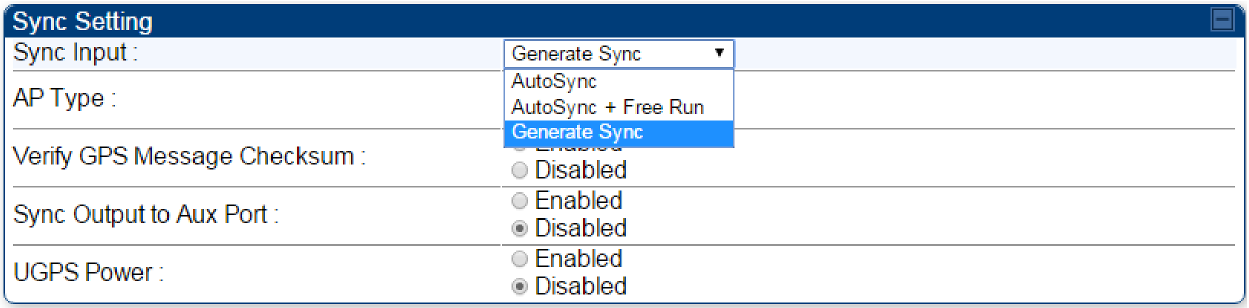
This section describe synchronization options for PMP and PTP configuration.

This **Sync Input** parameter can be configured under Sync Setting tab of **Configure > General** page (see General page on page 7-69).

PMP/PTP 450i has following sysnchronization options:

- AutoSync
- AutoSync + Free Run
- Generate Sync

Figure 65 Sync Setting configuration



Sync Setting

Sync Input :	Generate Sync ▼ AutoSync AutoSync + Free Run Generate Sync
AP Type :	
Verify GPS Message Checksum :	○ Disabled
Sync Output to Aux Port :	○ Enabled ● Disabled
UGPS Power :	○ Enabled ● 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.

Configuring security

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

- Managing module access by password on page 7-91: to configure the unit access password and access level
- Isolating from the internet on page 7-94: to ensure that APs are properly secured from external networks
- Encrypting radio transmissions on page 7-94: to configure the unit to operate with AES or DES wireless link security
- Requiring SM Authentication on page 7-94: to set up the AP to require SMs to authenticate via the AP, WM, or RADIUS server
- Filtering protocols and ports on page 7-95: to filter (block) specified protocols and ports from leaving the system
- Encrypting downlink broadcasts on page 7-99: to encrypt downlink broadcast transmissions
- Isolating SMs on page 7-99: to prevent SMs in the same sector from directly communicating with each other
- Filtering management through Ethernet on page 7-100: to prevent management access to the SM via the radio's Ethernet port
- Allowing management only from specified IP addresses on page 7-100: to only allow radio management interface access from specified IP addresses
- Restricting radio Telnet access over the RF interface on page 7-100: to restrict Telnet access to the AP
- Configuring SNMP Access on page 7-102
- Configuring Security on page 7-104

Managing module access by password

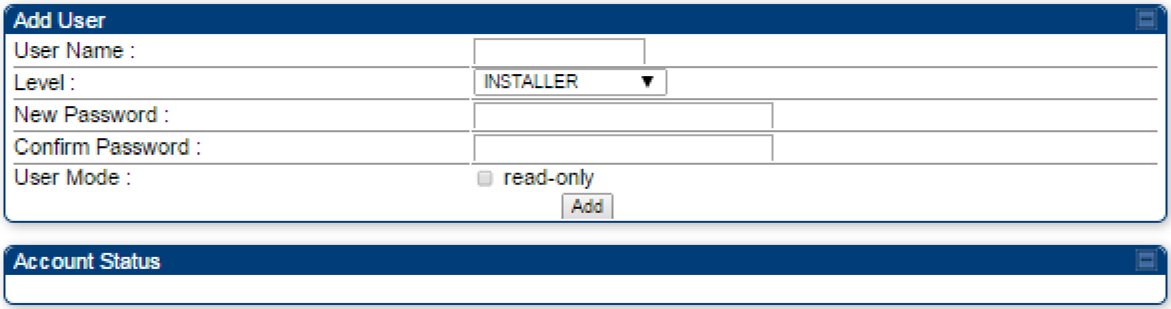
Appplicable products	PMP :	☑	AP	☑	SM	PTP:	☑	BHM	☑	BMS

See Managing module access by passwords on page 3-35.

Adding a User for Access to a module

The **Account > Add User** page allows to create a new user for accessing AP/SM/BHM/BHS. The Add User page is explained in Table 82.

Table 83 Add User page of account page - AP/ SM/BH



Add User

User Name :	
Level :	INSTALLER ▼
New Password :	
Confirm Password :	
User Mode :	□ read-only

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 3-35.
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.

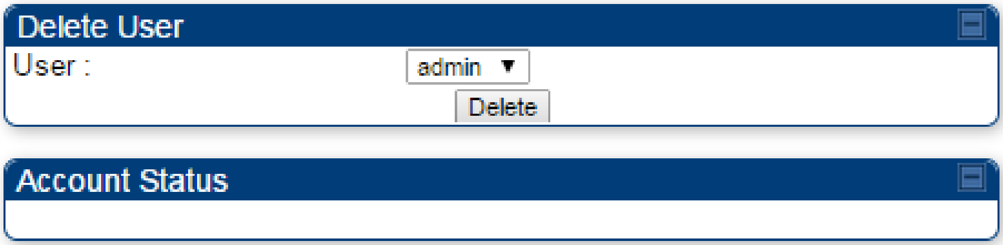
Note

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 Delele User page is explained in Table 83.

Table 84 Delete User page - AP/ SM/BH



Delete User

User : admin ▼

Account Status

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

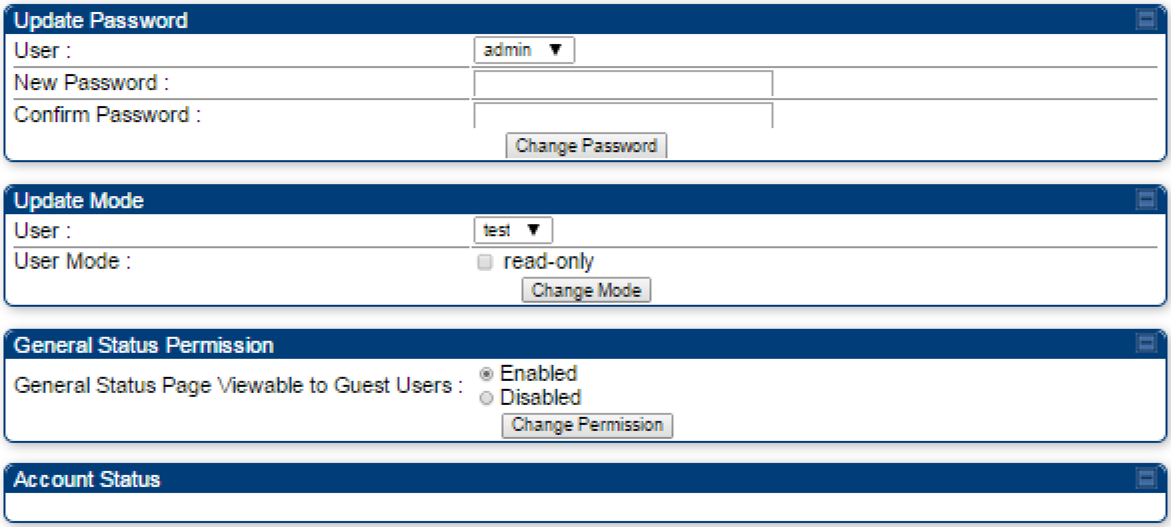
Changing a User Setting

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

From the factory default state, configure passwords for both the root and admin account at the ADMINISTRATOR permission level, using **Update Password** tab of Change Users Setting page.

The Change User Setting page is explained in Table 84.

Table 85 Change User Setting page - AP/ SM/BH



Update Password

User : admin ▼

New Password :

Confirm Password :

Update Mode

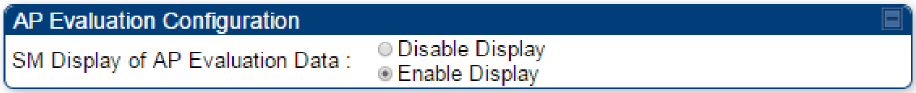
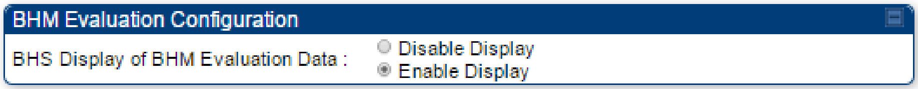
User : test ▼

User Mode : □ read-only

General Status Permission

General Status Page Viewable to Guest Users : ● Enabled ○ Disabled

Account Status

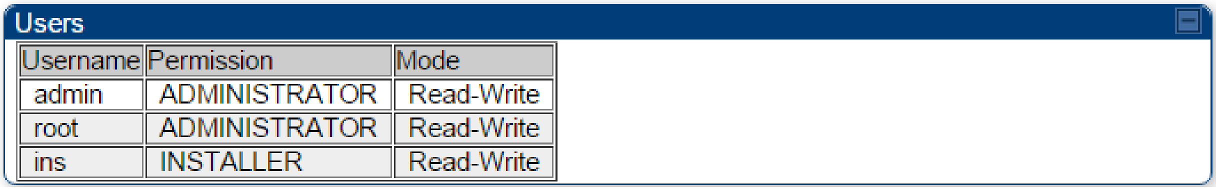
Attribute	Meaning
Update Password tab	This tab provides a drop down list of configured users from which a user is selected to change password.
Update Mode tab	This tab facilitates to convert a configured user to a Read-Only user.
General Status Permission tab	This tab enables and disables visibility of **General Status Page** for all Guest user. To display of Radio data on SMs/BHS main Login page for Guest login, it can be enabled or disabled in Security tab of Configuration page. **Figure 66** AP Evaluation Configuration parameter of Security tab for PMP  AP Evaluation Configuration SM Display of AP Evaluation Data : ○ Disable Display ● Enable Display **Figure 67** BHM Evaluation Configuration parameter of Security tab for PTP  BHM Evaluation Configuration BHS Display of BHM Evaluation Data : ○ Disable Display ● Enable Display

Users account

The **Account > Users** page allows to view all configured users account for accessing the module.

The Users page is explained in Table 85.

Table 86 User page – AP/SM/BH



Users

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 1-16

See Recovery mode options on page1-17

Isolating from the internet – APs/BHMs

Appplicable products	PMP :	☑ AP		PTP:	☑ BHM

See Isolating AP/BHM from the Internet on page 3-33.

Encrypting radio transmissions

Appplicable products	PMP :	☑ AP	☑ SM	PTP:	☑ BHM	☑ BMS

See Encrypting radio transmissions on page 3-33.

Requiring SM Authentication

Appplicable products	PMP :	☑ AP	☑ SM

Through the use of a shared AP key, or an external RADIUS (Remote Authentication Dial In User Service) server, it enhances network security by requiring SMs to authenticate when they register.

For descriptions of each of the configurable security parameters on the AP, see Configuring Security on page 7-104. For descriptions of each of the configurable security parameters on the SM, see Security on page 7-108.

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.
- **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 7-175.

Filtering protocols and ports

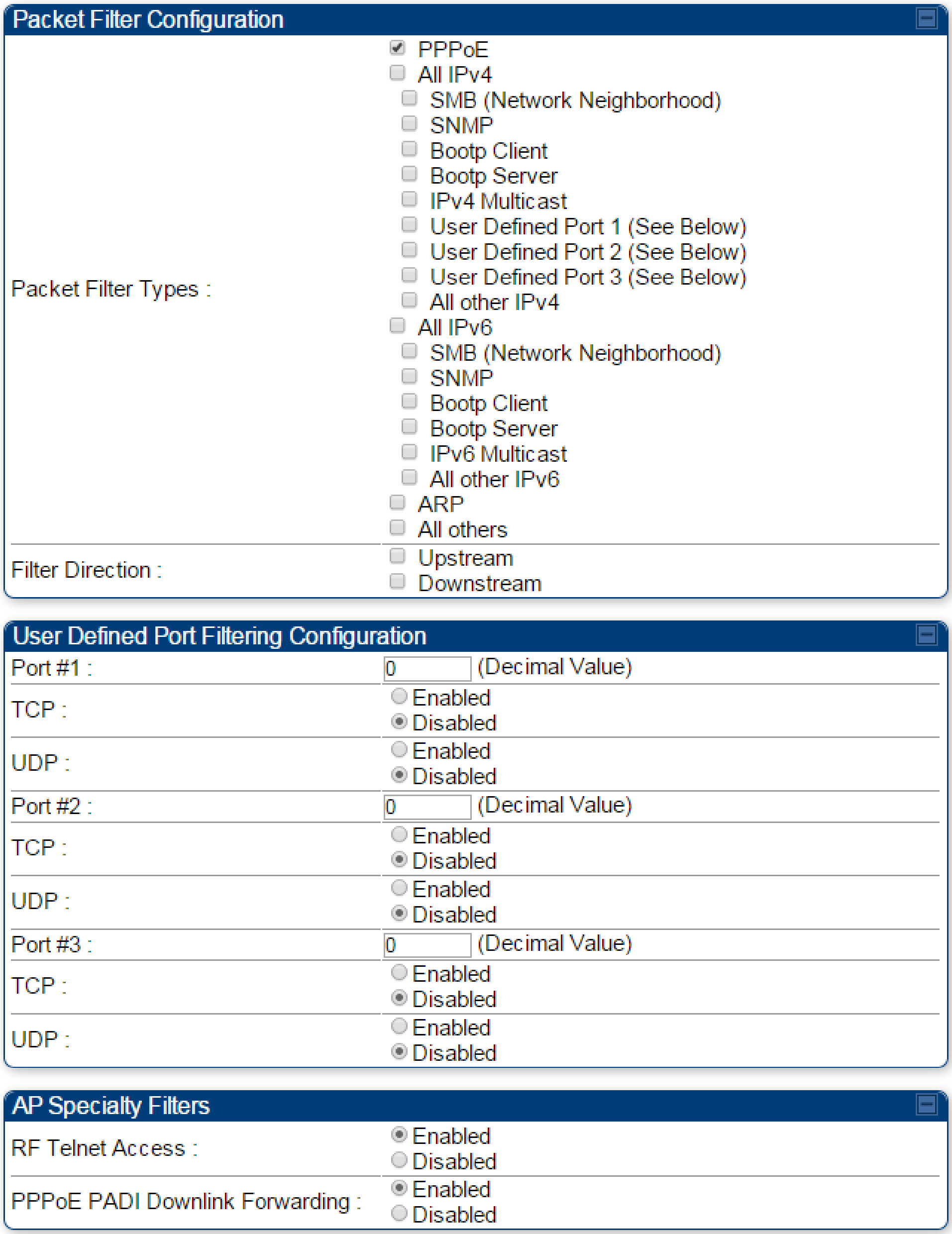
Appplicable products	PMP :	☑	AP	☑	SM	PTP:	☑	BHM	☑	BMS

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 3-36.

Protocol filtering page of AP/BHM

The Protocol Filtering page of AP/BHM is explained in Table 86.

Table 87 AP/BHM Protocol Filtering attributes



Packet Filter Configuration

Packet Filter Types :	☑ PPPoE □ All IPv4 □ SMB (Network Neighborhood) □ SNMP □ Bootp Client □ Bootp Server □ IPv4 Multicast □ User Defined Port 1 (See Below) □ User Defined Port 2 (See Below) □ User Defined Port 3 (See Below) □ All other IPv4 □ All IPv6 □ SMB (Network Neighborhood) □ SNMP □ Bootp Client □ Bootp Server □ IPv6 Multicast □ All other IPv6 □ ARP □ All others
Filter Direction :	□ Upstream □ Downstream

User Defined Port Filtering Configuration

Port #1 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #2 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #3 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled

AP Specialty Filters

RF Telnet Access :	● Enabled ○ Disabled
PPPoE PADI Downlink Forwarding :	● Enabled ○ Disabled

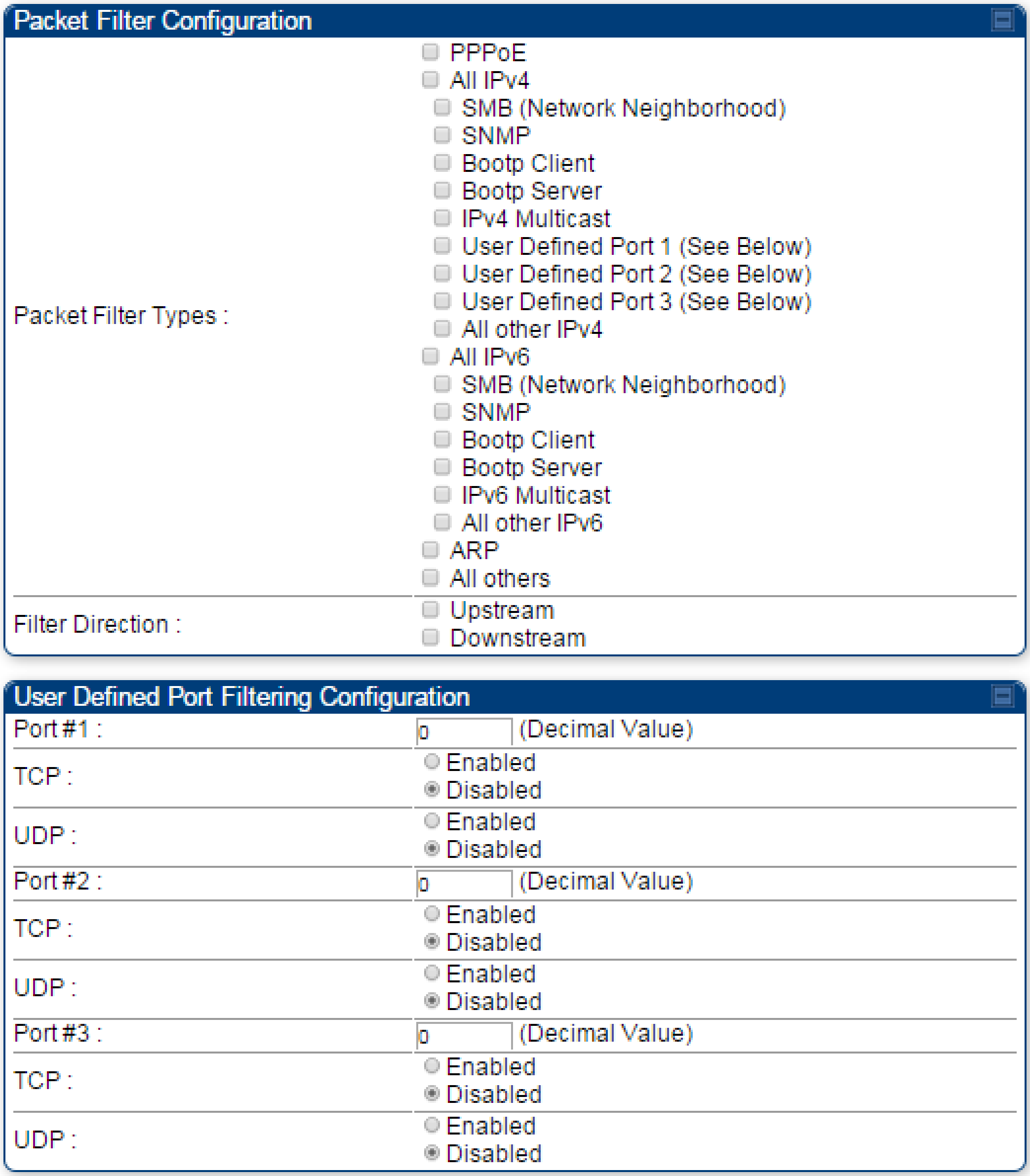
Attribute	Meaning
Packet Filter Types	For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. To filter packets in any of the user-defined ports, must do all of the following: Check the box for **User Defined Port *n* (See Below)** in the **Packet Filter Types** section of this tab. In the **User Defined Port Filtering Configuration** section of this tab: • provide a port number at **Port #*n***.

	• enable **TCP** and/or **UDP** by clicking the associated radio button
Filter Direction	Operators may choose to filter upstream (uplink) RF packets or downstream (downlink) RF packets.
User Defined Port Filtering Configuration	You can specify ports for which to block subscriber access, regardless of whether NAT is enabled.
RF Telnet Access	RF Telnet Access restricts Telnet access to the AP/BHM from a device situated below a network SM/BHS (downstream from the AP/BHM). This is a security enhancement to restrict RF-interface sourced AP access specifically to the LAN1 IP address and LAN2 IP address (Radio Private Address, typically 192.168.101.[LUID]). This restriction disallows unauthorized users from running Telnet commands on the AP/BHM that can change AP/BHM configuration or modifying network-critical components such as routing and ARP tables.
PPPoE PADI Downlink Forwarding	**Enabled**: the AP/BHM allows downstream and upstream transmission of PPPoE PADI packets. By default, PPPoE PADI Downlink Forwarding is set to “Enabled”. **Disabled**: the AP/BHM disallows PPPoE PADI packets from entering the Ethernet interface and exiting the RF interface (downstream to the SM/BHS). PPPoE PADI packets are still allowed to enter the AP’s RF interface and exit the AP’s /BHM’s Ethernet interface (upstream).

Protocol filtering page of SM/BHS

The Protocol Filtering page of SM/BHS is explained in Table 87.

Table 88 SM/BHS Protocol Filtering attributes



Packet Filter Configuration

Packet Filter Types :

- □ PPPoE
- □ All IPv4
  - □ SMB (Network Neighborhood)
  - □ SNMP
  - □ Bootp Client
  - □ Bootp Server
  - □ IPv4 Multicast
  - □ User Defined Port 1 (See Below)
  - □ User Defined Port 2 (See Below)
  - □ User Defined Port 3 (See Below)
  - □ All other IPv4
- □ All IPv6
  - □ SMB (Network Neighborhood)
  - □ SNMP
  - □ Bootp Client
  - □ Bootp Server
  - □ IPv6 Multicast
  - □ All other IPv6
- □ ARP
- □ All others

Filter Direction :

- □ Upstream
- □ Downstream

User Defined Port Filtering Configuration

Port #1 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #2 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled
Port #3 :	0 (Decimal Value)
TCP :	○ Enabled ● Disabled
UDP :	○ Enabled ● Disabled

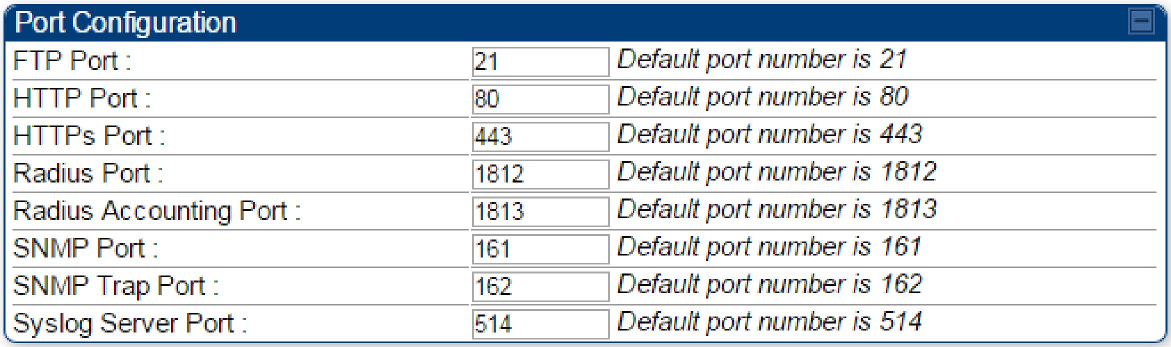
Attribute	Meaning
Packet Filter Configuration tab	See Table 86 AP/BHM Protocol Filtering attributes on page 7-96
User Defined Port Filtering Configuration tab	See Table 86 AP/BHM Protocol Filtering attributes on page 7-96

Port configuration

PMP/PTP 450i 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 88.

Table 89 Port Configuration attributes – AP/SM/BHM/BMS



Port Configuration

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

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

Encrypting downlink broadcasts

See Encrypting downlink broadcasts on page 3-40.

Isolating SMs

See Isolating SMs in PMP on page 3-40.

Filtering management through Ethernet

See Filtering management through Ethernet on page 3-40.

Allowing management only from specified IP addresses

See Allowing management from only specified IP addresses on page 3-41.

Restricting radio Telnet access over the RF interface

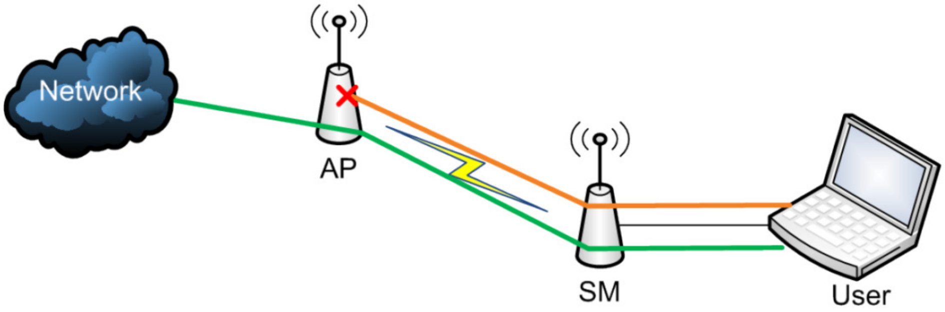
RF Telnet Access restricts Telnet access to the AP from a device situated below a network SM (downstream from the AP). This is a security enhancement to restrict RF-interface sourced AP access specifically to the LAN1 IP address and LAN2 IP address (Radio Private Address, typically 192.168.101. [LUID]). 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 68).

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", 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 68 RF Telnet Access Restrictions (orange) and Flow through (green)



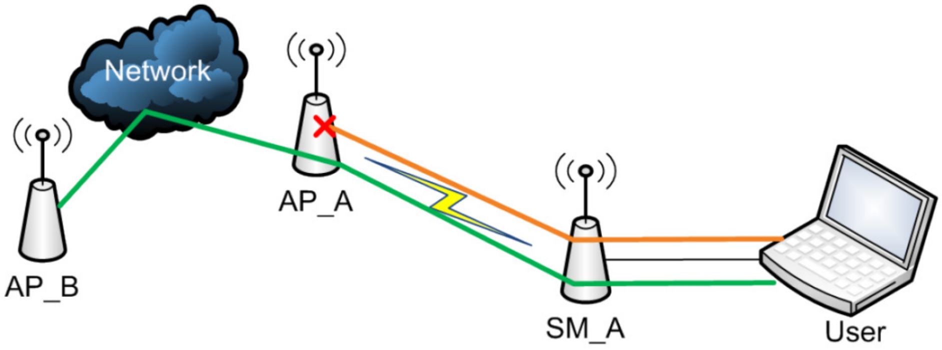
Key Security Considerations when using the RF Telnet Access Feature

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 69) via their Ethernet interfaces (since RF Telnet Access only prevents Telnet sessions originating from the AP's wireless interface).

Figure 69 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

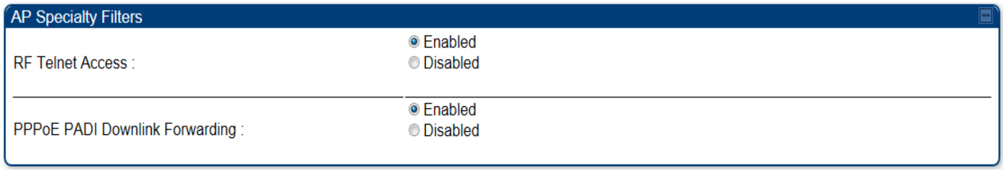
To restrict all Telnet access to the AP via the RF interface from downstream devices, follow these instructions using the AP GUI:

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 : ● Enabled ○ Disabled

PPPoE PADI Downlink Forwarding : ● Enabled ○ Disabled

4 Click the **Save** button

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

Configuring SNMP Access

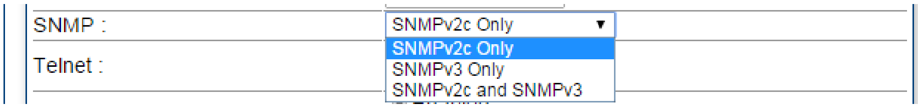
The SNMPv3 interface provides a more secure method to perform SNMP operations. This standard provides services for authentication, data integrity and message encryption over SNMP. Refer to Planning for SNMPv3 operation on page 3-34 for details.

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**



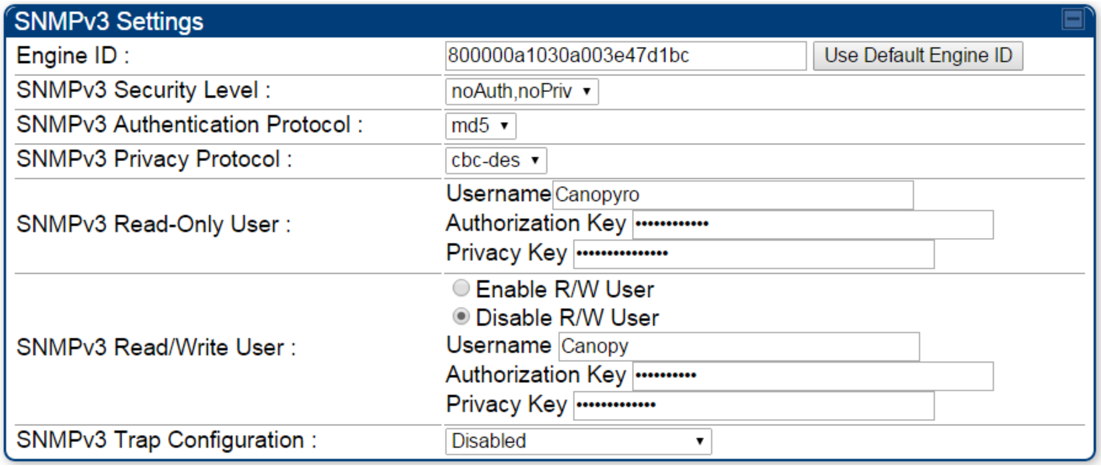
SNMP : SNMPv2c Only ▾

Telnet :

4 Click the **Save Changes** button

5 Go to **Configuration > SNMP Page**

6 Under GUI heading “SNMPv3 setting”, set **Engine ID, SNMPv3 Security Level, SNMPv3 Authentication Protocol, SNMPv3 Privacy Protocol, SNMPv3 Read-Only User, SNMPv3 Read/Write User, SNMPv3 Trap Configuration** parameters:



SNMPv3 Settings

Engine ID :	800000a1030a003e47d1bc [Use Default Engine ID]
SNMPv3 Security Level :	noAuth,noPriv ▾
SNMPv3 Authentication Protocol :	md5 ▾
SNMPv3 Privacy Protocol :	cbc-des ▾
SNMPv3 Read-Only User :	Username Canopyro Authorization Key •••••••••••• Privacy Key •••••••••••••••
SNMPv3 Read/Write User :	○ Enable R/W User ● Disable R/W User Username Canopy Authorization Key •••••••••• Privacy Key •••••••••••••
SNMPv3 Trap Configuration :	Disabled ▾

Engine ID :

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

SNMPv3 security level, Authentication and Privacy Protocol

The authentication allows authentication of SNMPv3 user and privacy allows for encryption of SNMPv3 message. PMP/PTP 450i 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

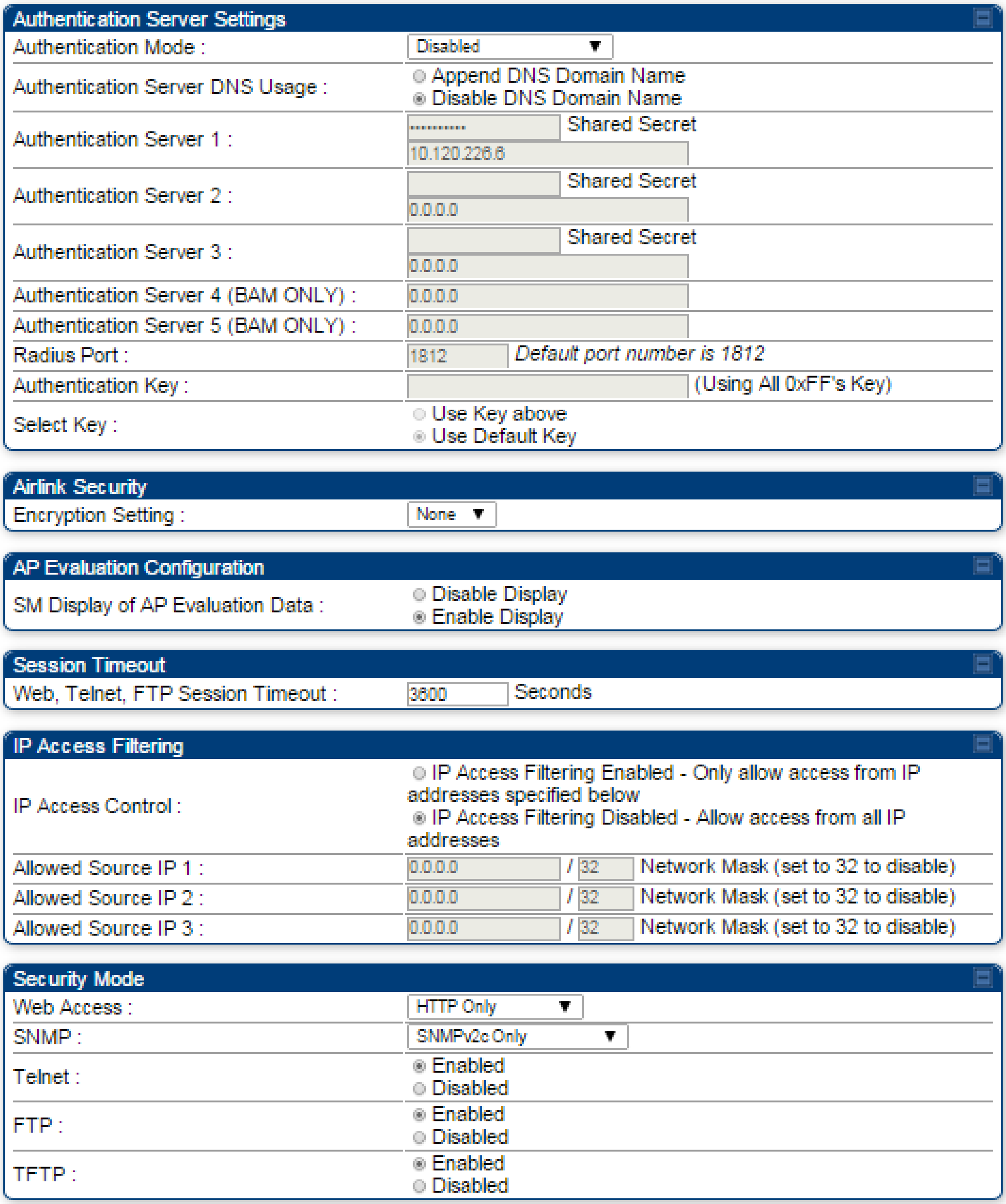
The traps may be sent from radios in SNMPv3 format based on parameter settings. It can be configured for Disabled, Enabled for Read-Only User, Enable for Read/Write User.

Configuring Security

Security page of AP/BHM

The security page of AP/BHM is explained in Table 89.

Table 90 Security tab of the AP



Authentication Server Settings

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

Airlink Security

Encryption Setting :	None ▼

AP Evaluation Configuration

SM Display of AP Evaluation Data :	○ Disable Display ● Enable Display

Session Timeout

Web, Telnet, FTP Session Timeout :	3600 Seconds

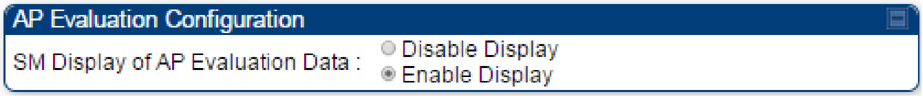
IP Access Filtering

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

Security Mode

Web Access :	HTTP Only ▼
SNMP :	SNMPv2c Only ▼
Telnet :	● Enabled ○ Disabled
FTP :	● Enabled ○ Disabled
TFTP :	● Enabled ○ Disabled

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

	server communication. The default value is *1812*. **Note** This parameter is applicable to BHM.
Authentication Key	The authentication key is a 32-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF. **Note** This parameter is applicable to BHM.
Select Key	This option allows operators to choose which authentication key is used: **Use Key above** means that the key specified in **Authentication Key** is used for authentication **Use Default Key** means that a default key (based off of the SM's MAC address) is used for authentication **Note** This parameter is applicable to BHM.
Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. **None** provides no encryption on the air link. **DES** (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. **AES** (Advanced Encryption Standard)**:** An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A. **Note** This parameter is applicable to BHM.
SM Display of AP Evaluation Data Or BHS Display of BHM Evaluation Data	Allows operators to suppress the display of data about this AP/BHM on the AP/BHM Evaluation tab of the Tools page in all SMs/BHS that register. PMP 450i – SM display of AP Evaluation Data parameter  AP Evaluation Configuration SM Display of AP Evaluation Data : ○ Disable Display ● Enable Display