Cambium Networks™

CONFIGURATION GUIDE

PMP/PTP 450 Series

System Release 16.2

Covers:

PMP 450 AP / PMP 450 SM / PTP 450 / PMP 450d

PMP 450i / PTP 450i

PMP 450b / PTP 450b

PMP 450m

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”). Any “High Risk Use” is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High Risk Use.

Contents

List of Figures

List of Tables

About This User Guide

This guide describes configuration and operation of the Cambium point-to-point and point-to-multipoint wireless Ethernet bridges. It covers PMP/PTP 450, 450i, 450b, 450d and PMP 450m platform Series. It is intended for use by the system designer, system installer and system administrator.

For system configuration, tools and troubleshooting, refer to the following chapters:

- Chapter 1: Configuration
- Chapter 2: :Tools
- Chapter 3: Operation
- Chapter 4: Reference information
- Chapter 5: Troubleshooting

Contacting Cambium Networks

Support website:	https://support.cambiumnetworks.com
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support/Repair enquiries:	https://support.cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/contact
Address:	Cambium Networks Limited, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Purpose

Cambium Networks Point-to-Multi-Point (PMP)/Point-To-Point (PTP) 450 documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium PMP/PTP equipment and ancillary devices of 450 Platform Family. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Product notation conventions in document

This document covers Cambium 450 Series, 450b series, 450i Series and 450m Series products. The following notation conventions are followed while referring to product series and product family:

Product notation	Description
450 Platform Family	Refers to the complete 450 Series family, which includes 450 Series, 450i Series, 450b Series and 450m Series

450 Series	Refers to 450 Series devices in the following configurations:
	- PMP 450
	  - AP [2.4, 3.5, 3.65, 5 GHz]
	  - Connectorized
	  - SM [900 MHz and 2.4, 3.5, 3.65, 5 GHz]
	  - Connectorized/ Integrated
	- PTP 450 BHM/ BHS [900 MHz and 3.5, 3.65, 5 GHz]
	  - Connectorized/ Integrated
	- PMP 450d SM [5 GHz]

450i Series	Refers to 450i Series devices in the following configurations:
	- PMP 450i
	  - AP [900 MHz and 3, 5 GHz]
	  - Connectorized/ Integrated
	  - SM [3 GHz and 5 GHz]
	  - Connectorized/ Integrated
	- PTP 450i BHM/ BHS [3 GHz and 5 GHz]
	  - Connectorized/ Integrated

450b Series	Refers to 450b Series devices in the following configurations:
	- PMP 450b Mid-Gain
	  - SM [5 GHz]
	  - Integrated
	- PMP/PTP 450b High Gain
	  - SM [5 GHz] - Dish

Product notation	Description

450m Series	Refers to 450m Series device configuration:
	- PMP 450m AP 5 GHz
	  - Integrated
	- PMP 450m AP 3 GHz
	  - Integrated

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. To provide feedback, visit our support website.https://support.cambiumnetworks.com.

Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation

Important regulatory information

The 450 Platform Family products are certified as an unlicensed device in frequency bands where it is not allowed to cause interference to licensed services (called primary users of the bands).

Application software

Download the latest 450 Platform Family software and install it in the Outdoor Units (ODUs) before deploying the equipment. Instructions for installing software are provided in Upgrading the software version and using CNUT on page 1-67.

USA specific information

The USA Federal Communications Commission (FCC) requires manufacturers to implement special features to prevent interference to weather radar systems that operate in the band 5600 MHz to 5650 MHz. These features must be implemented in all products able to operate outdoors in the band 5470 MHz to 5725 MHz.

Manufacturers must ensure that such radio products cannot be configured to operate outside of FCC rules; specifically, it must not be possible to disable or modify the radar protection functions that have been demonstrated to the FCC.

Cambium supplies variants of the 5 GHz 450, 450i, 450b, and 450m Series specifically for operation in the USA to comply with FCC requirements (KDB 905462 D02 UNII DFS Compliance Procedures New Rules v02). These variants are only allowed to operate with license keys that comply with FCC rules.

To ensure compliance when using PMP 450 Series and PTP 450 Series, follow the recommendation in Avoidance of weather radars (USA only).

External antennas

When using a connectorized version of the product, the conducted transmit power may need to be reduced to ensure the regulatory limit on transmitter EIRP is not exceeded. The installer must have an understanding of how to compute the effective antenna gain from the actual antenna gain and the feeder cable losses.

The range of permissible values for maximum antenna gain and feeder cable losses are included in this user guide together with a sample calculation. The product GUI automatically applies the correct conducted power limit to ensure that it is not possible for the installation to exceed the EIRP limit, when the appropriate values for antenna gain and feeder cable losses are entered into the GUI.

Avoidance of weather radars (USA only)

To comply with FCC rules (KDB 443999: Interim Plans to Approve UNII Devices Operating in the 5470 - 5725 MHz Band with Radar Detection and DFS Capabilities), units which are installed within 35 km (22 miles) of a Terminal Doppler Weather Radar (TDWR) system (or have a line of sight propagation path to such a system) must be configured to avoid any frequency within +30 MHz or –30 MHz of the frequency of the TDWR device. This requirement applies even if the master is outside the 35 km (22 miles) radius but communicates with outdoor clients which may be within the 35 km (22 miles) radius of the TDWRs. If interference is not eliminated, a distance limitation based on line-of-sight from TDWR will need to be used. Devices with bandwidths greater than 20 MHz may require greater frequency separation.

When planning a link in the USA, visit http://spectrumbridge.com/udia/home.aspx, enter the location of the planned link and search for TDWR radars. If a TDWR system is located within 35 km (22 miles) or has line of sight propagation to the PTP device, perform the following tasks:

- Register the installation on http://spectrumbridge.com/udia/home.aspx.
- Make a list of channel center frequencies that must be barred, that is, those falling within +30 MHz or –30 MHz of the frequency of the TDWR radars.

The 450 Platform Family AP must be configured to not operate on the affected channels.

Canada specific information

Caution

This device complies with ISEDC 's license-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

ISEDC requires manufacturers to implement special features to prevent interference to weather radar systems that operate in the band 5600 MHz to 5650 MHz. These features must be implemented in all products able to operate outdoors in the band 5470 MHz to 5725 MHz.

Manufacturers must ensure that such radio products cannot be configured to operate outside of ISEDC rules; specifically it must not be possible to disable or modify the radar protection functions that have been demonstrated to ISEDC .

In order to comply with these ISEDC requirements, Cambium supplies variants of the 450 Platform Family for operation in Canada. These variants are only allowed to operate with license keys that comply with ISEDC rules. In particular, operation of radio channels overlapping the band 5600 MHz to 5650 MHz is not allowed and these channels are permanently barred.

In addition, other channels may also need to be barred when operating close to weather radar installations.

Other variants of the 450 Platform Family are available for use in the rest of the world, but these variants are not supplied to Canada except under strict controls, when they are needed for export and deployment outside Canada.

Renseignements specifiques au Canada

Attention

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISEDC a demandé aux fabricants de mettre en œuvre des mécanismes spécifiques pour éviter d'interférer avec des systèmes radar fonctionnant dans la bande 5600 MHz à 5650 MHz. Ces mécanismes doivent être mis en œuvre dans tous les produits capables de fonctionner à l'extérieur dans la bande 5470 MHz à 5725 MHz.

Les fabricants doivent s'assurer que les produits de radiocommunications ne peuvent pas être configurés pour fonctionner en dehors des règles ISEDC, en particulier, il ne doit pas être possible de désactiver ou modifier les fonctions de protection des radars qui ont été démontrés à ISEDC.

Afin de se conformer à ces exigences de ISEDC, Cambium fournit des variantes du 450 Platform Family exclusivement pour le Canada. Ces variantes ne permettent pas à l'équipement de fonctionner en dehors des règles de ISEDC. En particulier, le fonctionnement des canaux de radio qui chevauchent la bande 5600-5650 MHz est interdite et ces canaux sont définitivement exclus.

ISEDC Approved Antennas

The list of antennas used to obtain ISEDC approvals is provided in section Country specific radio regulations, Innovation Science and Economic Development Canada (ISEDC) , Table 225.

Antennas externes

Lorsque vous utilisez une version du produit sans antenne intégrée, il peut être nécessaire de réduire la puissance d'émission pour garantir que la limite réglementaire de puissance isotrope rayonnée équivalente (PIRE) n'est pas dépassée. L'installateur doit avoir une bonne compréhension de la façon de calculer le gain de l'antenne réelle et les pertes dans les câbles de connections.

La plage de valeurs admissibles pour un gain maximal de l'antenne et des pertes de câbles de connections sont inclus dans ce guide d'utilisation avec un exemple de calcul. L'interface utilisateur du produit applique automatiquement la limite de puissance menée correct afin de s'assurer qu'il ne soit pas possible pour l'installation de dépasser la limite PIRE, lorsque les valeurs appropriées pour le gain d'antenne et les pertes de câbles d'alimentation sont entrées dans l'interface utilisateur.

Antennes approuvées par ISEDC

La liste des antennas approveés pour l'operation au Canada est founie dans le chapitre Country specific radio regulations, Innovation Science and Economic Development Canada (ISEDC) tableaux Table 225.

EU Declaration of Conformity

Hereby, Cambium Networks declares that the Cambium 450 Series, 450b Series, 450i Series and 450m Series Wireless Ethernet Bridge complies with the essential requirements and other relevant provisions of Radio Equipment Directive 2014/53/EU. The declaration of conformity may be consulted at:

https://www.cambiumnetworks.com/eu_dofc

Specific expertise and training for professional installers

To ensure that the 450 Platform Family products – PMP/PTP 450 Series, PMP/PTP 450i Series, PMP 450m Series are installed and configured in compliance with the requirements of ISEDC and the FCC, installers must have the radio engineering skills and training described in this section.

The Cambium Networks technical training program details can be accessed from below link:

https://www.cambiumnetworks.com/training/

Ethernet networking skills

The installer must have the ability to configure IP addressing on a PC and to set up and control products using a web browser interface.

Lightning protection

To protect outdoor radio installations from the impact of lightning strikes, the installer must be familiar with the normal procedures for site selection, bonding and grounding. Installation guidelines for the 450 Platform Family can be found in Chapter 2: System hardware and Chapter 3: System planning of *450 Platform Planning and Installation Guide*.

Training

The installer needs to have basic competence in radio and IP network installation. The specific requirements applicable to the 450 Platform should be gained by reading:

- Chapter 4: Preparing for installation and Chapter 5: Installation of *450 Platform Planning and Installation Guide*,
- Chapter 1: Configuration, Chapter 2: :Tools, and Chapter 3: Operation of *450 Platform Configuration Guide* (this document),
- And by performing sample set ups at base workshop before live deployments.

The Cambium Networks technical training program details can be accessed from below link:

https://www.cambiumnetworks.com/training/

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1 Search this document and the software release notes of supported releases.

2 Visit the support website.

3 Ask for assistance from the Cambium product supplier.

4 Gather information from affected units, such as any available diagnostic downloads.

5 Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website (http://www.cambiumnetworks.com/support).

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register PMP and PTP products or activate warranties, visit the support website. For warranty assistance, contact the reseller or distributor. The removal of the tamper-evident seal will void the warranty.

Caution

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

Warning

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

Caution

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

Note

Note text.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.

Disposal of Cambium equipment

European Union (EU) Directive 2012/19/EU Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to https://www.cambiumnetworks.com/support/compliance/

Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Chapter 1: Configuration

This chapter describes how to use the web interface to configure the 450 Platform 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 Legal and Open Sources Guide, 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 chapter Compliance with radio regulations in Legal and Open Sources Guide.

Connecting to the unit

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

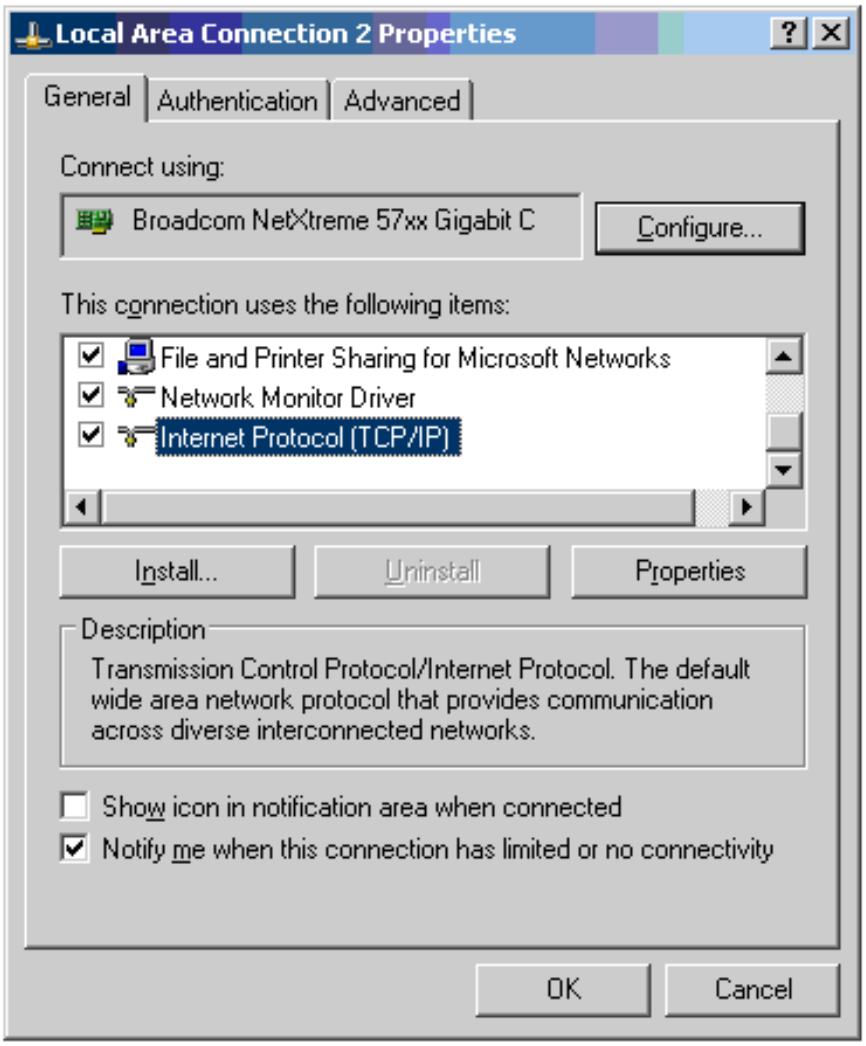
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the 450 Platform ODU.

Procedure 1 Configuring the management PC

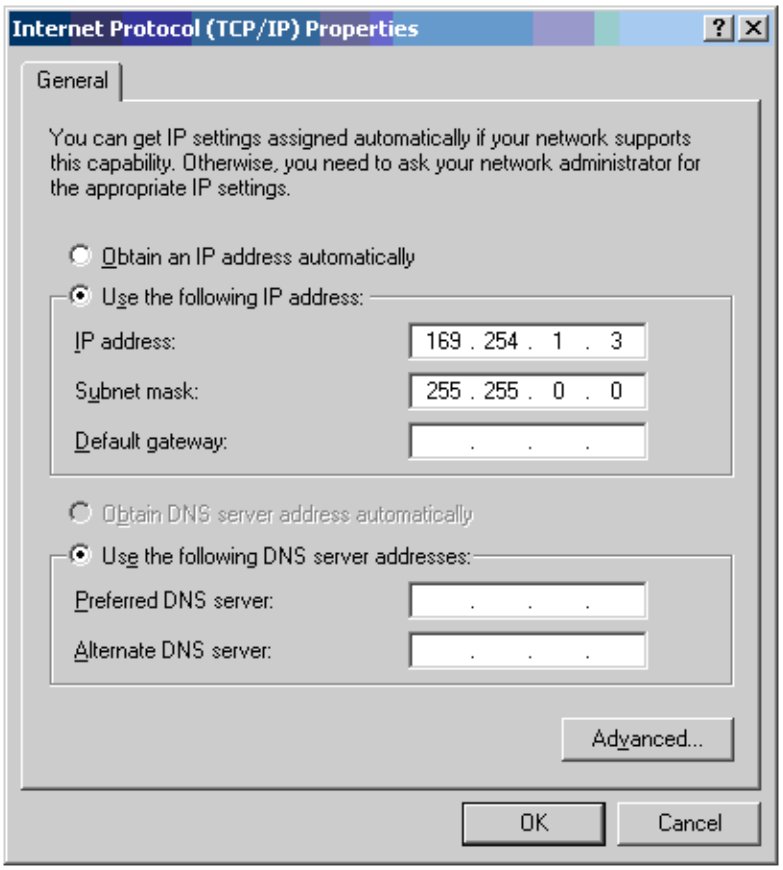
1 Select **Properties** for the Ethernet port. In Windows 7 this is found in **Control Panel > Network and Internet > Network Connections > Local Area Connection**.

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



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:



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 450 platform ODU.

Procedure 2 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 450 Platform Family web interface and use its menus.

Logging into the web interface

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

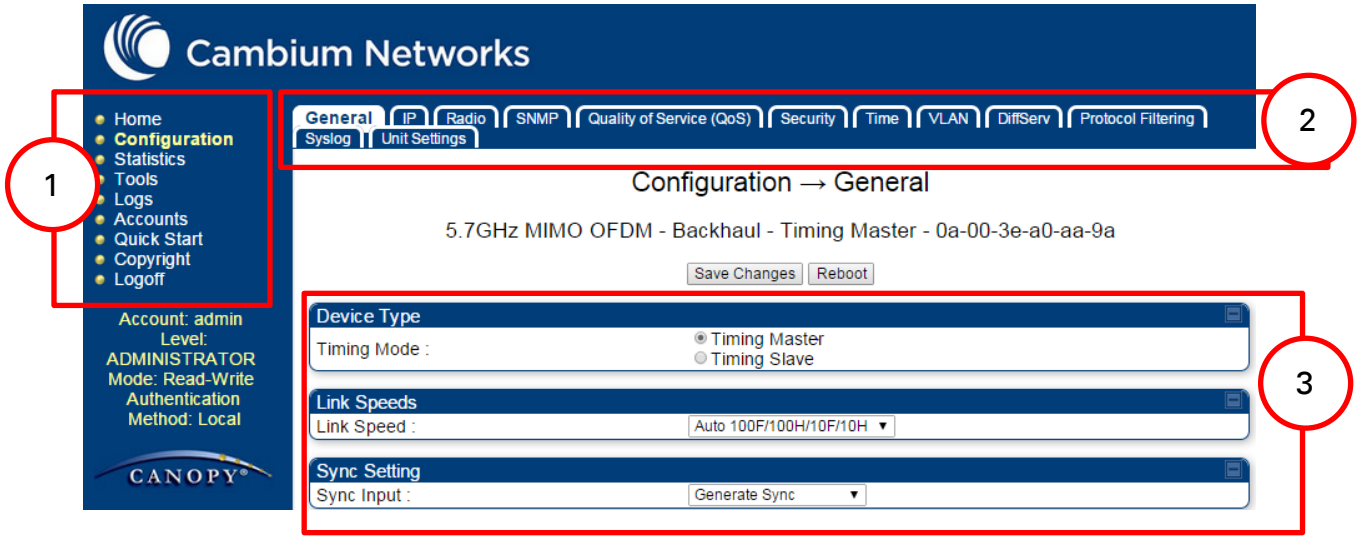
Procedure 3 Logging into the web interface

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:

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

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

Web GUI



Field Name	Description
Main Menu	Click an option in side navigation bar (area marked as “1”). Multiple options in sub-navigation bars appear
Menu Options	Click top sub-navigation bar to choose one configuration page (area marked as “2”)
Parameters	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 1 to locate information about using each web page.

Table 1 Menu options and web pages

Main menu	Menu options	Applicable module	Description
Home			
	General Status	All	Viewing General Status on page 3-2
	Session Status	AP, BHM	Viewing Session Status on page 3-24
	Event Log	All	Interpreting messages in the Event Log on page 3-35
	Network Interface	All	Viewing the Network Interface on page 3-38
	Layer 2 Neighbors	All	Viewing the Layer 2 Neighbors on page 3-38
Configuration			
	General	All	General configuration on page 1-71
	IP	All	Configuring IP and Ethernet interfaces on page 1-23
	Radio	All	Configuring radio parameters on page 1-145.
	SNMP	All	Setting up SNMP agent on page 1-218
	cnMaestro	All	Configuring cnMaestroTM Connectivity on page 1-270
	Quality of Service (QoS)	All	Configuring quality of service on page 1-236
	Security	All	Configuring security on page 1-109
	Time	AP, BHM	Setting up time and date Time page of 450 Platform Family - AP/BHM on page 1-103

Main menu	Menu options	Applicable module	Description
	VLAN	All	VLAN configuration for PMP on page 1-45 VLAN configuration for PTP on page 1-56
	DiffServ	All	IPv4 and IPv6 Prioritization on page 1-62
	Protocol Filtering	All	Filtering protocols and ports on page 1-63
	Syslog	All	Configuring syslog on page 1-227
	Ping Watchdog	All	Configuring Ping Watchdog on page 1-315
	Unit Setting	All	Configuring Unit Settings page on page 1-99
Statistics			
	Scheduler	All	Viewing the Scheduler statistics on page 3-39
	Registration Failures	AP, BHM	Viewing list of Registration Failures statistics on page 3-41
	Bridge Control Block	All	Interpreting Bridge Control Block statistics on page 3-72
	Bridging Table	All	Interpreting Bridging Table statistics on page 3-43
	Ethernet	All	Interpreting Ethernet statistics on page 3-44
	Radio	All	Interpreting RF Control Block statistics on page 3-47
	VLAN	All	Interpreting VLAN statistics on page 3-51
	Data Channels	All	Interpreting Data Channels statistics on page 3-52
	MIR/Burst	AP, SM	Interpreting MIR/Burst statistics on page 9-6
	Throughput	AP, BHM	Interpreting Throughput statistics on page 3-58

Main menu	Menu options	Applicable module	Description
	Filter	All	Interpreting Filter statistics on page 3-65
	ARP	All	Viewing ARP statistics on page 3-66
	Overload	All	Interpreting Overload statistics on page 3-61
	Syslog Statistics	All	Interpreting syslog statistics on page 3-78
	Translation Table	SM	Interpreting Translation Table statistics on page 3-43
	DHCP Relay	AP	Interpreting DHCP Relay statistics on page 3-63
	NAT Stats	SM	Viewing NAT statistics on page 3-66
	NAT DHCP	SM	Viewing NAT DHCP Statistics on page 3-68
	Pass Through Statistics	AP	Interpreting Pass Through Statistics on page 3-75
	Sync Status	AP	Interpreting Sync Status statistics on page 3-69
	PPPoE	SM	Interpreting PPPoE Statistics for Customer Activities on page 3-70
	SNMPv3 Statistics	All	Interpreting SNMPv3 Statistics on page 3-76
	Frame Utilization	AP, BH	Interpreting Frame Utilization statistics on page 3-76
Tools			
	Link Capacity Test	All	Using the Link Capacity Test tool on page 2-338
	Spectrum Analyzer	All	Spectrum Analyzer tool on page 2-318
	Remote Spectrum Analyzer	All	Remote Spectrum Analyzer tool on page 2-328
	AP/BHM Evaluation	SM, BHS	Using AP Evaluation tool on page 2-347 Using BHM Evaluation tool on page 2-352

Main menu	Menu options	Applicable module	Description
	Subscriber Configuration	AP	Using the Subscriber Configuration tool on page 2-360
	OFDM Frame Calculator	All	Using the OFDM Frame Calculator tool on page 2-356
	BER results	SM, BHS	Using BER Results tool on page 2-369
	Alignment Tool	SM, BHS	Using the Alignment Tool on page 2-331
	Link Status	All	Using the Link Status tool on page 2-361
	Sessions	AP, BHM	Using the Sessions tool on page 2-370
	Ping Test	All	Using the Ping Test tool on page 2-371
Logs			
Accounts			
	Change User Setting	All	Changing a User Setting on page 1-111
	Add user	All	Adding a User for Access to a module on page 1-110
	Delete User	All	Deleting a User from Access to a module on page 1-111
	User	All	Users account on page 1-112
Quick Start			
	Quick Start	AP, BHM	Quick link setup on page 1-13
	Region Settings	AP, BHM	Quick link setup on page 1-13
	Radio Carrier Frequency	AP, BHM	Quick link setup on page 1-13
	Synchronization	AP, BHM	Quick link setup on page 1-13
	LAN IP Address	AP, BHM	Quick link setup on page 1-13
	Review and Save Configuration	AP, BHM	Quick link setup on page 1-13
PDA			
	Quick Status	SM	
	Spectrum Results (PDA)	SM	

Main menu	Menu options	Applicable module	Description
	Information	SM	The PDA web-page includes 320 x 240 pixel formatted displays of information important to installation 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

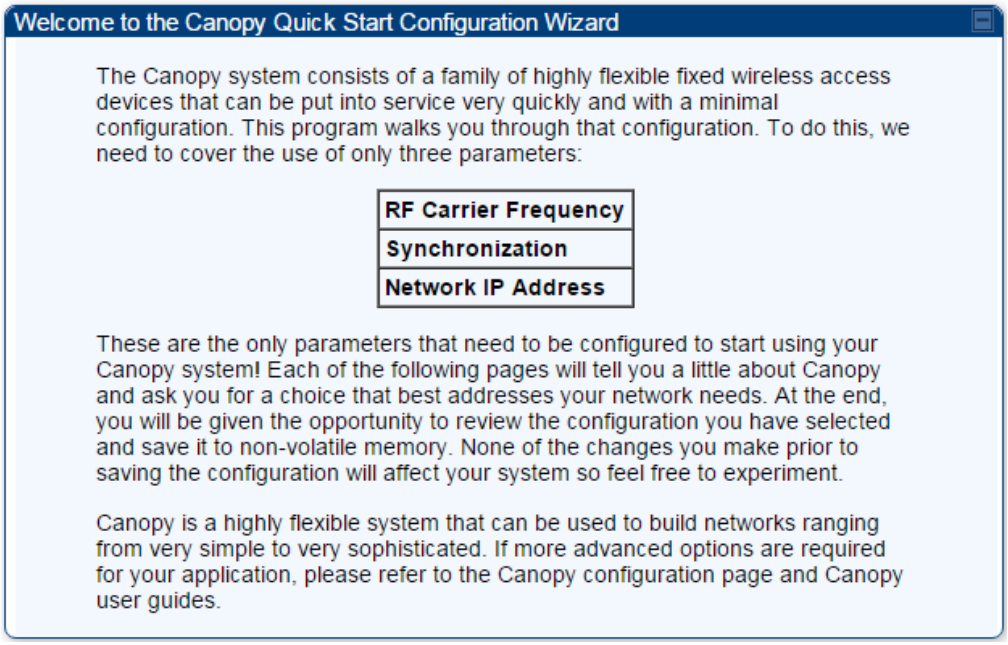
This section describes how to use the Quick Start Wizard to complete the essential system configuration tasks that must be performed on a PMP/PTP configuration.

Initiating Quick Start Wizard

Applicable 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 1 Disarm Installation page (top and bottom of page shown)



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

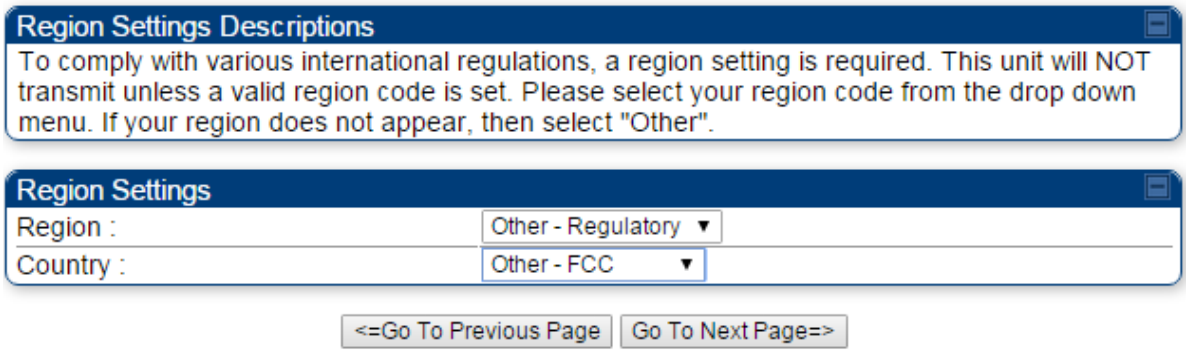
- specify the settings to satisfy the requirements of the network.
- review the configuration selected.
- save the configuration to non-volatile memory.

Procedure 4 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.

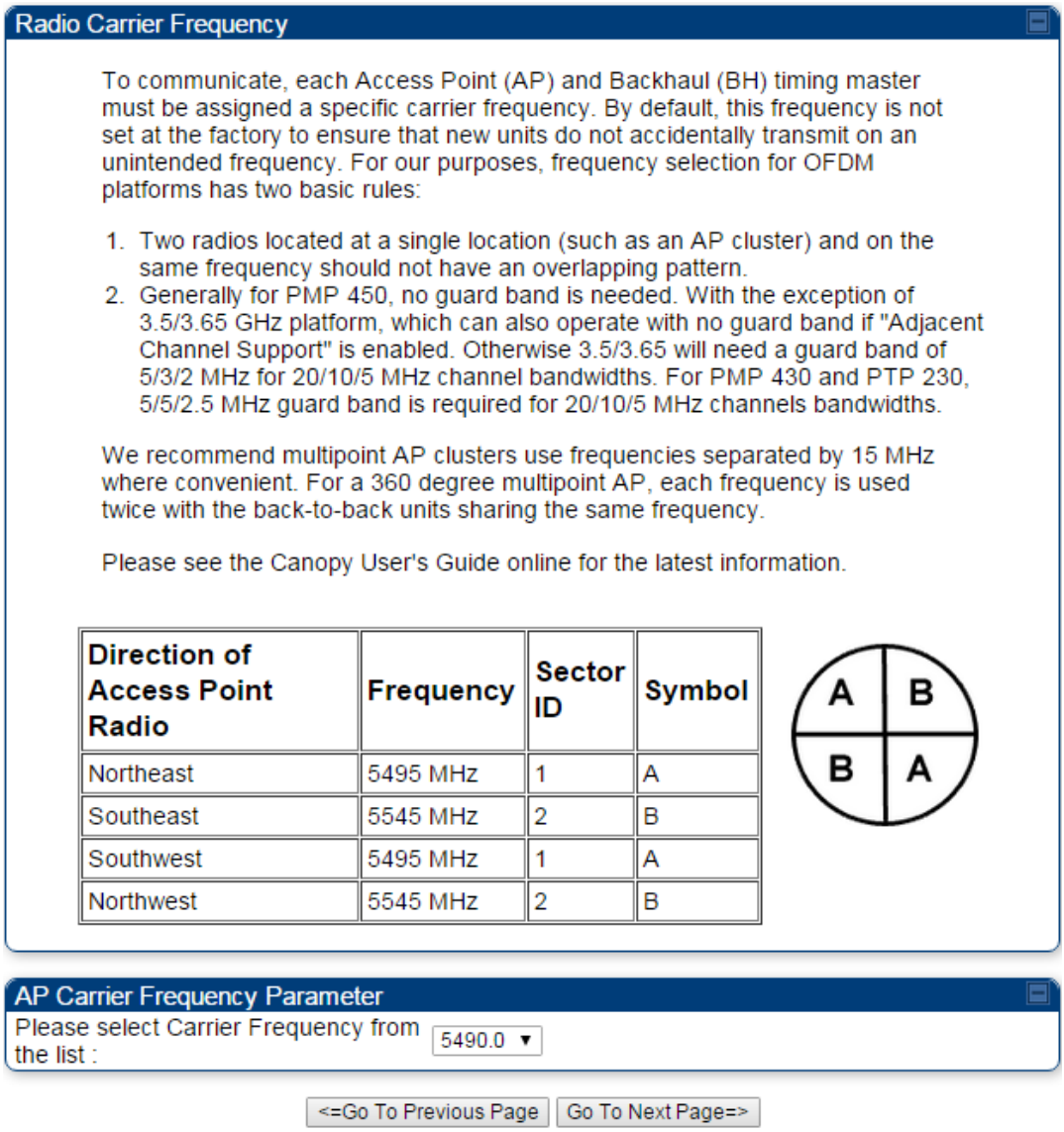
Figure 2 Regional Settings tab of AP/BHM



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

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

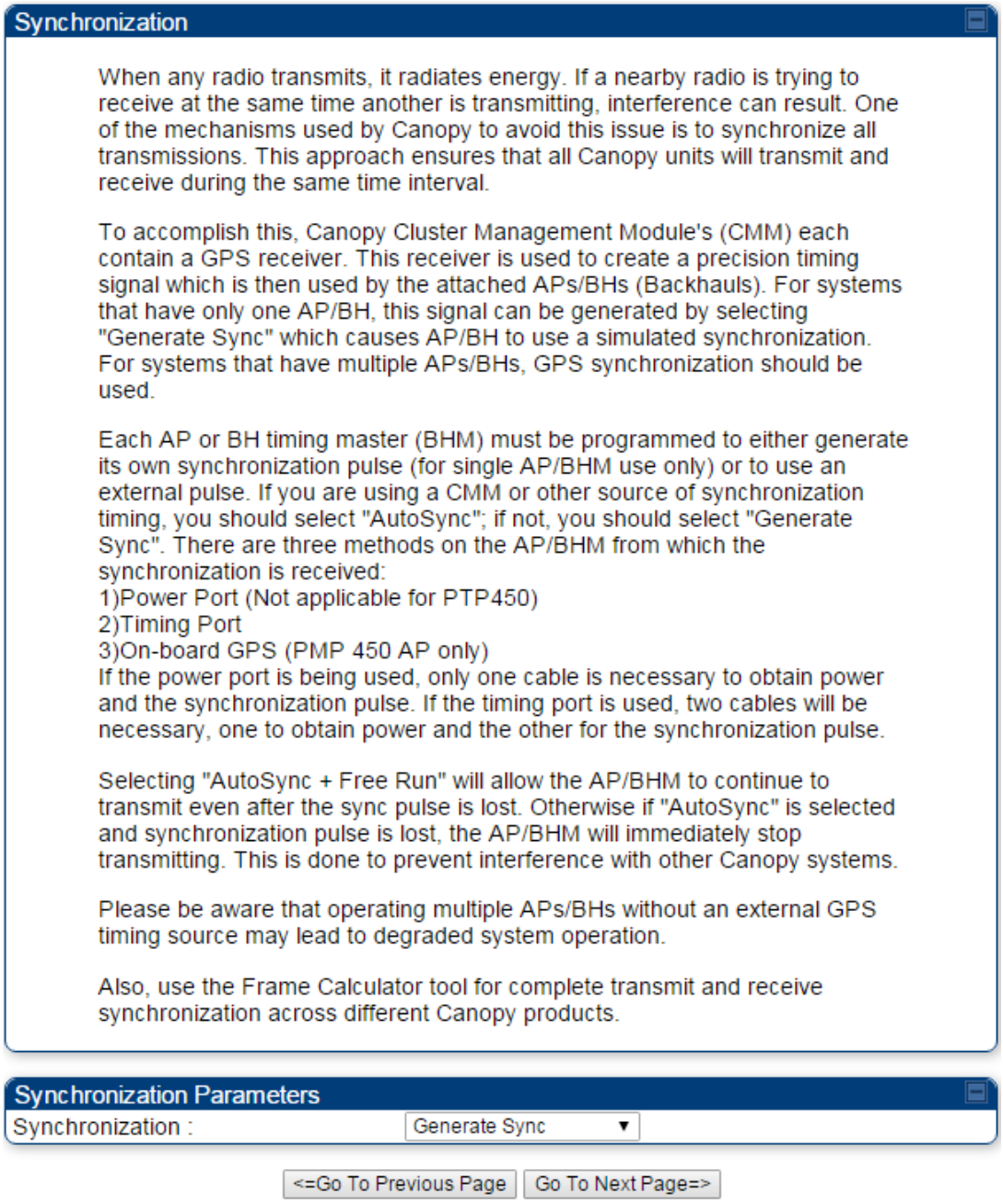
Figure 3 Radio Carrier Frequency tab of AP/BHM



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

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

Figure 4 Synchronization tab of AP/BHM

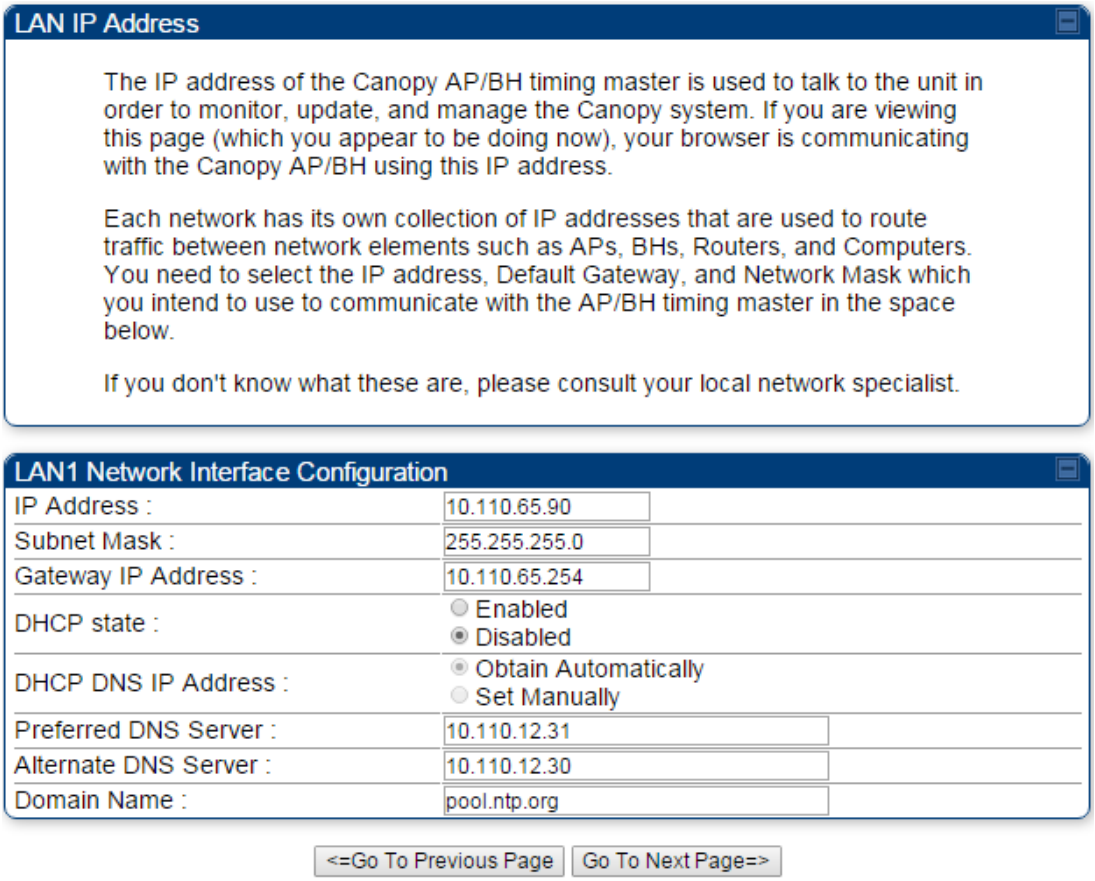


7 Click the **Go To Next Page** button.

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 5 LAN IP Address tab of the AP/BHM



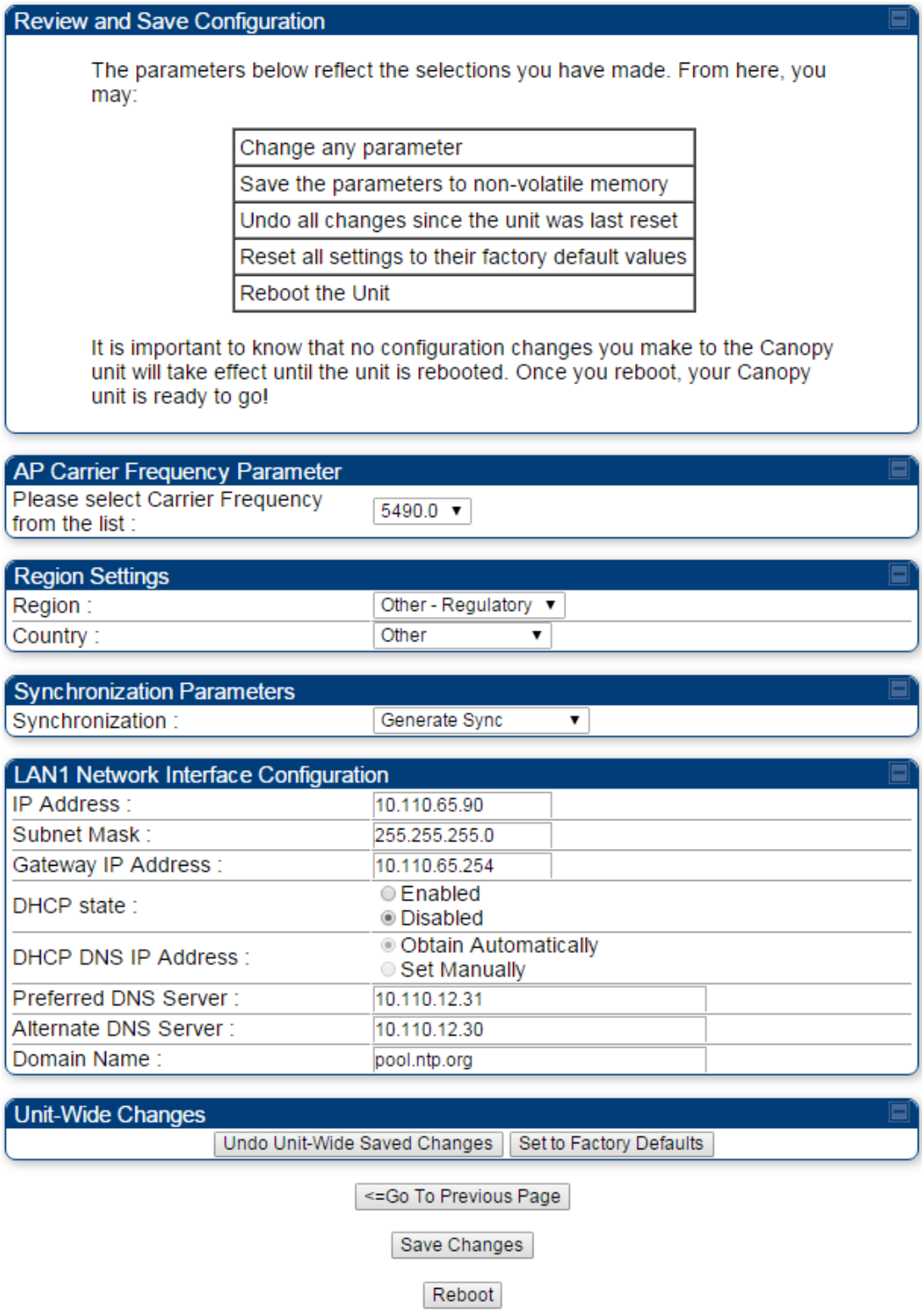
Note

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 6 Review and Save Configuration tab of the AP/BHM



11 Click **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.

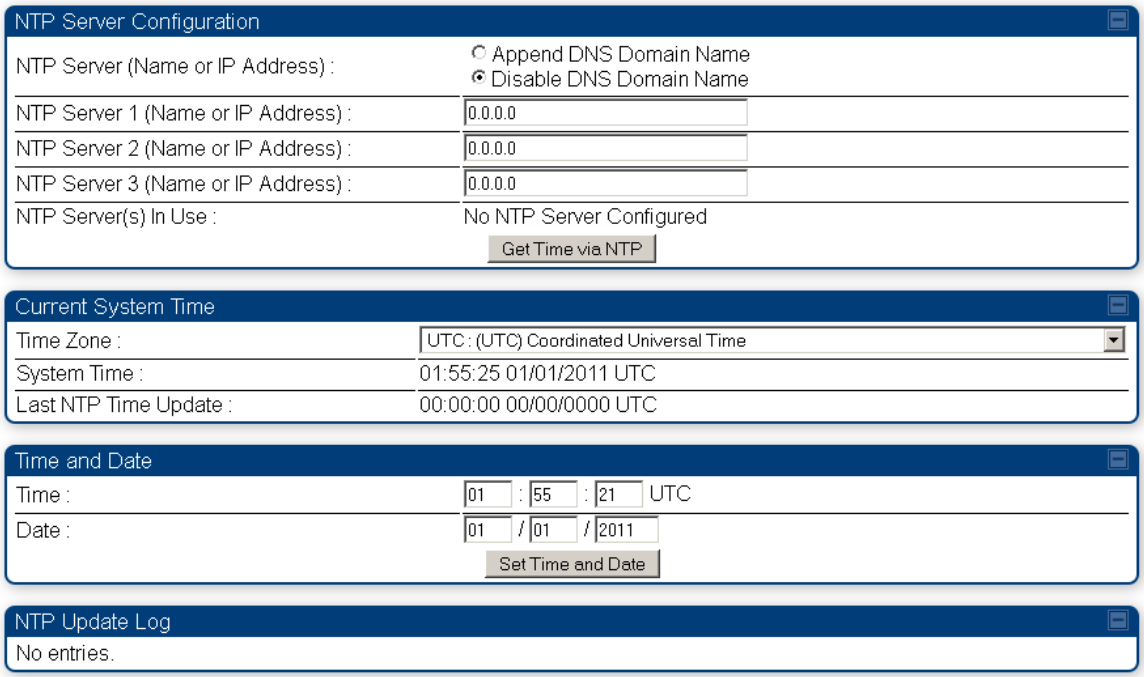
15 Wait until the red indicator LEDs are not lit.

Configuring time settings

Applicable 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 7 Time tab of the AP/BHM



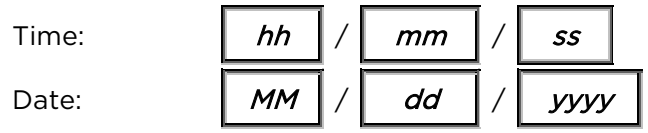
To have each log in the AP/BHM correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP/BHM or you must set the time and date whenever a power cycle of the AP/BHM has occurred. A network element passes time and date in any of the following scenarios:

- 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 8 Time and date entry formats



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 5 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 device is set to automatically refresh

Powering the SM/BHS for test

Procedure 6 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 CAT5 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 in chapter 11.

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.

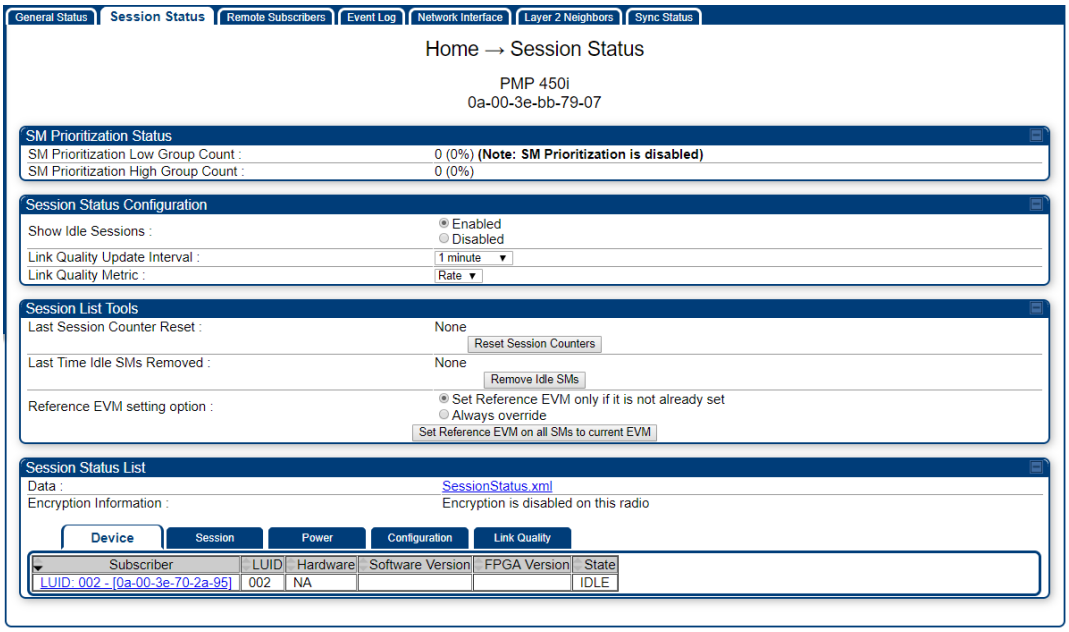
Idle subscribers may be included or removed from the session status display by enabling or disabling, respectively, the **Show Idle Sessions** parameter. Enabling or disabling this parameter only affects the GUI display of subscribers, not the registration status.

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 7 Viewing the AP Session Status page

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

Figure 9 Session Status tab of AP



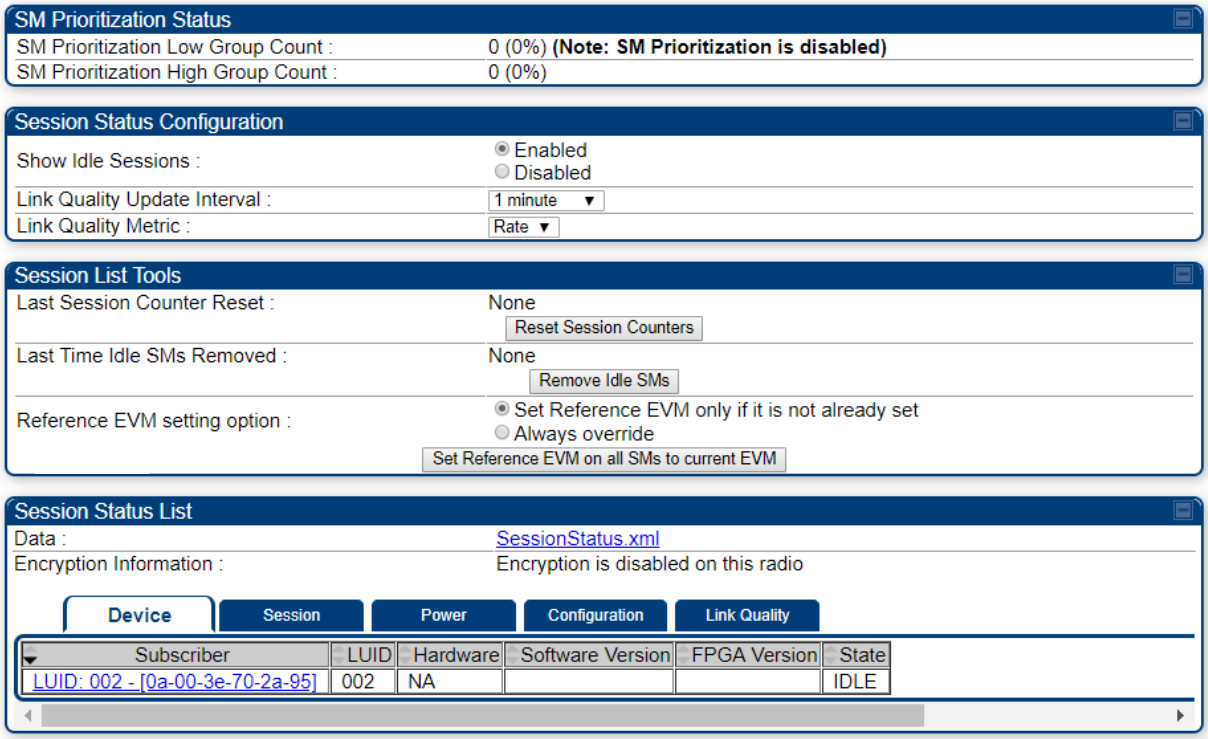
Note

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 2.

Table 2 Session Status Attributes – AP



Attribute	Meaning
Show Idle Sessions	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.
Last Session Counter Reset	This field displays date and time stamp of last session counter reset.
Reference EVM setting option	Option to configure reference EVM for all connected SMs.
Last Time Idle SMs Removed	This field displays date and time stamp of last Idle SMs Removed. On click of “Remove Idle SMs” button, all the SMs which are in Idle state are flushed out.
Data	See Exporting Session Status page of AP/BHM on page 1-259
Device tab	See Device tab on page 3-24
Session tab	See Session tab on page 3-26
Power tab	See Power tab on page 3-27
Configuration tab	See Configuration tab on page 3-30
Link Quality	See Link Quality tab on page 3-33

Configuring IP and Ethernet interfaces

This task consists of the following sections:

Configuring the IP interface

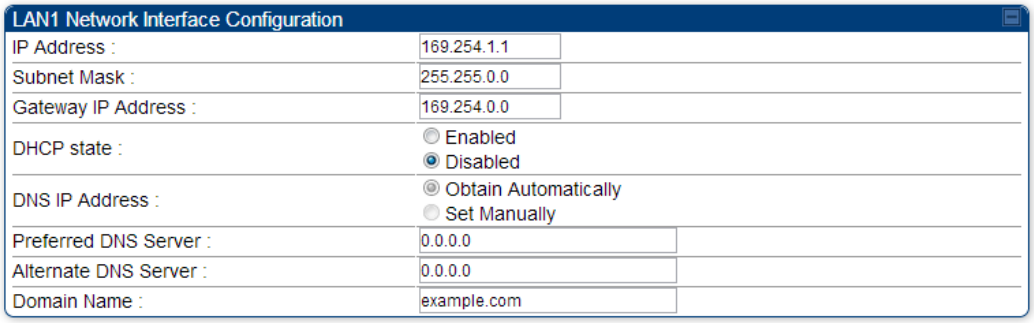
The IP interface allows users to connect to the 450 Platform Family web interface, either from a locally connected computer or from a management network.

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

To configure the IP interface, follow these instructions:

Procedure 8 Configuring the AP/BHM IP interface

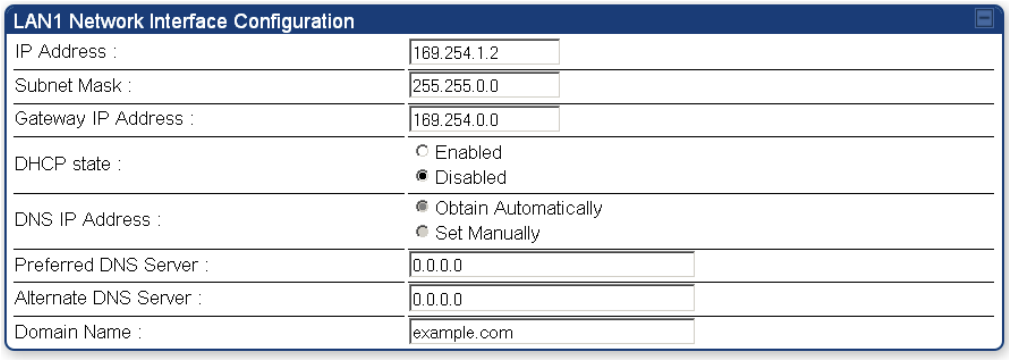
1 Select menu option **Configuration** > **IP**. The LAN configuration page is displayed:



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 3 IP interface attributes).

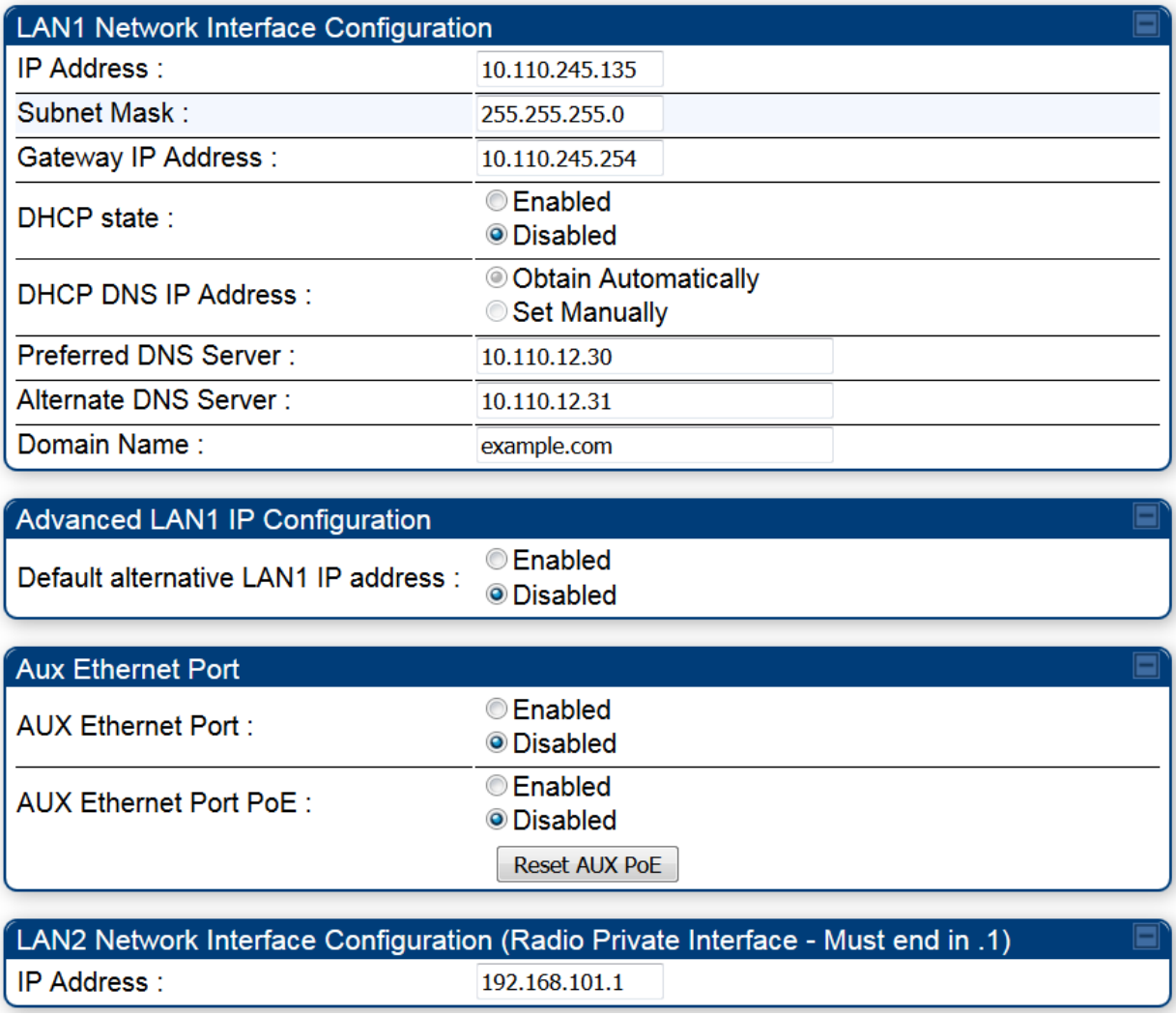
4 Click **Save**. “Reboot Required” message is displayed:



5 Click **Reboot** button.

The IP page of AP/SM/BHM/BHS is explained in Table 3.

Table 3 IP interface attributes



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.
Gateway IP Address	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.
Advanced LAN1 IP Configuration – Default alternate LAN1 IP address	Hardcoded default alternate IP address (169.254.1.1) that is available only when connected to the Ethernet port. When enabled, user can configure a second IP address for the bridge which is other than the hardcoded IP address (169.254.1.1).
AUX Ethernet Port – AUX Ethernet Port	Enabled: Data is enabled for Auxiliary port Disabled: Data is disabled for Auxiliary port
AUX Ethernet Port – AUX Ethernet Port PoE	Enabled: PoE out is enable for Auxiliary port Disabled: PoE out is disabled for Auxiliary port
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 4 SM/BHS private IP and LUID

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

Auxiliary port

An additional Ethernet port labeled “Aux” for Auxiliary port is implemented for downstream traffic. This feature is supported only for PTP/PMP 450i ODUs.

To enable the Aux port, follow these instructions:

Procedure 9 Enabling Aux port interface

1 Select menu option **Configuration > IP > Aux Network Interface** tab.:

2 Click Enable button of Aux Ethernet Port parameter to enable Aux Ethernet port

3 Click Enable button of Aux Ethernet Port PoE parameter to enable Aux port PoE out.

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

5 Click **Reboot**.

Table 5 Aux port attributes

Attribute	Meaning
Aux Ethernet Port	Enabled: Data is enabled for Auxiliary port Disabled: Data is disabled for Auxiliary port
Aux Ethernet Port PoE	Enabled: PoE out is enable for Auxiliary port Disabled: PoE out is disabled for Auxiliary port

By disabling this feature, the data at the Auxiliary port will be disabled.

NAT, DHCP Server, DHCP Client and DMZ

Applicable 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

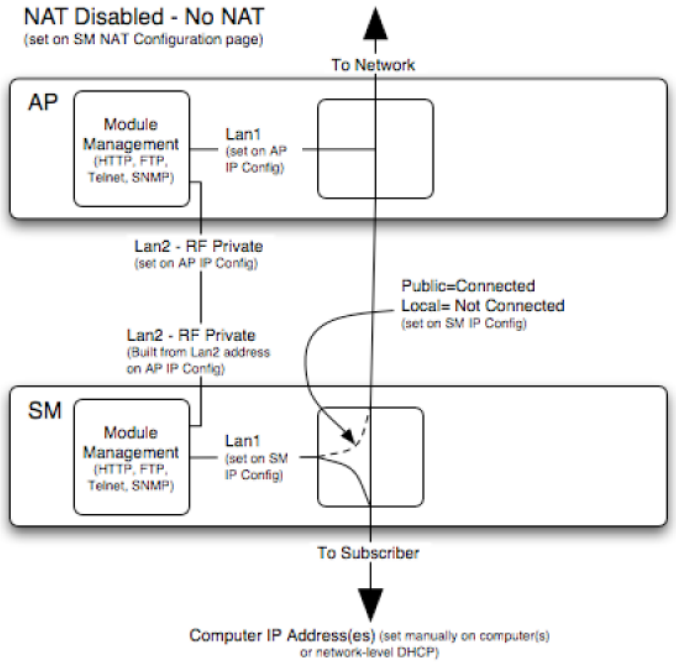
In conjunction with the NAT features, a DMZ (Demilitarized Zone) allows the allotment of one IP address behind the SM for a device to logically exist outside the firewall and receive network traffic. The first three octets of this IP address must be identical to the first three octets of the NAT private 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 10.

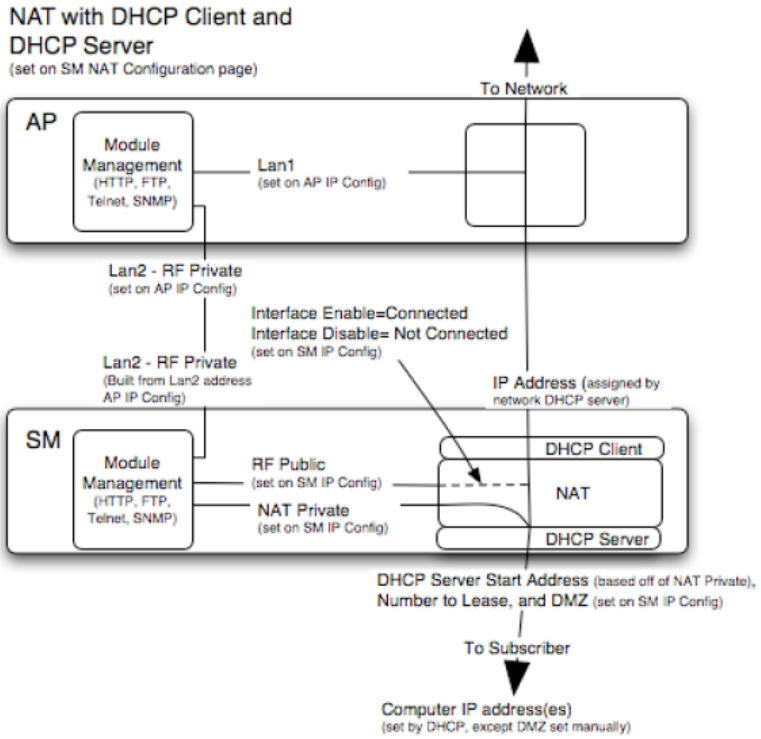
Figure 10 NAT disabled implementation



NAT with DHCP Client and DHCP Server

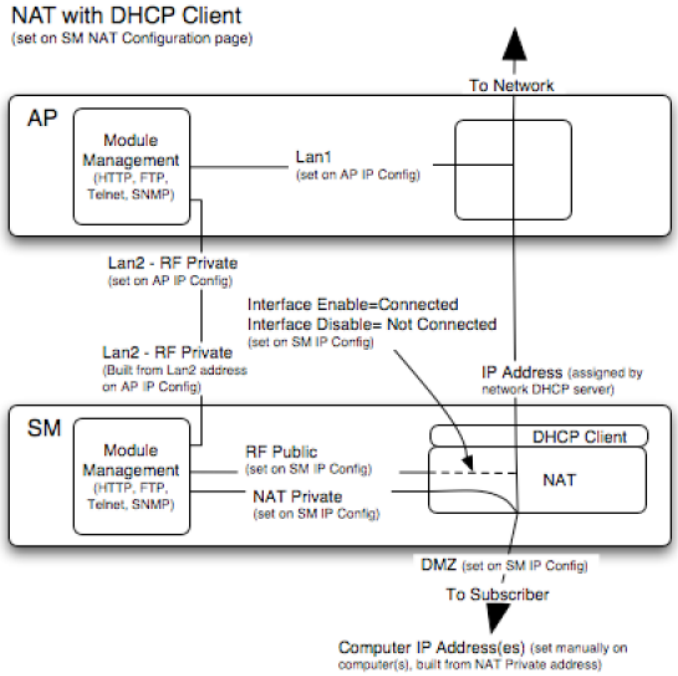
The NAT with DHCP Client and DHCP server is illustrated in Figure 11.

Figure 11 NAT with DHCP client and DHCP server implementation



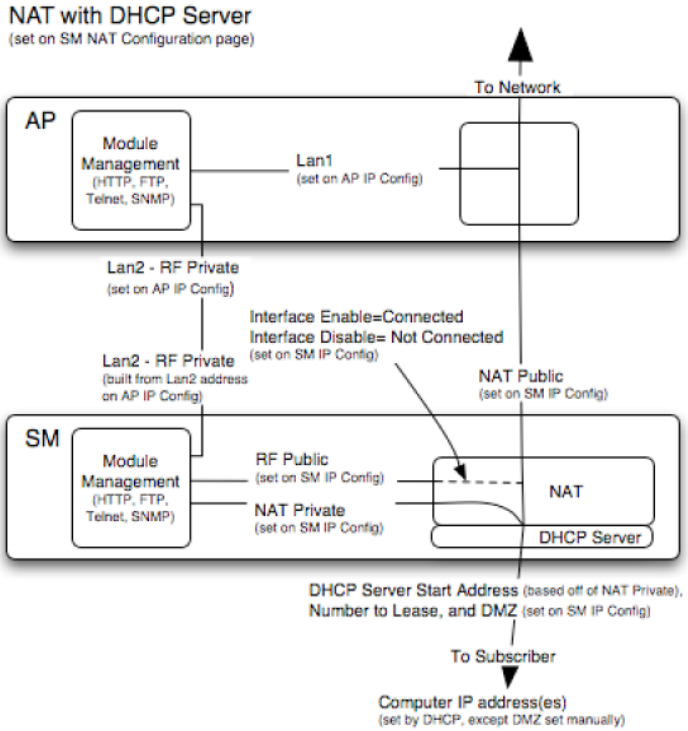
NAT with DHCP Client

Figure 12 NAT with DHCP client implementation



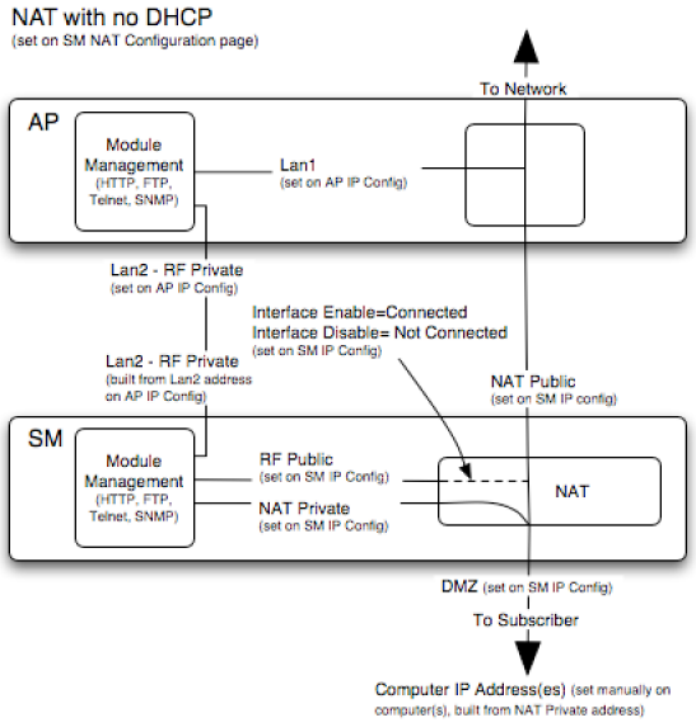
NAT with DHCP Server

Figure 13 NAT with DHCP server implementation



NAT without DHCP

Figure 14 NAT without DHCP implementation



NAT and VPNs

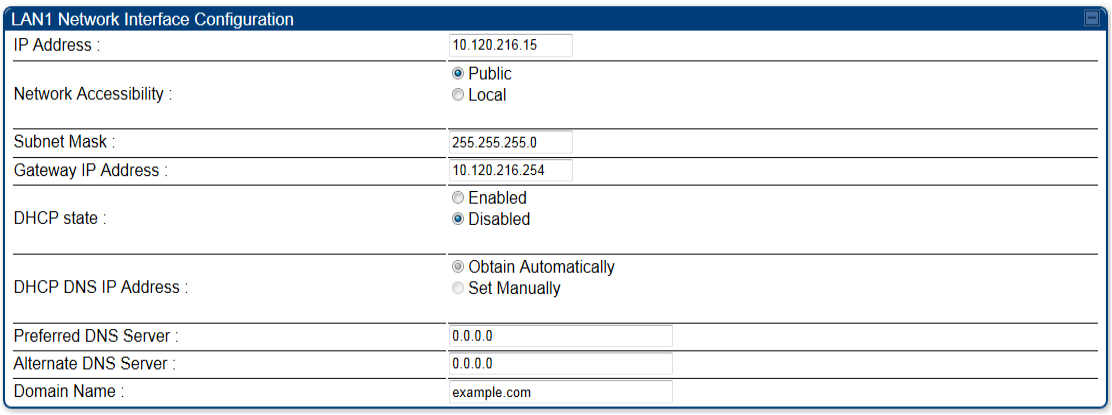
VPN technology provides the benefits of a private network during communication over a public network. One typical use of a VPN is to connect employees remotely (who are at home or in a different city), with their corporate network through a public Internet. Any of several VPN implementation schemes is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

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

IP interface with NAT disabled - SM

The IP page of SM with NAT disabled is explained in Table 6.

Table 6 IP attributes - SM with NAT disabled



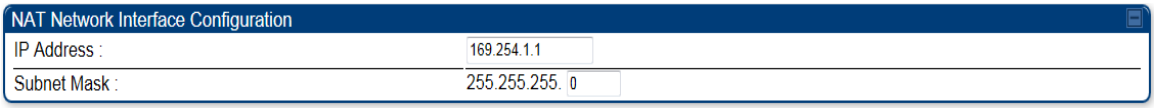
Attribute	Meaning
IP Address	Enter the non-routable IP address to associate with the Ethernet connection on this SM. (The default IP address from the factory is 169.254.1.1.) If you forget this parameter, you must both: • physically access the module. • use recovery mode to access the module configuration parameters at 169.254.1.1. **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 7.

Table 7 IP attributes - SM with NAT enabled

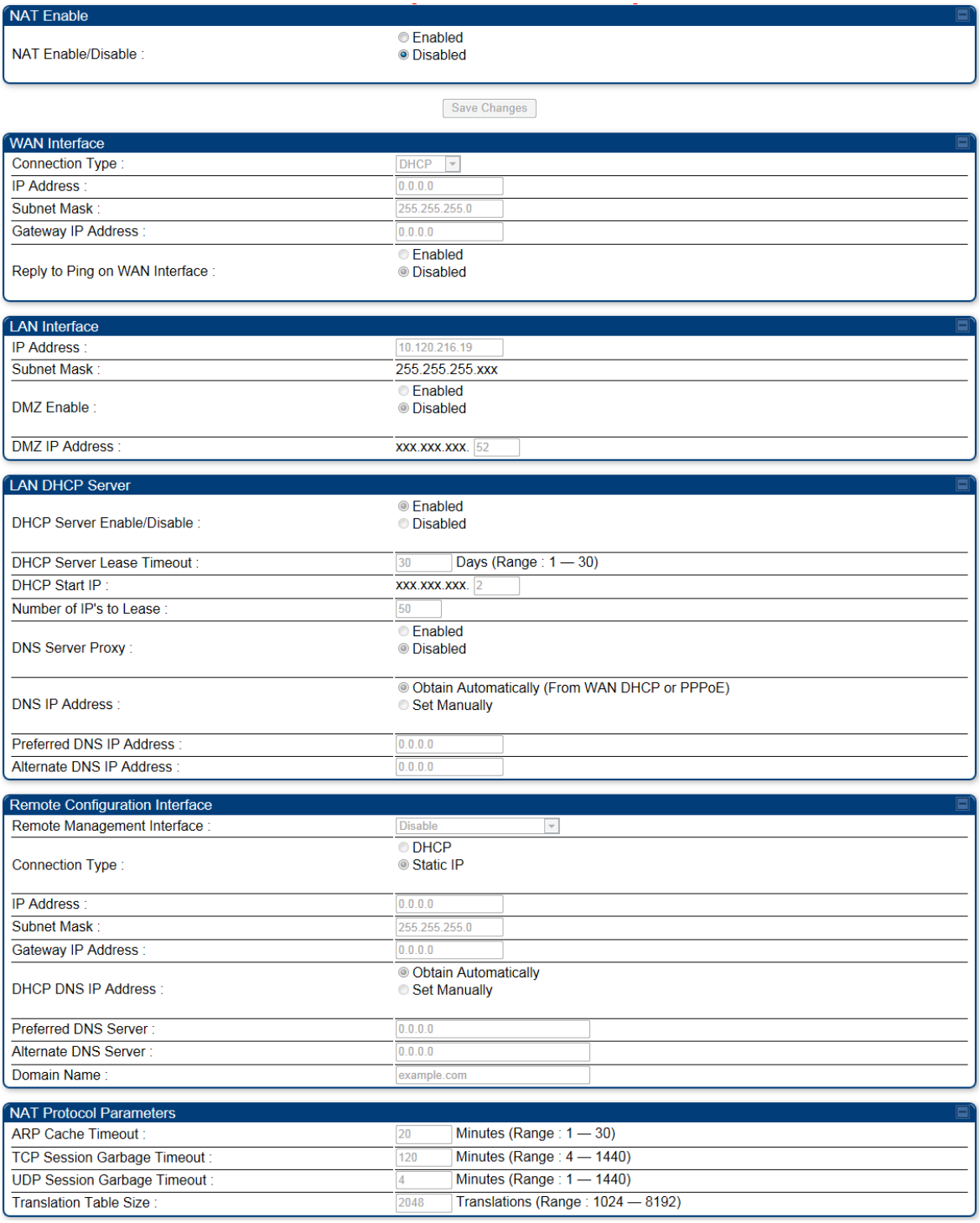


Attribute	Meaning
IP Address	Assign an IP address for SM/BHS management through Ethernet access to the SM/BHS. Set only the first three bytes. The last byte is permanently set to 1. This address becomes the base for the range of DHCP-assigned addresses.
Subnet Mask	Assign a subnet mask of 255.255.255.0 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 8.

Table 8 NAT attributes - SM with NAT disabled



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 configurable:

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

LAN Interface > IP Address

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

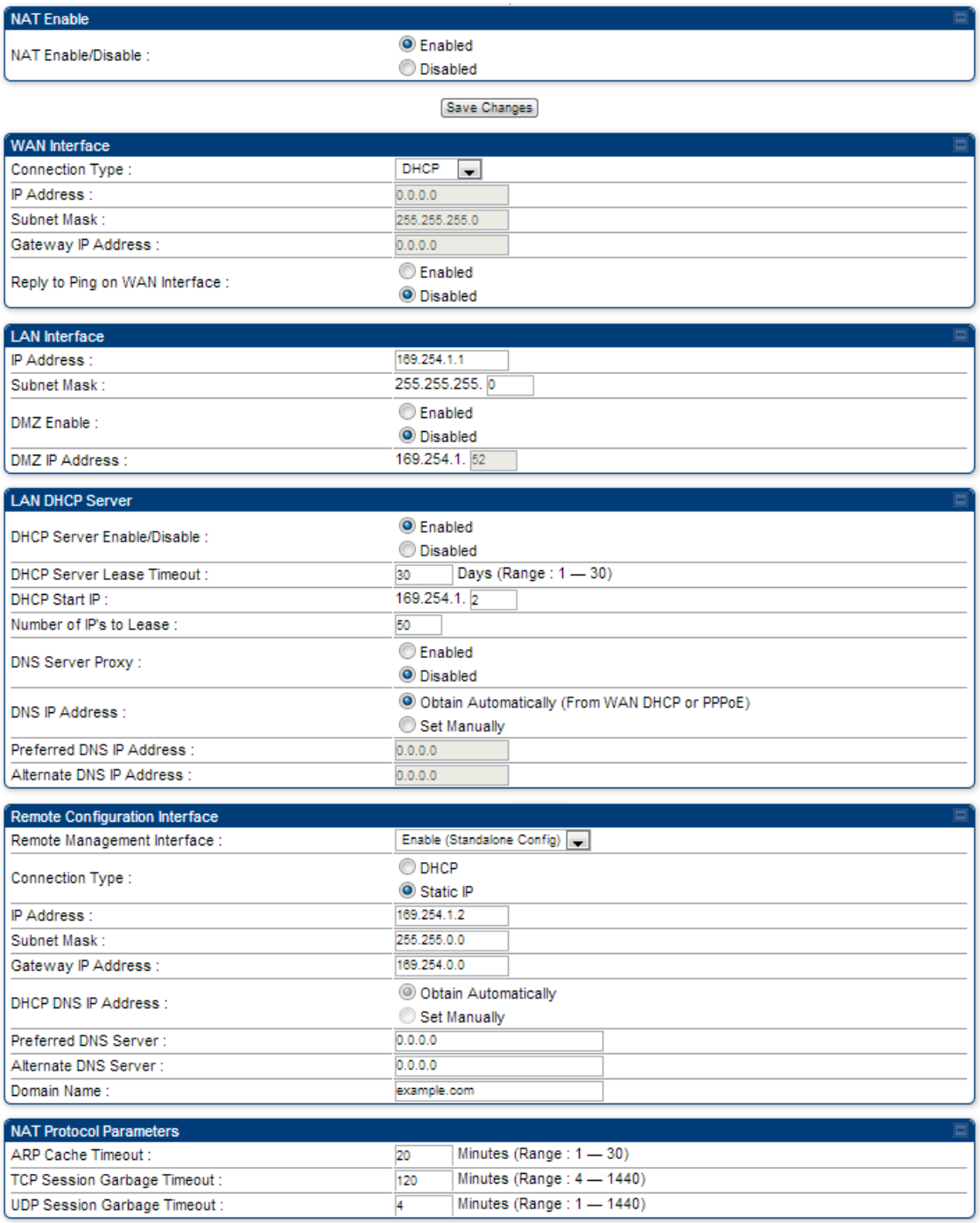
Remote Management Interface > Remote Management Interface, IP address, Subnet Mask, DHCP DNS IP Address, Preferred DNS Server, Alternate DNS Server, Domain Name

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

NAT tab with NAT enabled - SM

The NAT tab of SM with NAT enabled is explained in Table 9.

Table 9 NAT attributes - SM with NAT enabled



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 Address	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.
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 are 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.

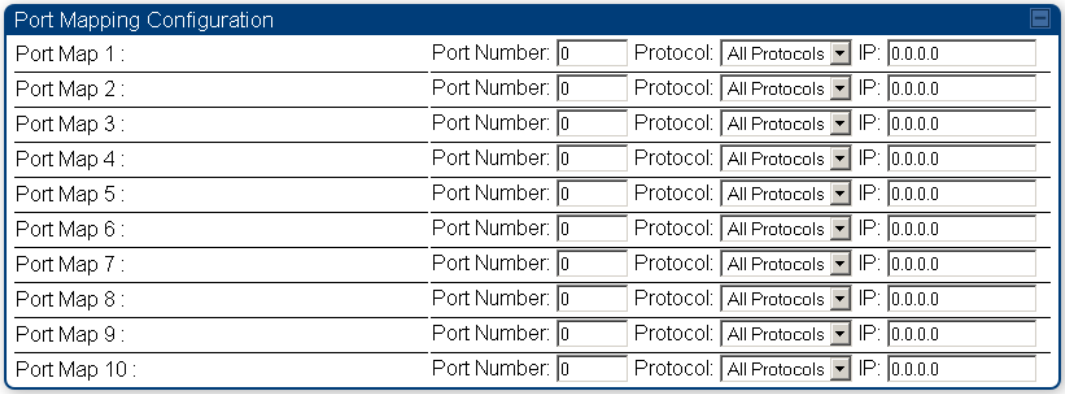
Table 10 SM DNS Options with NAT Enabled

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 11.

Table 11 NAT Port Mapping attributes - SM



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

DHCP – BHS

Applicable products	PTP: ☑ BHM

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

In conjunction with the NAT features, each BHS provides:

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

Reconnecting to the management PC

If the IP Address, Subnet Mask and Gateway IP Address of the unit have been updated to meet network requirements, then reconfigure the local management PC to use an IP address that is valid for the network. See Configuring the management PC on page 1-4.

Once the unit reboots, log in using the new IP address. See Logging into the web interface on page 1-6.

VLAN configuration for PMP

Applicable products	**PMP:** ☑ AP ☑ SM

VLAN Remarking

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

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

Note

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

VLAN ID Remarking

SM supports the ability to re-mark the VLAN ID on both upstream and downstream VLAN frames at the Ethernet interface. For instance, a configuration can be added to re-mark VLAN ID ‘x’ to VLAN ID ‘y’ as shown in Table 12. AP does not support VLAN ID remarking.

Table 12 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 VIDs
- 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.

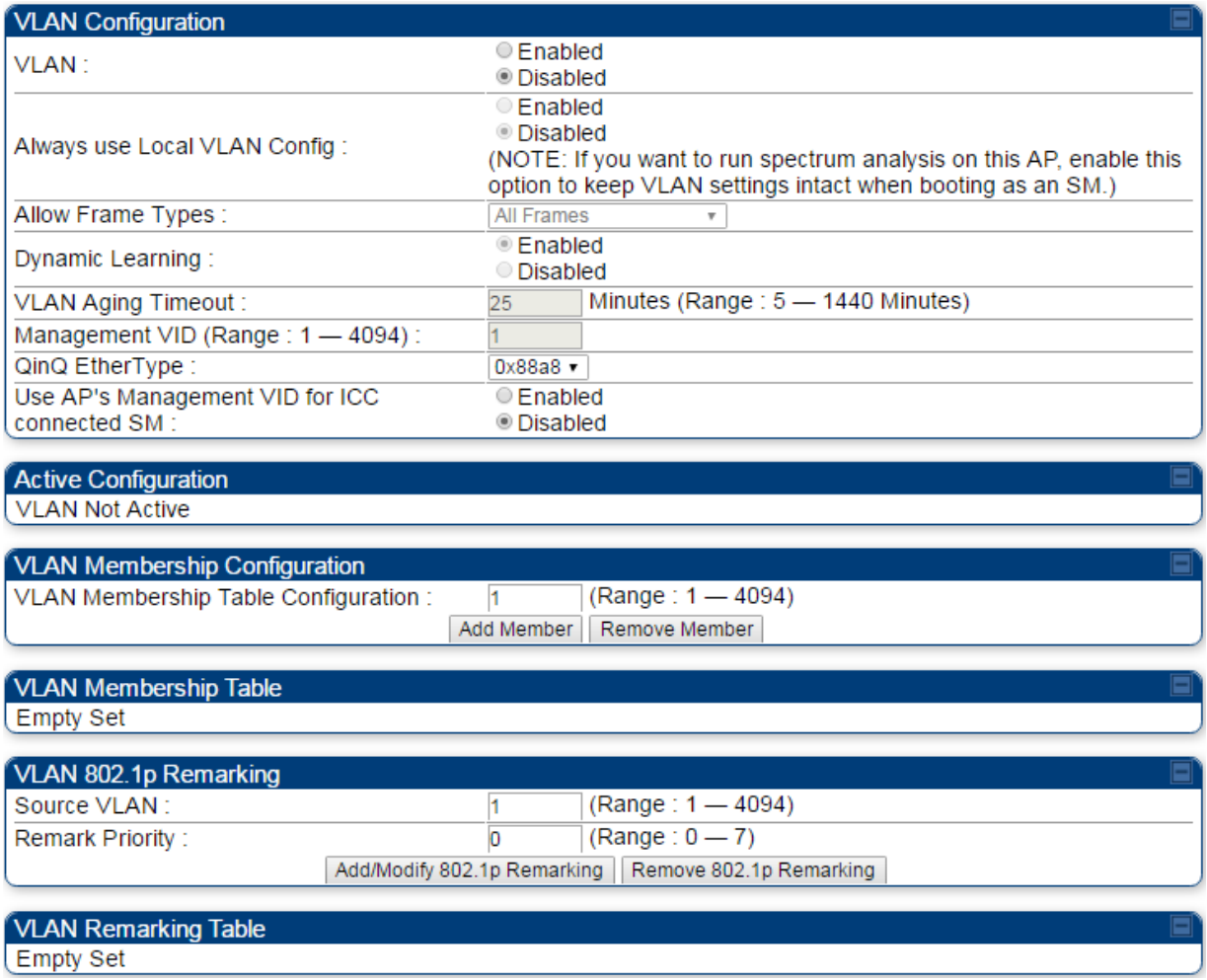
Use AP's Management VID for ICC connected SM

This feature allows the SM to use the AP's management VLAN ID when the SM is registered to the AP via ICC. This feature is useful for the customer who uses a different management VID for the SM and AP and Zero Touch feature is enabled for configuration. This parameter may be accessed via the **Configuration > VLAN** page on the AP's web management interface.

VLAN page of AP

The **VLAN** tab of the AP/BHM is explained in Table 13.

Table 13 AP/BHM VLAN tab attributes



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

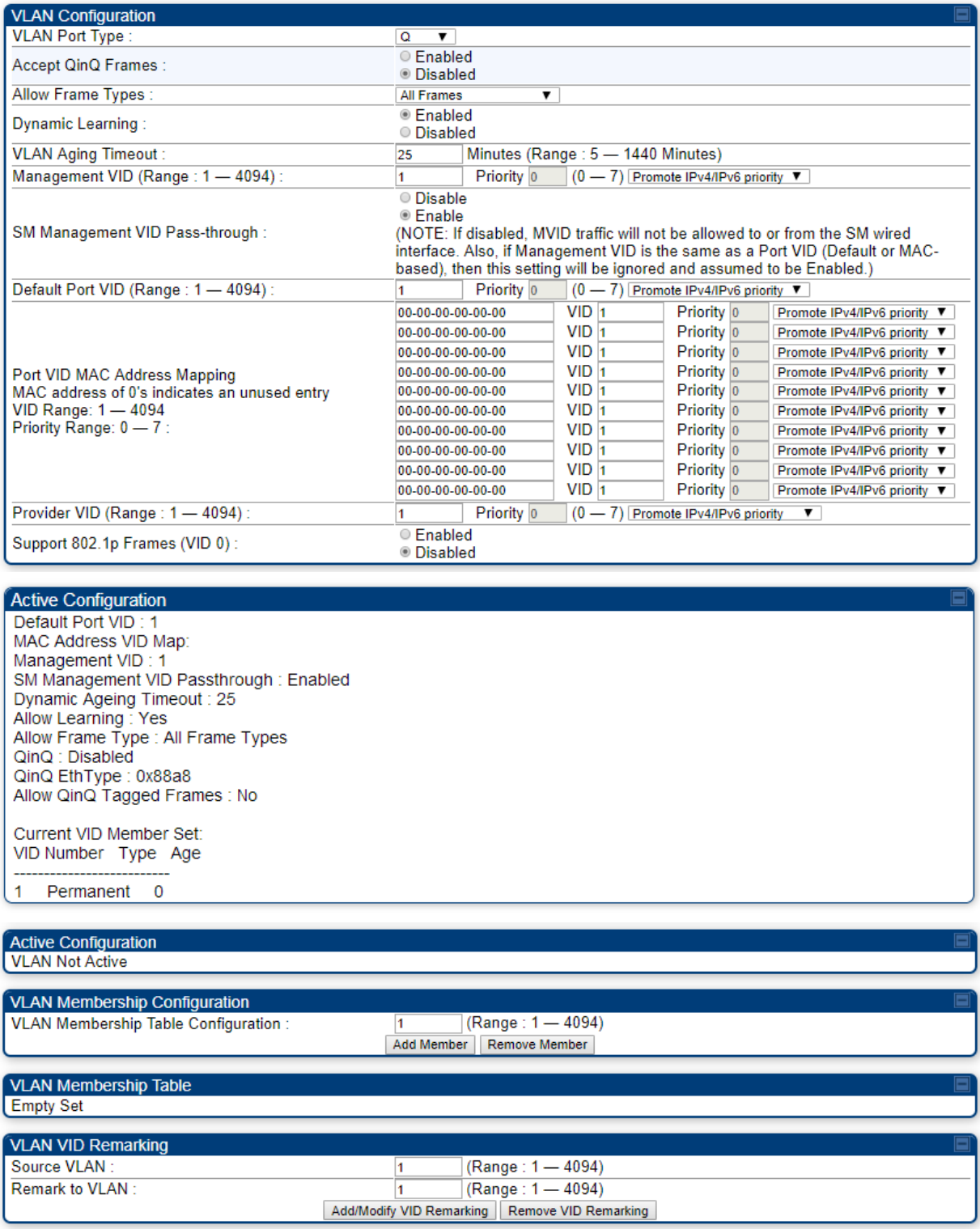
<table>
<tr><th>Attribute</th><th>Meaning</th></tr>
<tr><td>VLAN Aging Timeout</td><td>Specify how long the AP must keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is 25 (minutes).
 
Note
VIDs that you enter for the Management VID and VLAN Membership parameters do not time out.</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 1.</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:
Table 14 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 Configuration > VLAN web page of the AP. The Q-in-Q EtherType parameter is configured with a default EtherType of 0x88a8 in addition to four alternate EtherTypes that can be configured to aid in interoperability with existing networks that use a different EtherType than the default.
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>Use AP's Management VID for ICC connected SM</td><td>This field allows the SM to use the AP’s management VLAN ID when the SM is registered to the AP via ICC.</td></tr>
</table>

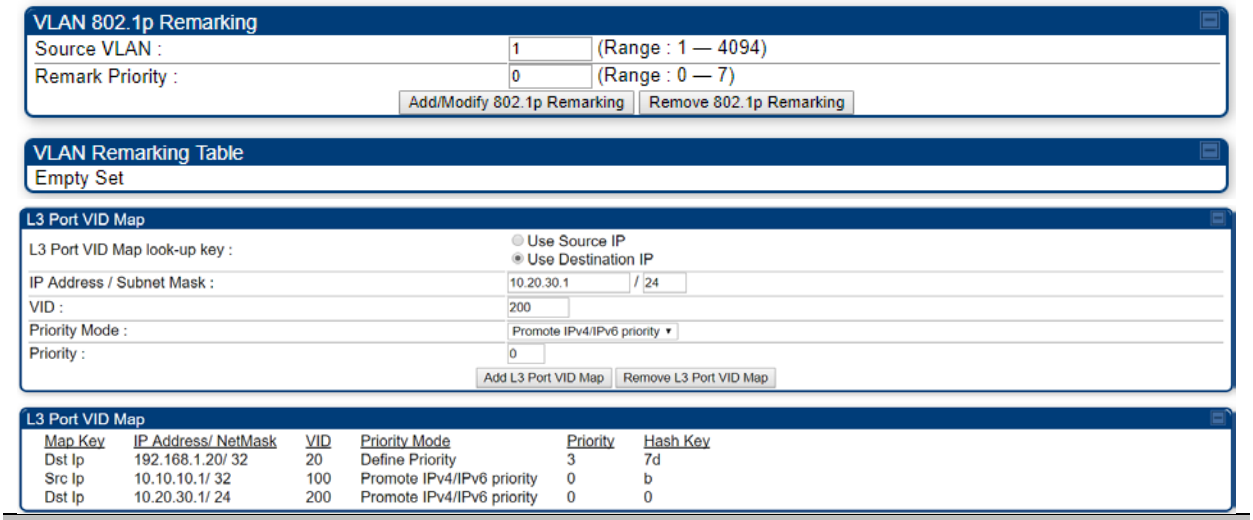
VLAN Not Active	When VLAN is enabled in the AP, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of 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 15.

Table 15 SM VLAN attributes





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.
Support 802.1p Frames	This parameter allows the operator to enable or disable 802.1p frames. When 802.1p feature is enabled on SM, the packets are added with VID=0 and priority bits are set.

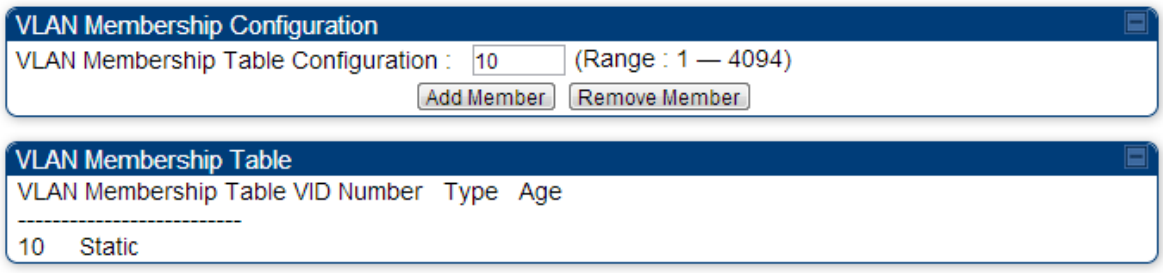
Active Configuration, Default Port VID	This is the value of the parameter of the same name, configured above.
Active Configuration, MAC Address VID Map	This is the listing of the MAC address VIDs configured in **Port VID MAC Address Mapping**.
Active Configuration, Management VID	This is the value of 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.
IP Lookup Direction	This parameter supports following options. • **Use Source IP:** Mapping is done based on the source IP of the incoming packet. • **Use Destination IP:** Mapping is done based on the Destination IP of the incoming packet.
IP Address / Subnet Mask	This parameter specifies the IP Address and the Subnet Mask which needs to be matched.
VID	This parameter specifies the VLAN which is tagged to the packet.
Priority Mode	This parameter specifies the priority precedence to decide if 802.1p or DSCP Priority bits need to be used when making priority decisions.
Priority	This parameter specifies the 802.1p Priority bits in the VLAN tag.
L3 Port VID Map	This field displays the Map key, IP address/subnet mask, VID, Priority mode, Priority, and Hash key information of the tagged packets.

VLAN Membership tab of SM

The **Configuration > VLAN > VLAN Membership** tab is explained in Table 16.

Table 16 SM VLAN Membership attributes



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

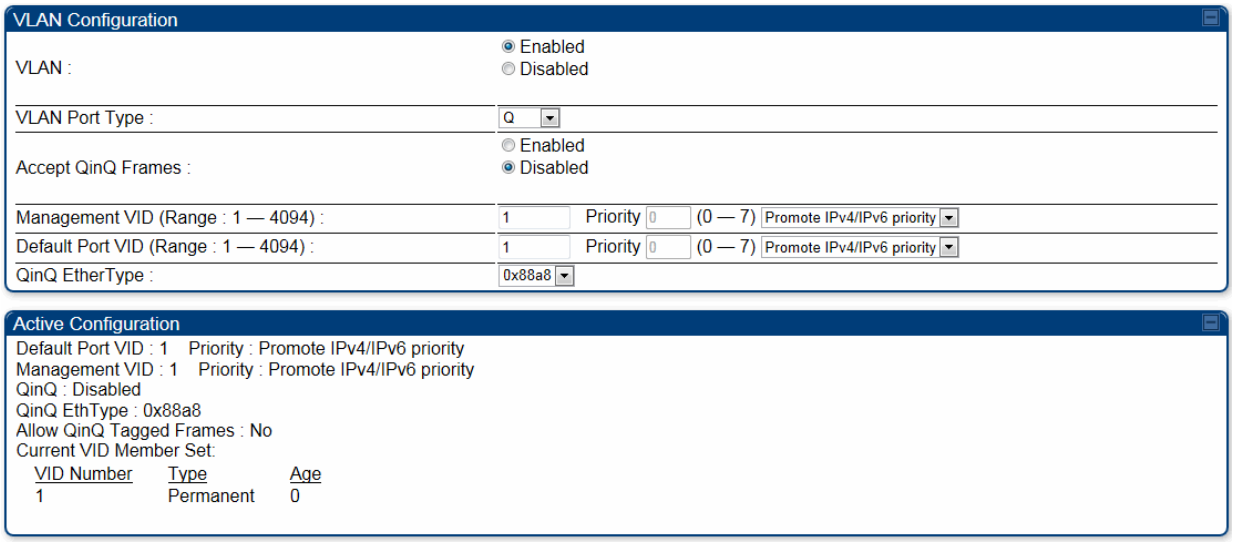
VLAN configuration for PTP

Applicable products	PTP: ☑ BHM ☑ BMS

VLAN page of BHM

The VLAN tab of BHS is explained in Table 17.

Table 17 BHM VLAN page attributes



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

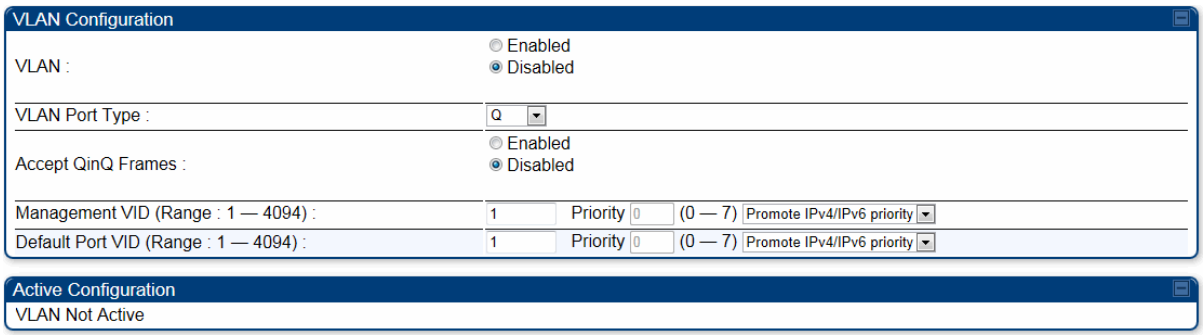
Management VID (Range 1-4094)	Enter the VID that the BHS must share with the BHM. The range of values is 1 to 4095. The default value is **1**.
Default Port VID (Range 1-4094)	This is the VID that is used for untagged frames and corresponds to the Q-Tag for 802.1Q frames (if VLAN Port Type is Q), or the C-Tag for 802.1ad frames (if the VLAN Port Type is Q-in- Q).
QinQ Ether Type	Modules can be configured with 802.1ad Q-in-Q DVLAN (Double-VLAN) tagging which is a way for an operator to put an 802.1Q VLAN inside of an 802.1ad VLAN. A nested VLAN, which is the original 802.1Q tag and a new second 802.1ad tag, allows for bridging of VLAN traffic across a network and segregates the broadcast domains of 802.1Q VLANs. Q-in-Q can be used with PPPoE and/or NAT. The 802.1ad standard defines the S-VLAN as the Service Provider VLAN and the C-VLAN as the customer VLAN. The radio software does 2-layer Q-in-Q whereby the C-VLAN is the 802.1Q tag and the S-VLAN is the second layer Q tag as shown below: The 802.1ad S-VLAN is the outer VLAN that is configurable on the **Configuration > VLAN** web page of the BHM. The Q-in-Q EtherType parameter is configured with a default EtherType of 0x88a8 in addition to four alternate EtherTypes that can be configured to aid in interoperability with existing networks that use a different EtherType than the default. The C-VLAN is the inner VLAN tag, which is the same as 802.1Q. As a top-level concept, this operates on the outermost tag at any given time, either “pushing” a tag on or “popping” a tag off. This means packets will at most transition from an 802.1Q frame to an 801.ad frame (with a tag “pushed” on) or an untagged 802.1 frame (with the tag “popped” off. Similarly, for an 802.1ad frame, this can only transition from an 802.1ad frame to an 802.1Q frame (with the tag “popped” off) since the radio software only supports 2 levels of tags.
VLAN Not Active	When VLAN is enabled in the BHM, the Active Configuration block provides the following details as read-only information in this tab. In the Cambium fixed wireless broadband IP network, each device of any type is automatically a permanent member of VID 1. This facilitates deployment of devices that have VLAN enabled with those that do not.

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

VLAN page of BHS

The VLAN tab of BHS is explained in Table 18.

Table 18 BHS VLAN page attributes



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

PPPoE page of SM

Applicable products	**PMP:**	☑ 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.

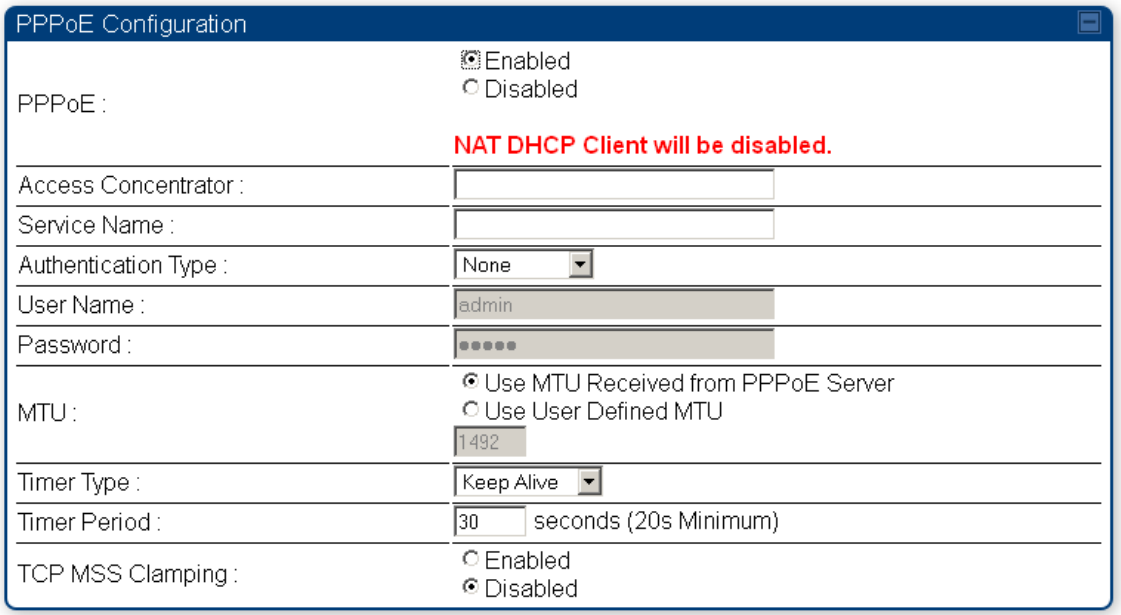
In order to enable PPPoE, NAT MUST be enabled on the SM and Translation Bridging MUST be disabled on the AP. These items are strictly enforced for you when you are trying to enable PPPoE. A message will indicate any prerequisites not being met. Also, the NAT Public IP DHCP client cannot be enabled, because 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 19.

Table 19 SM PPPoE attributes



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

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

IPv4 and IPv6 Prioritization

450 Platform Family 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 20 DiffServ attributes – AP/BHM

DiffServ Configuration

CodePoints (00) — (07):
CP00 : 0 CP01 : 1 CP02 : 1 CP03 : 1 CP04 : 1 CP05 : 1 CP06 : 1 CP07 : 1
CodePoints (08) — (15):
CP08 : 1 CP09 : 1 CP10 : 1 CP11 : 1 CP12 : 1 CP13 : 1 CP14 : 1 CP15 : 1
CodePoints (16) — (23):
CP16 : 2 CP17 : 1 CP18 : 2 CP19 : 1 CP20 : 2 CP21 : 1 CP22 : 2 CP23 : 1
CodePoints (24) — (31):
CP24 : 3 CP25 : 1 CP26 : 3 CP27 : 1 CP28 : 3 CP29 : 1 CP30 : 3 CP31 : 1
CodePoints (32) — (39):
CP32 : 4 CP33 : 1 CP34 : 4 CP35 : 1 CP36 : 4 CP37 : 1 CP38 : 4 CP39 : 1
CodePoints (40) — (47):
CP40 : 5 CP41 : 1 CP42 : 1 CP43 : 1 CP44 : 1 CP45 : 1 CP46 : 5 CP47 : 1
CodePoints (48) — (55):
CP48 : 6 CP49 : 1 CP50 : 1 CP51 : 1 CP52 : 1 CP53 : 1 CP54 : 1 CP55 : 1
CodePoints (56) — (63):
CP56 : 7 CP57 : 1 CP58 : 1 CP59 : 1 CP60 : 1 CP61 : 1 CP62 : 1 CP63 : 1

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

MPLS Configuration

MPLS Traffic Class (TC) 0 :	0
MPLS Traffic Class (TC) 1 :	1
MPLS Traffic Class (TC) 2 :	2
MPLS Traffic Class (TC) 3 :	3
MPLS Traffic Class (TC) 4 :	4
MPLS Traffic Class (TC) 5 :	5
MPLS Traffic Class (TC) 6 :	6
MPLS Traffic Class (TC) 7 :	7

<table>
<tr><th>Attribute</th><th>Meaning</th></tr>
<tr><td>Codepoints 1 through 63</td><td>The PMP family of APs support four levels of QoS. The mapping of these eight priority values to data channels is determined by the number of data channels configured per SM as shown in the table below:
<table><tr><th>Number of QoS levels →</th><th>1</th><th>2</th><th>3</th><th>4</th></tr><tr><td>Level 1</td><td>0-7</td><td>0-3</td><td>0-1</td><td>0-1</td></tr><tr><td>Level 2</td><td>-</td><td>4-7</td><td>2-3</td><td>2-3</td></tr><tr><td>Level 3</td><td>-</td><td>-</td><td>4-7</td><td>4-5</td></tr><tr><td>Level 4</td><td>-</td><td>-</td><td>-</td><td>6-7</td></tr></table>
For example, for an AP that uses the default table shown above has configured 3 QoS levels per SM, would see codepoints 0 through 15 mapped to the Low Priority data channels, codepoint 16 would be mapped to the Medium Priority data channels, and so on.
Note that CodePoints 0, 8, 16, 24, 32, 48, and 56 are predefined to the fixed values shown in Table 20 above and are not user configurable. Operator cannot change any of these three fixed priority values. Among the configurable 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.</td></tr>
<tr><td>CodePoint Select</td><td>This represents the CodePoint Selection to be modified via Priority Select.</td></tr>
<tr><td>Priority Select</td><td>The priority setting input for the CodePoint selected in CodePoint Select.</td></tr>
<tr><td>Priority Precedence</td><td>Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.</td></tr>
<tr><td>PPPoE Control Message Priority</td><td>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.</td></tr>
<tr><td>MPLS Traffic Class (TC) 0 through MPLS Traffic Class (TC) 7</td><td>The Multi-Protocol Label Switching (MPLS) protocol is used to route traffic based on the priority setting configured each MPLS Traffic Class.
MPLS Traffic Class (TC) 0 through MPLS Traffic Class (TC) 7 can be configured with 0 through 7 priority settings.</td></tr>
</table>

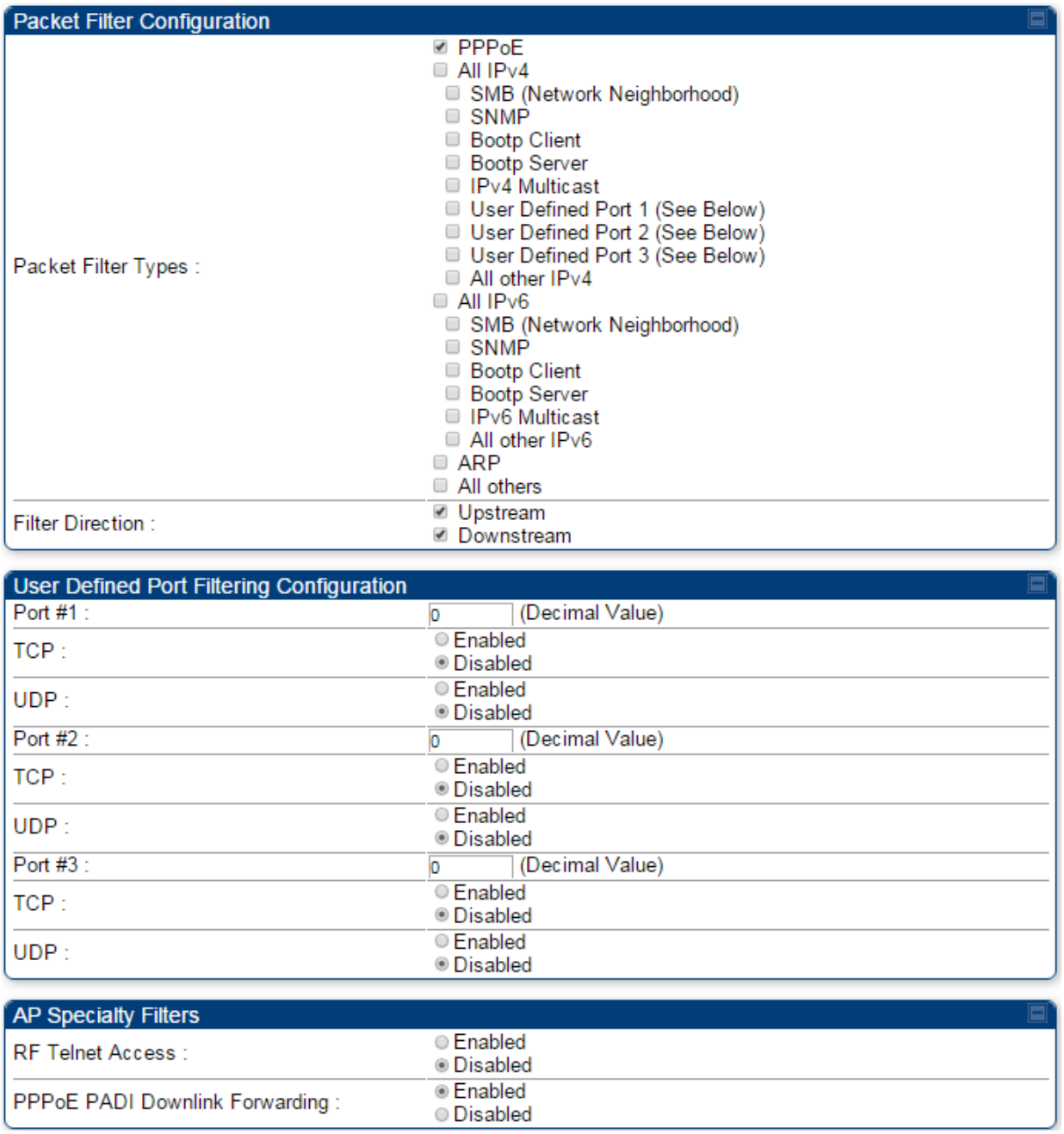
IPv4 and IPv6 Filtering

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 21 Packet Filter Configuration attributes



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 1-67
  Upgrading to a new software version on page 1-67

Caution

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

Use CNUT 4.11.2 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

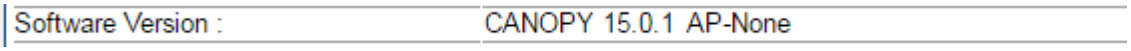
Checking the installed software version

To check the installed software version, follow these instructions:

Procedure 10 Checking the installed software version

1. Click on **General** tab under **Home** menu.
2. Note the installed Software Version (under Device Information):

   PMP/PTP 450/450i/450m

3. Go to the support website (see Contacting Cambium Networks on page 1) and find Point-to-Multipoint software updates. Check that the latest 450 Platform Family 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 1-67.

Upgrading to a new software version

All 450 platform modules are upgraded using the Canopy Network Updater Tool. The Canopy Network Updater Tool (CNUT) manages and automates the software 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 Auto update 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: https://www.cambiumnetworks.com/products/software-tools/cambium-network-updater-tool/

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

CNUT functions

The Canopy Network Updater tool has the following functions:

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

- An md5 checksum calculator utility for identifying corruption of downloaded image files before Network Updater is set to apply them.

Network element groups

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

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

Network layers

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

Script engine

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

The Autodiscovery capability in Network Updater finds all of your network elements.
This comprehensive discovery:

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

The following scripts are included with CNUT:

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

Software dependencies for CNUT

CNUT functionality requires

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

CNUT download

CNUT can be downloaded together with each system release that supports CNUT. Software for these system releases is available from https://www.cambiumnetworks.com/products/software-tools/cambium-network-updater-tool/, 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 11 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 tree using the **Add Elements to Network Root** operation (located at **Edit > Add Elements to Network Root**).

5 In the **Add Elements** dialogue, select a type of **Access Point** or **Subscriber Module** and enter the IP address of **169.254.1.1**.

6 Make sure that the proper Installation Package is active with the **Package Manager** dialogue (located at **Update > Manage Packages**).

7 To verify connectivity with the radio, perform a **Refresh**, **Discover Entire Network** operation (located at **View > Refresh/Discover Entire Network**). You must see the details columns for the new element filled in with ESN and software version information.

8 Initiate the upgrade of the radio using **Update Entire Network Root** operation (located at **Update > Update Entire Network Root**). When this operation finishes, the radio is done being upgraded.

General configuration

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

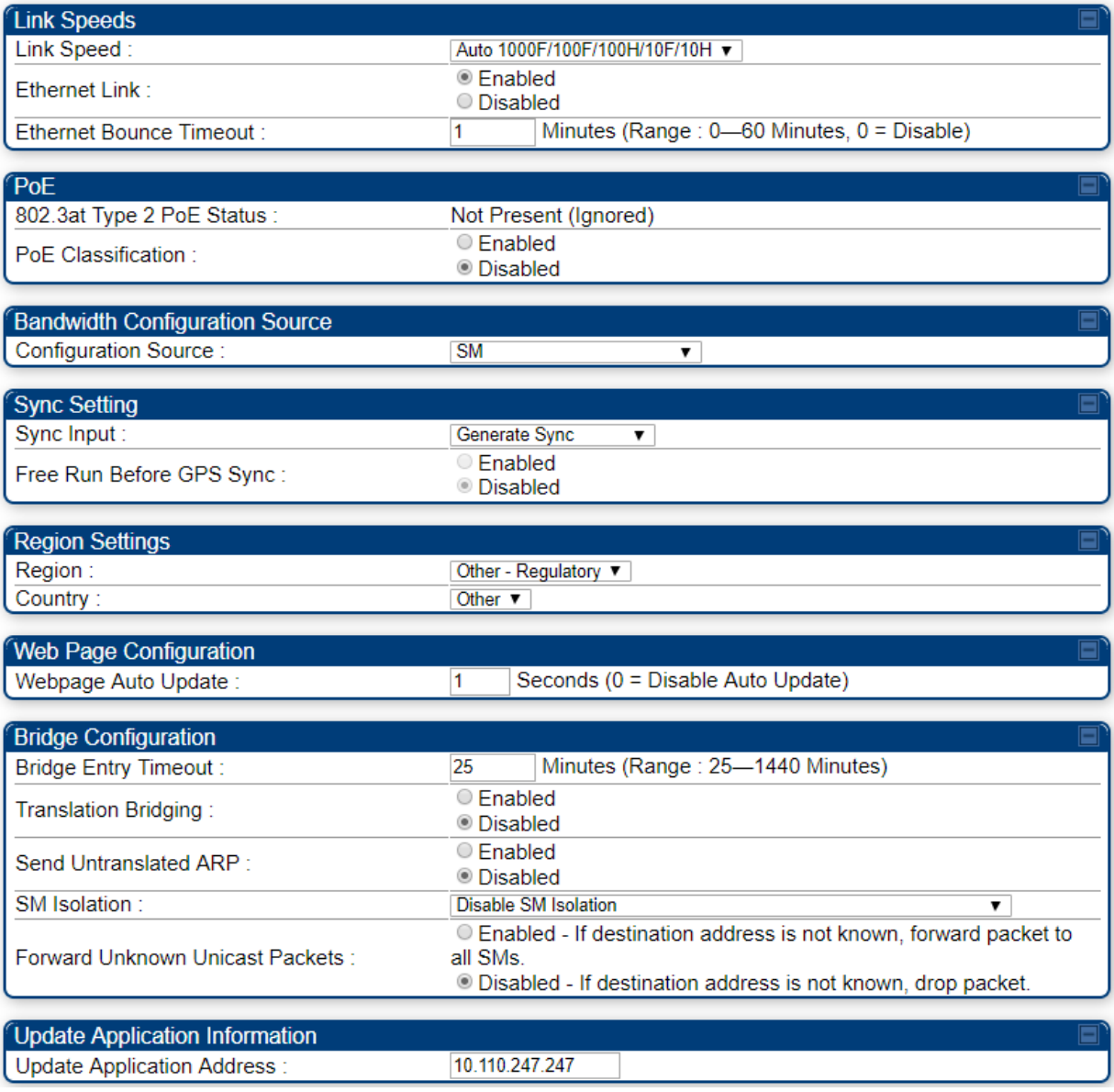
Applicable products	PMP: ☑ AP ☑ SM	PTP: ☑ BHM ☑ BMS

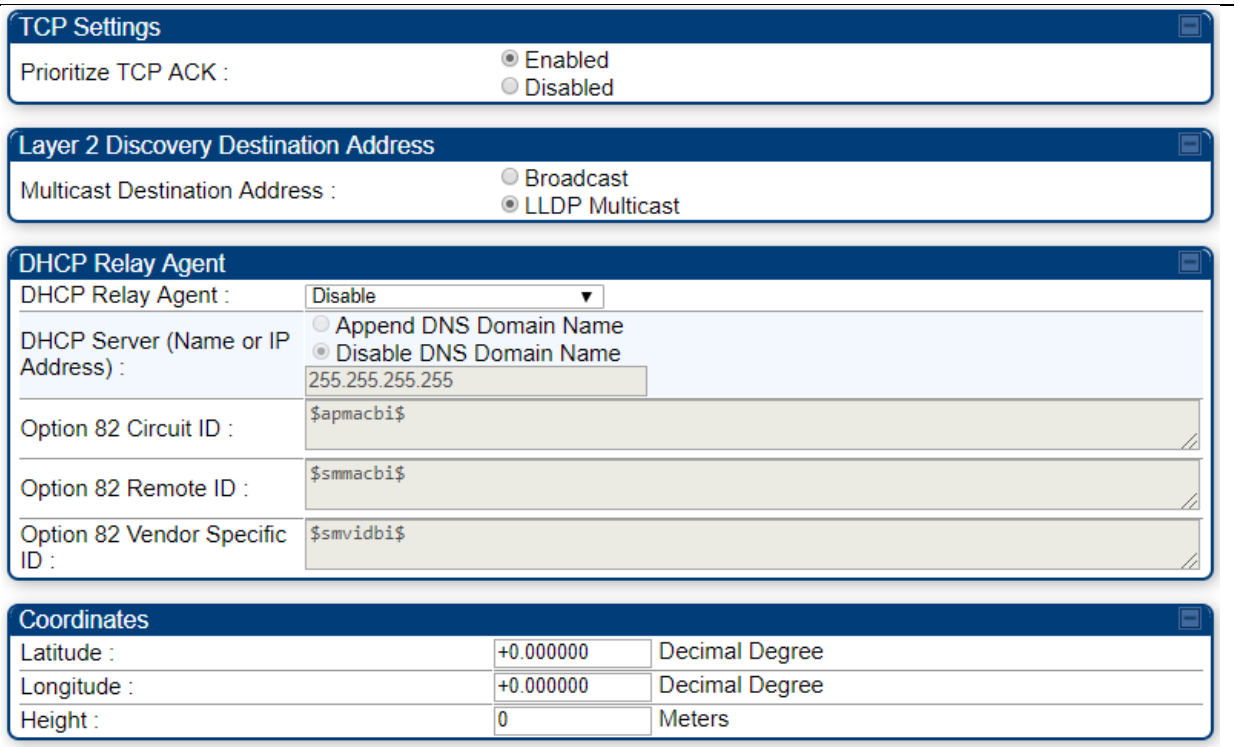
PMP 450m and PMP/PTP 450i Series

General page - PMP 450i AP

The General page of AP is explained in Table 22.

Table 22 General page attributes – PMP 450i AP





Attribute	Meaning
Ethernet Port Selection	Ethernet Port selection is applicable to the 450m platform only with two choices in the drop-down list: • Main: A selection of main indicates that link connectivity and power to the 450m is provided through the RF45 connection on the Main port of the AP • SFP: A selection of SFP indicates that link connectivity will be provided through the SFP port on the 450m Power continues to be provided via the RJ45 Main port
Link Speeds	From the drop-down list of options, select the type of link speed for the Ethernet connection. The Auto settings allow the two ends of the link to automatically negotiate with each other the best possible speed, and check whether the Ethernet traffic is full duplex or half duplex. However, some 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.
Ethernet Link	This parameter allows the operator to enable or disable Ethernet Link.
Ethernet Bounce Timeout	This parameter allows the operator to configure Ethernet bouce timeout ranging from 0 to 60 minutes. Value 0 disables Ethernet bounce timeout.
802.3at Type 2 PoE Status and	When the PoE Classification functionality is enabled and if Type 2 power is not present, the PAs do not power up and draw too much power. By default, the PoE Classification feature is disabled and the PAs will power up regardless of the classification presented by the power source.

PoE Classification (PMP 450i Series only)	This is supported only on 450i series devices. PoE Classification configuration status also can be check under home > General > Device Information tab: 802.3at Type 2 PoE Status : Not Present (Ignored)
Configuration Source	See Setting the Configuration Source on page 1-246.
Sync Input	See Configuring synchronization on page 1-105
Free Run Before GPS Sync	See Configuring synchronization on page 1-107
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 Series ODUs 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 128 IP devices at any time are valid to send data to the AP from behind the SM. SM 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 128 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.
Forward Unknown Unicast Packets	**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 Address	Enter the address of the server to access for software updates on this AP 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.

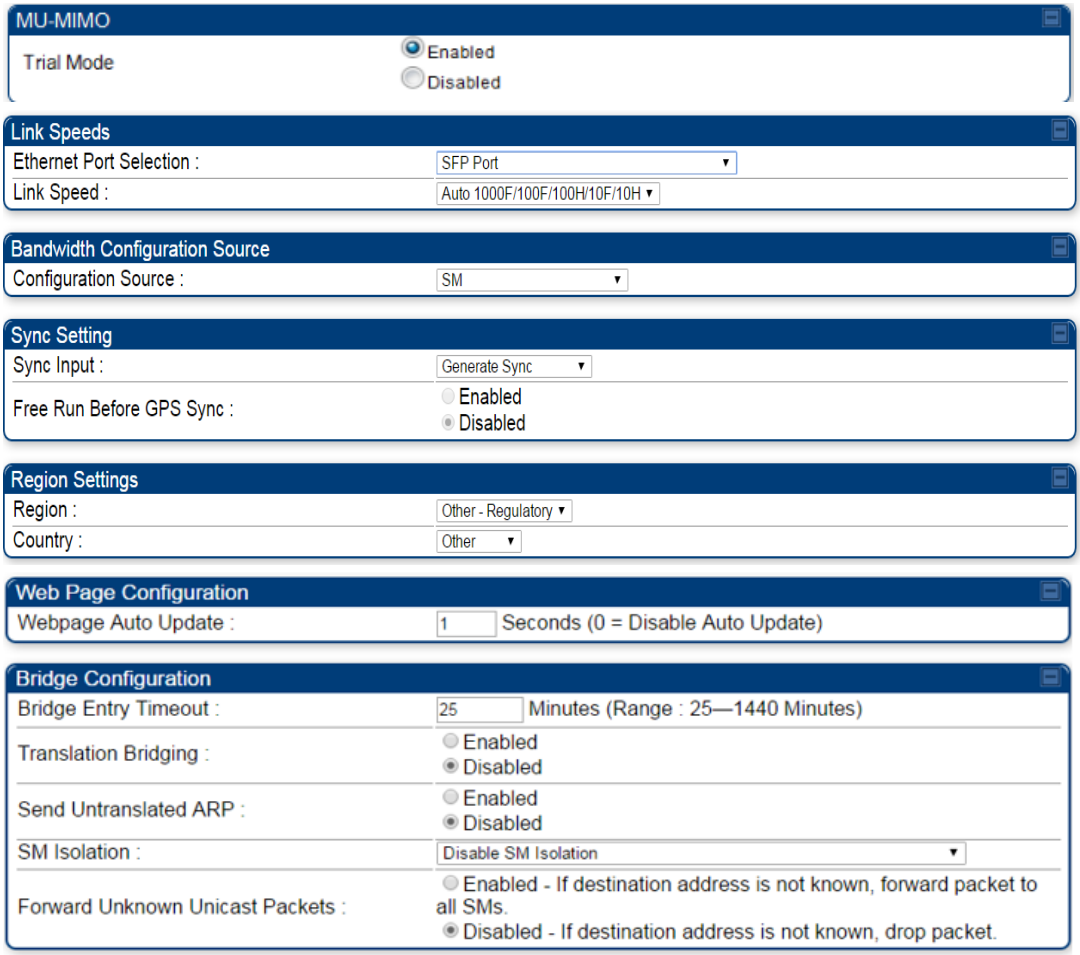
DHCP Server (Name or IP Address)	The DHCP relay server may be either a DNS name or a static IP address in dotted decimal notation. Additionally, the management DNS domain name may be toggled such that the name of the DHCP relay server only needs to be specified and the DNS domain name is automatically appended to that name. The default DHCP relay server addresses are 255.255.255.255 with the appending of the DNS domain name disabled.
Option 82 Circuit ID	This parameter specifies the Circuit ID for DHCP Relay Option 82 data. Following wildcards are supported: • $apmac$ - AP MAC adddress in ascii format, no delimiters • $apmacbi$ - AP MAC address in hex format (6 bytes) • $smmac$ - SM MAC adddress in ascii format, no delimiters • $smmacbi$ - SM MAC address in hex format (6 bytes) • $apsn$ - AP Site Name (may be truncated to 32 chars) • $smsn$ - SM Site Name (may be truncated to 32 chars) • $smvid$ - SM Port VID in ascii format, leading 0 included, 4 chars long • $smvidbi$ - SM Port VID in hex format (2 bytes) • $smluid$ - SM LUID Default value is $apmacbi$ **Note:** Overall expanded Option 82 data is limited to 255 bytes.
Option 82 Remote ID	This parameter specifies the Remote ID for DHCP Relay Option 82 data. Following wildcards are supported: • $apmac$ - AP MAC adddress in ascii format, no delimiters • $apmacbi$ - AP MAC address in hex format (6 bytes) • $smmac$ - SM MAC adddress in ascii format, no delimiters • $smmacbi$ - SM MAC address in hex format (6 bytes) • $apsn$ - AP Site Name (may be truncated to 32 chars) • $smsn$ - SM Site Name (may be truncated to 32 chars) • $smvid$ - SM Port VID in ascii format, leading 0 included, 4 chars long • $smvidbi$ - SM Port VID in hex format (2 bytes) • $smluid$ - SM LUID Default value is $smmacbi$ **Note:** Overall expanded Option 82 data is limited to 255 bytes.
Option 82 Vendor Specific ID	This parameter specifies the Vendor Specific ID for DHCP Relay Option 82 data. Following wildcards are supported: • $apmac$ - AP MAC adddress in ascii format, no delimiters • $apmacbi$ - AP MAC address in hex format (6 bytes) • $smmac$ - SM MAC adddress in ascii format, no delimiters • $smmacbi$ - SM MAC address in hex format (6 bytes)

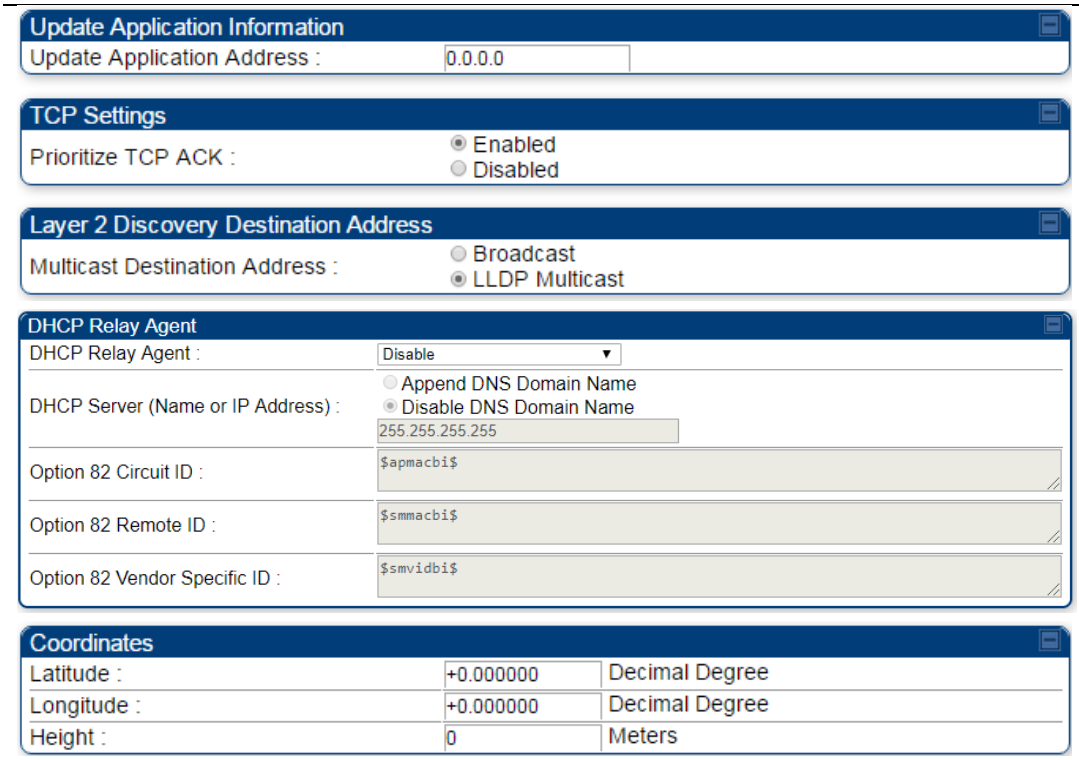
	• $apsn$ - AP Site Name (may be truncated to 32 chars) • $smsn$ - SM Site Name (may be truncated to 32 chars) • $smvid$ - SM Port VID in ascii format, leading 0 included, 4 chars long • $smvidbi$ - SM Port VID in hex format (2 bytes) • $smluid$ - SM LUID Default value is $smvidbi$ **Note:** Overall expanded Option 82 data is limited to 255 bytes.
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 - PMP 450m AP

The General page of AP is explained in Table 23.

Table 23 General page attributes –PMP 450m AP





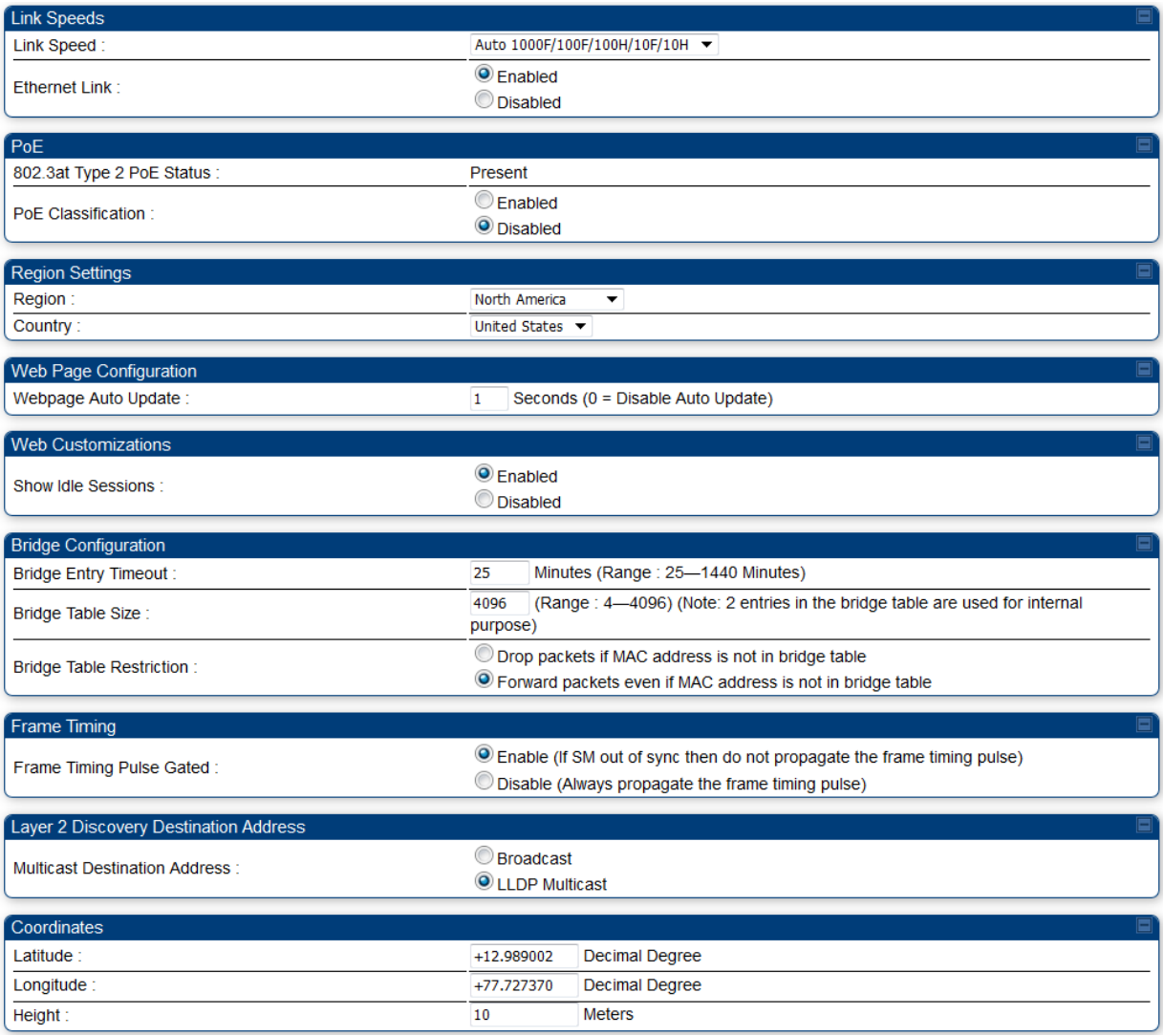
Attribute	Meaning
Trial Mode	This parameter allows to enable or disable Trial mode for radios with a Limited key. Once the trial key is applied, the 30-day trial can be enabled or disabled at any time.

For information about remaining attributes, refer Table 22.

General page - PMP 450i SM

The General page of PMP 450i SM is explained in Table 24. The General page of PMP 450 SM looks the same as PMP 450i SM.

Table 24 General page attributes – PMP 450i SM



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.
802.3at Type 2 PoE Status and PoE Classification	When the PoE Classification functionality is enabled and if Type 2 power is not present, the Pas do not power up and draw too much power. By default, the PoE Classification feature is disabled, and the Pas will power up regardless of the classification presented by the power source. This is supported only on 450i series ODUs.

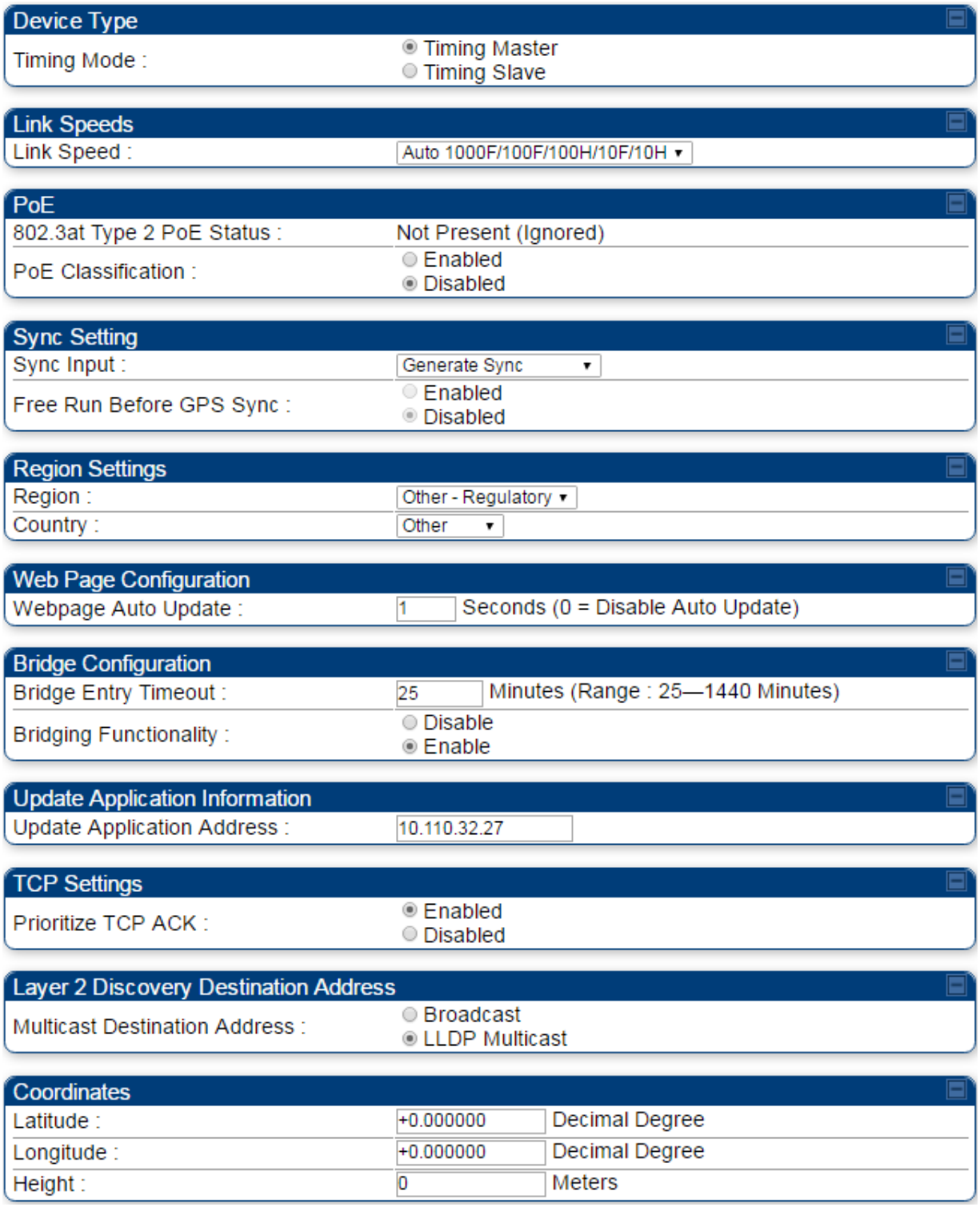
	PoE Classification configuration status also can be check under home > General > Device Information tab: 802.3at Type 2 PoE Status : Not Present (Ignored)
Ethernet Link Enable/Disable	Specify whether to enable or disable Ethernet/802.3 connectivity on the wired port of the SM. This parameter has no effect 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 Series ODU shipped to the United States is locked to a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
Webpage Auto Update	See Table 22 General page attributes – PMP 450i AP on page 1-71
Show Idle Sessions	This parameter allows to enable or disable displaying idle sessions.
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.
Bridge Table Size	This parameter allows to restrict devices to connect to the SM. It is configurable from 4 to 4096. **Note** Configure **Bridge Table Restriction parameter** to **Drop packets if MAC address is not in bridge table** option to restrict the number of devices configured from connecting to SM.
Bridge Table Restriction	This parameter allows to either allow or restrict devices to connect to SM using the following options: • Drop packets if MAC address is not in bridge table: Select this option to restrict communication from devices not listed in bridge table. • Forward packets even if MAC address is not in bridge table: Select this option to allow communication from any device.
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 another 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 another AP.
Multicast Destination Address	Using Link Layer Discovery Protocol (LLDP), a module exchanges multicast addresses with the device to which it is wired on the Ethernet interface. Although some switches (CMM4, for example) do not pass LLDP addresses upward in the network, a radio can pass it as the value of the **Multicast Destination Address** parameter value in the connected device that has it populated.
Coordinates	Physical radio location data may be configured via the **Latitude**, **Longitude** and **Height** fields.

General page - PTP 450i BHM

The General page of BHM is explained in Table 25. The General page of PTP 450 BHM looks the same as PTP 450i BHM.

Table 25 General page attributes – PTP 450i BHM



Attribute	Meaning
Timing Mode	Allows the user to choose the mode between Timing Master and Timing Slave.
Link Speed	See Table 22 General page attributes – PMP 450i AP on page 1-71
802.3at Type 2 PoE Status and PoE Classification	When the PoE Classification functionality is enabled and if Type 2 power is not present, the PAs do not power up and draw too much power. By default, the PoE Classification feature is disabled and the PAs will power up regardless of the classification presented by the power source. This is supported only on 450i Series ODUs. PoE Classification configuration status also can be check under home > General > Device Information tab: 802.3at Type 2 PoE Status : Not Present (Ignored)
Sync Input	See Configuring synchronization on page 1-105
Free Run Before GPS Sync	See Configuring synchronization on page 1-107
Region Country Webpage Auto Update Bridge Entry Timeout	See Table 22 General page attributes – PMP 450i AP on page 1-71
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 Multicast Destination Address	See Table 22 General page attributes – PMP 450i AP on page 1-71

Latitude
Longitude
Height

General page - PTP 450i BHS

The General page of PTP 450i BHS is explained in Table 26. The General page of PTP 450 BHS looks the same as PTP 450i BHS.

Table 26 General page attributes – PTP 450i BHS

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.
802.3at Type 2 PoE Status and PoE Classification	When the PoE Classification functionality is enabled and if Type 2 power is not present, the PAs do not power up and draw too much power. By default, the PoE Classification feature is disabled and the PAs will power up regardless of the classification presented by the power source. This is supported only on 450i Series ODUs. PoE Classification configuration status also can be check under home > General > Device Information tab: 802.3at Type 2 PoE Status : Not Present (Ignored)
Region	This parameter allows you to set the region in which the radio will operate. The BHS radio automatically inherits the Region type of the master. This behavior ignores the value of the **Region** parameter in the BHS, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter must be always set to the value that corresponds to the local region.
Country	This parameter allows you to set the country in which the radio will operate. The BHS radio automatically inherits the Country Code type of the master. This behavior ignores the value of the **Country** parameter in the BHS, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter must be always set to the value that corresponds to the local region. PMP/PTP 450i Series ODU shipped to the United States is locked to a Region Code setting of “United States”. Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
Webpage Auto Update	See Table 22 General page attributes – PMP 450i AP on page 1-71
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 22 General page attributes – PMP 450i AP on page 1-71
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 22 General page attributes – PMP 450i AP on page 1-71
Latitude Longitude Height	See Table 22 General page attributes – PMP 450i AP on page 1-71

General page – PMP 450b SM

The General page of PMP 450b SM is explained in Table 27. The General page of PMP 450b SM looks the same as PMP 450i SM.

Table 27 General page attributes – PMP 450b SM

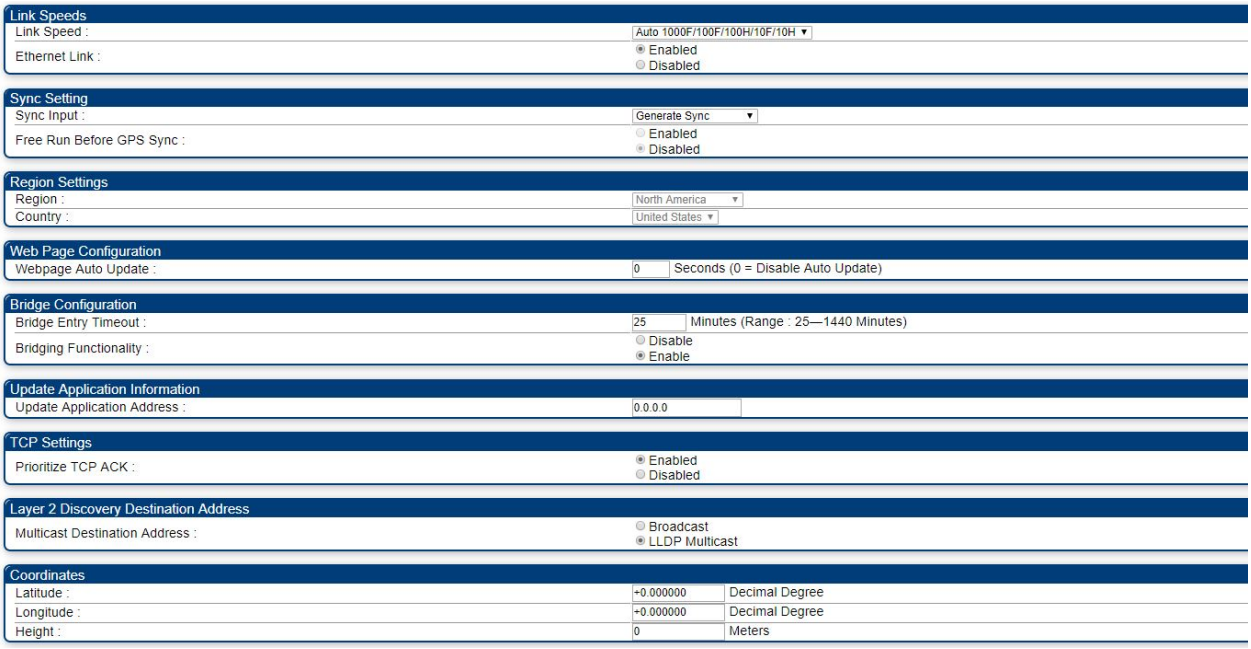
Attribute	Meaning
Link Mode	• Multipoint: Select this option to configure the device as a multipoint SM. • Backhaul: Select this option to configure the device as a Backhaul.
Timing Mode	• Timing Master: Select this option when **Link Mode** parameter is set to **Backhaul**. • Timing Slave: Select this option when **Link Mode** parameter is set to **Multipoint**.
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 APs and SMs in the operator network.
Ethernet Link Enabled/Disabled	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 Series ODU shipped to the United States is locked to a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.

Webpage Auto Update	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. 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.
Bridge Table Size	This parameter allows to restrict devices to connect to the SM. It is configurable from 4 to 4096.  **Note** Configure **Bridge Table Restriction parameter** to **Drop packets if MAC address is not in bridge table** option to restrict the number of devices configured from connecting to SM.
Bridge Table Restriction	This parameter allows to either allow or restrict devices to connect to SM using the following options: • Drop packets if MAC address is not in bridge table: Select this option to restrict communication from devices not listed in bridge table. Forward packets even if MAC address is not in bridge table: Select this option to allow communication from any device.
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 another 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 another 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.

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.*

PTP 450b BHM

Table 28 General page attributes – PMP 450b BHM



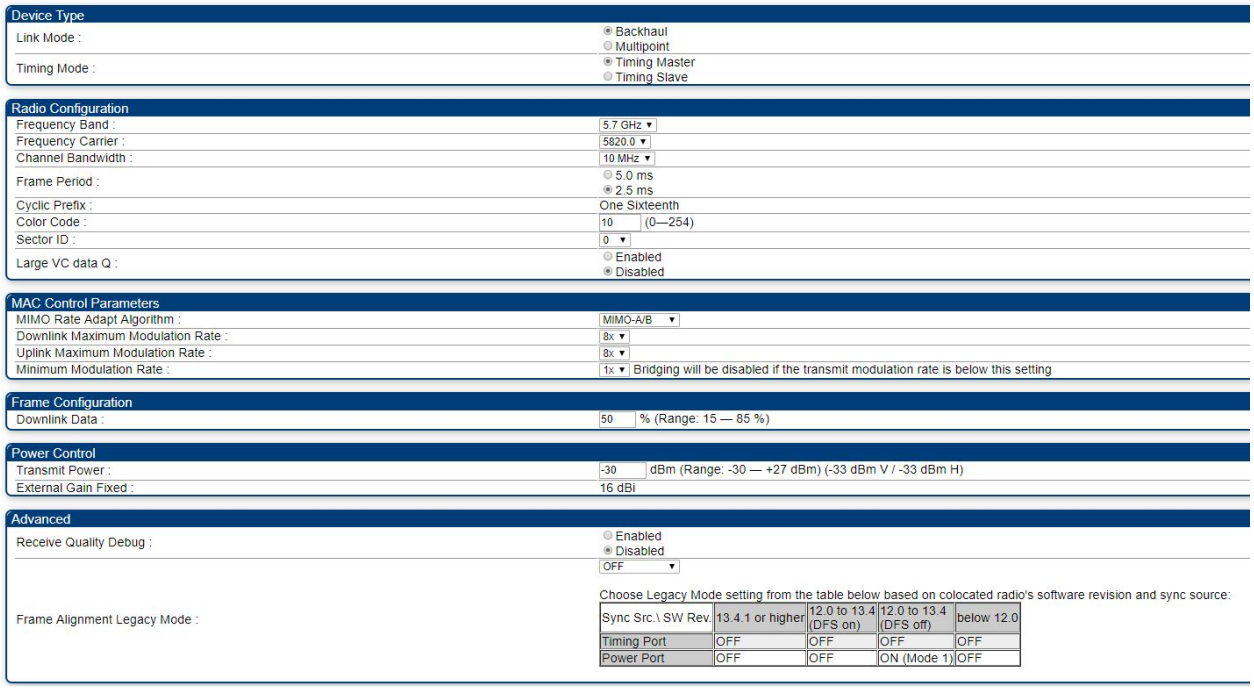
Attribute	Meaning
Link Speed	From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs and SMs in the operator network.
Ethernet Link Enabled/Disabled	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.
Sync Input	See Configuring synchronization on page 1-105

Attribute	Meaning
Free Run Before GPS Sync	See Configuring synchronization on page 1-107
Region	This field displays the AP's configured Country Code setting.
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 Series ODU shipped to the United States is locked to a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
Webpage Auto Update	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.
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.

Attribute	Meaning
Update Application Address	Enter the address of the server to access for software updates on this BHM and registered BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to **Enabled**. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements.
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.
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.*

PTP 450b BHS

Table 29 General page attributes – PMP 450b BHS



Attribute	Meaning
Link Mode	Backhaul to run the radio in PTP mode. Multipoint to run radio in PMP SM mode.
Timing Mode	Allows the user to choose the mode between Timing Master and Timing Slave.
Frequency Band	Select the desired operating frequency band.
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is None. For a list of channels in the band, see the drop-down list on the radio GUI.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM. The supported Channel Bandwidths are 5 MHz, 10 MHz, 15 MHz, 20 MHz, 30 MHz, and 40 MHz.
Frame Period	Select the Frame Period of the radio. The supported Frame Periods are: 5 ms and 2.5 ms.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Color Code	Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
Sector ID	This pull-down menu helps in configuring the Sector ID at a configurable value from 0 to 15.
Large VC data Q	SM and BH have a configurable option used to prevent packet loss in the uplink due to bursting IP traffic. This is designed for IP burst traffic particular to video surveillance applications.
MIMO Rate Adapt Algorithm	This pull-down menu helps in configuring the Rate Adapt Algorithm to MIMO-A/B, MIMO-B only, or MIMO-A only.
Downlink Maximum Modulation Rate	This pull-down menu helps in configuring the Downlink Maximum Modulation Rate at a configurable rate of 1X, 2X, 3X, 4X, 6X, or 8X. The default value is “8X”. The Rate Adapt Algorithm does not allow the modulation to go beyond this limit.

Attribute	Meaning
Uplink Maximum Modulation Rate	This pull-down menu helps in configuring the Uplink Maximum Modulation Rate at a configurable rate of 1X, 2X, 3X, 4X, 6X, or 8X. The default value is "8X". The Rate Adapt Algorithm does not allow the modulation to go beyond this limit.
Minimum Modulation Rate	This pull-down menu helps in configuring the Minimum Modulation Rate at a configurable rate of 1X, 2X, 3X, 4X, 6X, or 8X. The default value is "1X". If the Rate Adapt Algorithm is below this limit, then bridging is disabled. This is used if PTP network can route the traffic through another path.
Downlink Data	Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 90 Mb, then 75% specified for this parameter allocates 67.5 Mb for the downlink and 22.5 Mb for the uplink. The default for this parameter is 75%. This parameter must be set in the range of 15% - 85%, otherwise the invalid input will not be accepted and the previously-entered valid setting is used.
Transmit Power	This value represents the combined power of the BHM's two transmitters. Nations and regions may regulate transmit power. For example • PTP 450i Series modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. The professional installer of the equipment has the responsibility to: • Maintain awareness of applicable regulations. • Calculate the permissible transmitter output power for the module. • Confirm that the initial power setting is compliant with national or regional regulations. Confirm that the power setting is compliant following any reset of the module to factory defaults.
External Gain Fixed	This value needs to correspond to the published gain of the antenna used to ensure the radio will meet regulatory requirements.
Receive Quality Debug	To aid in link performance monitoring, the BHM and BHS now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM and 256-QAM) and per channel (polarization). **Note** Due to CPU load, this slightly degrades the packet during per second processing.
Frame Alignment Legacy Mode	See Table 48 PMP 450i AP Radio attributes - 5 GHz on page 1-156.

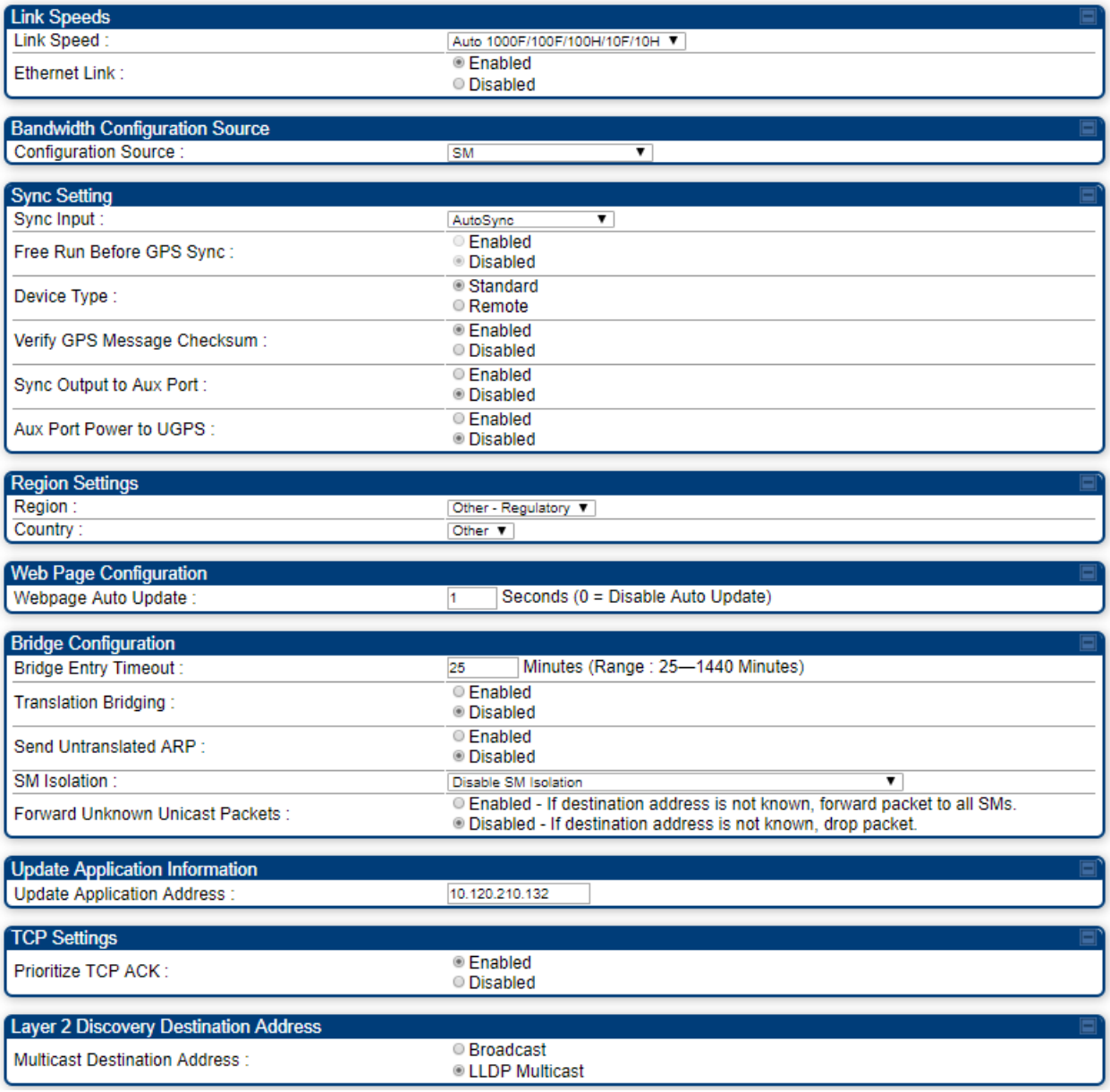
PMP/PTP 450 Series

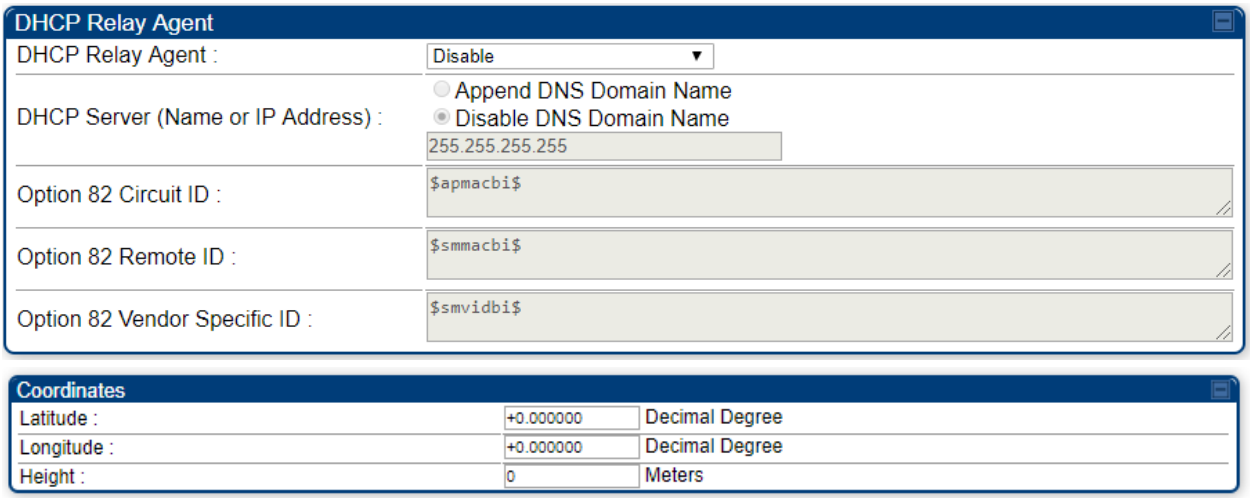
Note

Refer Table 22 and Table 24 for PMP 450 AP/SM General page parameters details.

General page - PMP 450 AP

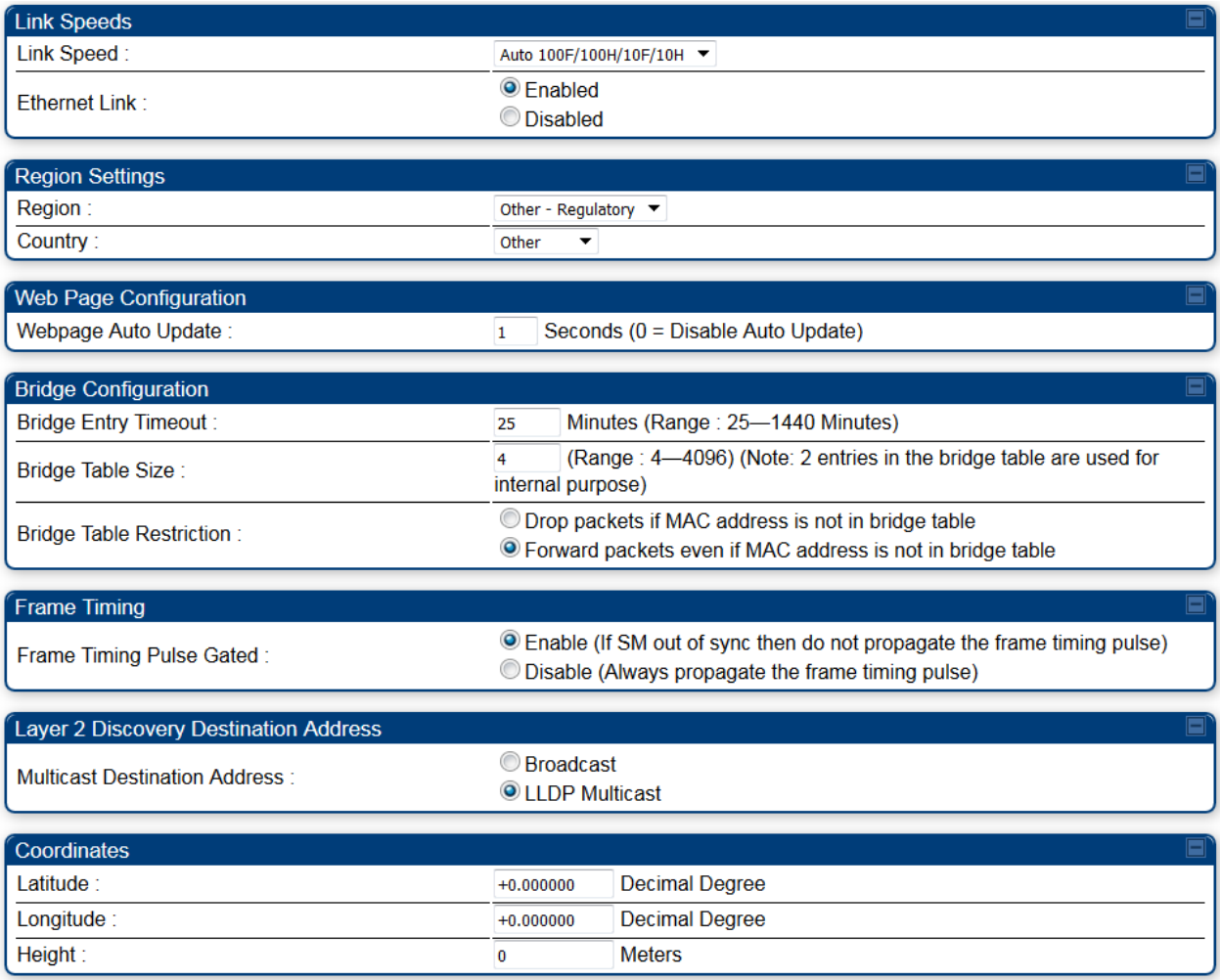
Figure 15 General page attributes - PMP 450 AP





General page - PMP 450 SM

Figure 16 General page attributes - PMP 450 SM

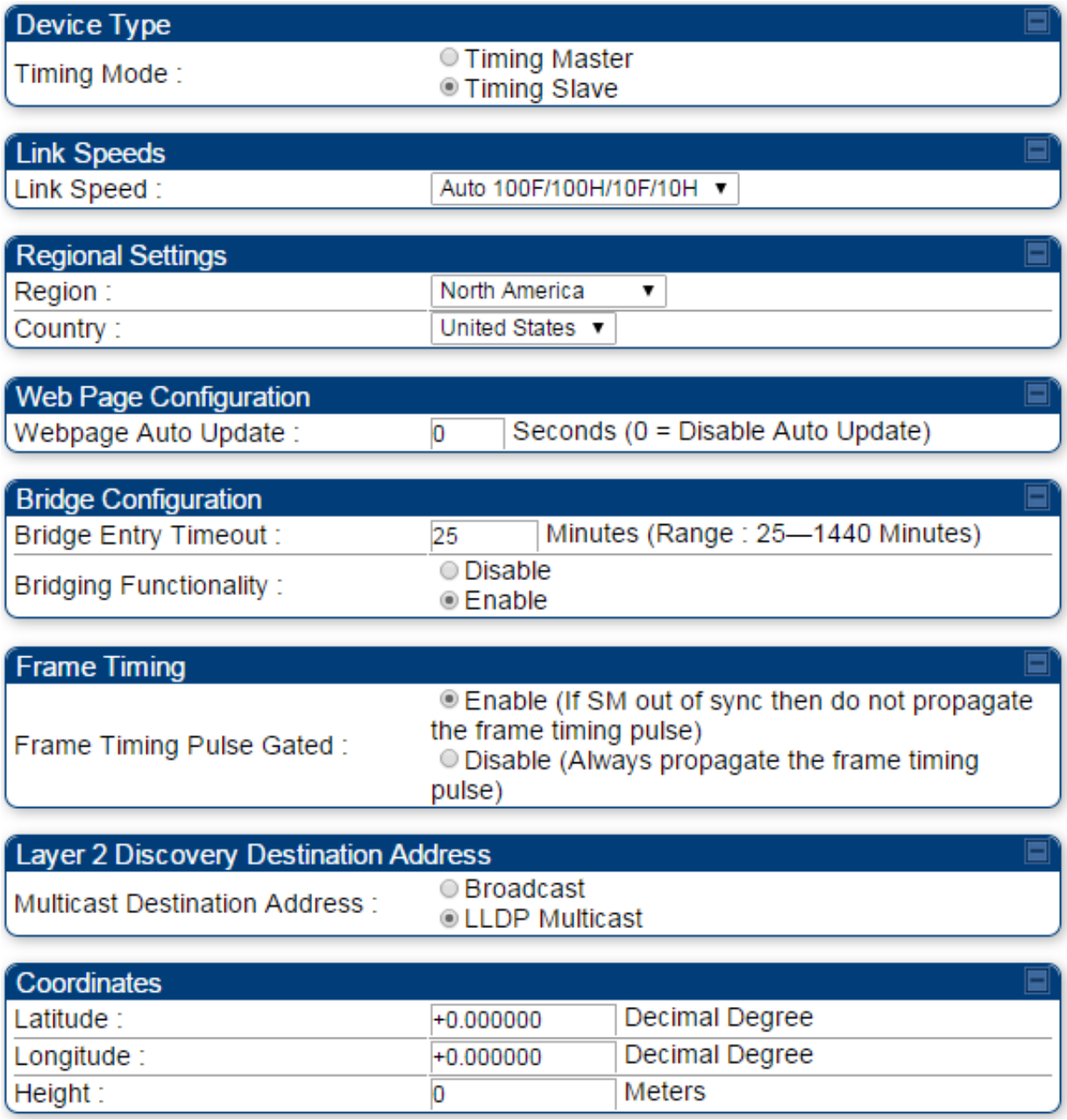


General page – PTP 450 BHM

Figure 17 General page attributes - PTP 450 BHM

General page – PTP 450 BHS

Figure 18 General page attributes - PTP 450 BHS



Configuring Unit Settings page

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

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

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

Note

LED Panel setting is applicable for SM and BHS only.

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

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

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

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

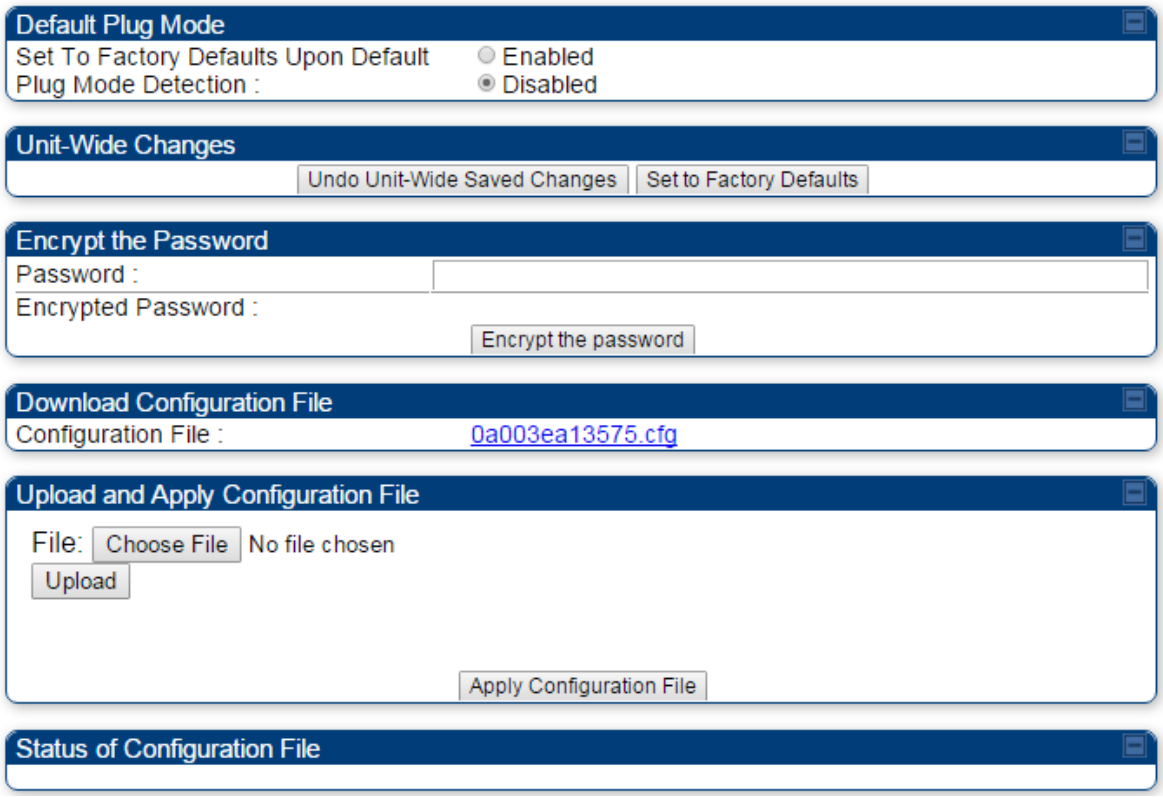
The Import and Export procedure of configuration file is described in Import and Export of config file on page 1-268.

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

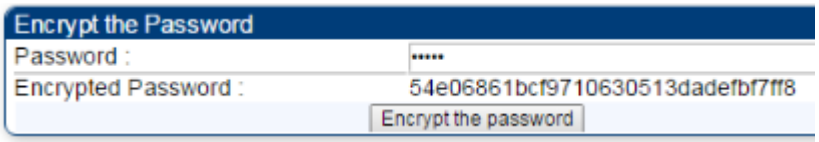
Unit Settings page of 450 Platform Family - AP/BHM

The Unit Setting page of AP/BHM is explained in Table 30.

Table 30 Unit Settings attributes – 450 Platform Family AP/BHM



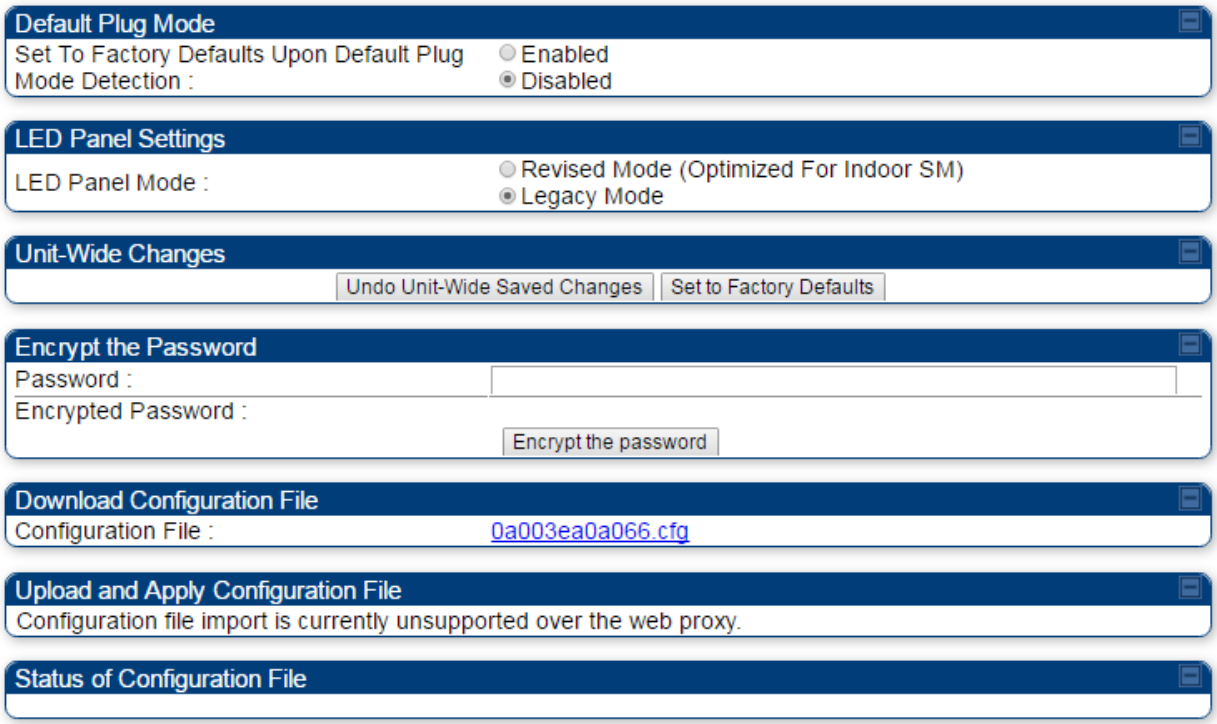
Attribute	Meaning
Set to Factory Defaults Upon Default Mode Detection	If **Enabled** is checked, then the default mode functions is enabled. When the module is rebooted with Default mode enabled, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults. 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 are disabled. **Caution** When **Set to Factory Defaults Upon Default Mode** is set to **Enable**, the radio does not select all of the frequencies for Radio Frequency Scan Selection List. It needs to be selected manually.
Undo Unit-Wide Saved Changes	When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.
Set to Factory Defaults	When you click this button, *all configurable parameters on all tabs* are 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.
Password	This allows to provide encrypted password for a given password. On click of 'Encrypt the password' button, the Encrypted Password field will display encrypted value of entered plain text password in 'Password' field. 
Configuration File	This allows to download the configuration file of the radio. This configuration file contains the complete configuration including all the default values. The configuration file is highlighted as downloadable link and the naming convention is "<mac address of AP>.cfg".
Apply Configuration File	This allows to import and apply configuration to the AP. **Chose File**: Select the file to upload the configuration. The configuration file is named as "<file name>.cfg". **Upload**: Import the configuration to the AP. **Apply Configuration File**: Apply the imported configuration file to the AP. The imported configuration file may either contain a full device configuration or a partial device configuration. If a partial configuration file is imported, only the items contained in the file will be updated, the rest of the device configuration parameters will remain the same. Operators may also include a special flag in the configure file to instruct the device to first revert to factory defaults then to apply the imported configuration.
Status of Configuration file	This section shows the results of the upload.

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

The Unit Settings page of PMP/PTP 450i SM/BHS is explained in Table 31.

Table 31 SM Unit Settings attributes



Attribute	Meaning
Set to Factory Defaults Upon Default Plug Detection	See Table 30 Unit Settings attributes – 450 Platform Family AP/BHM on page 1-100
LED Panel Settings	Legacy Mode configures the radio to operate with standard LED behavior.
Undo Unit-Wide Saved Changes	
Password	
Set to Factory Defaults	See Table 30 Unit Settings attributes – 450 Platform Family AP/BHM on page 1-100
Configuration File	
Status of Configuration file	

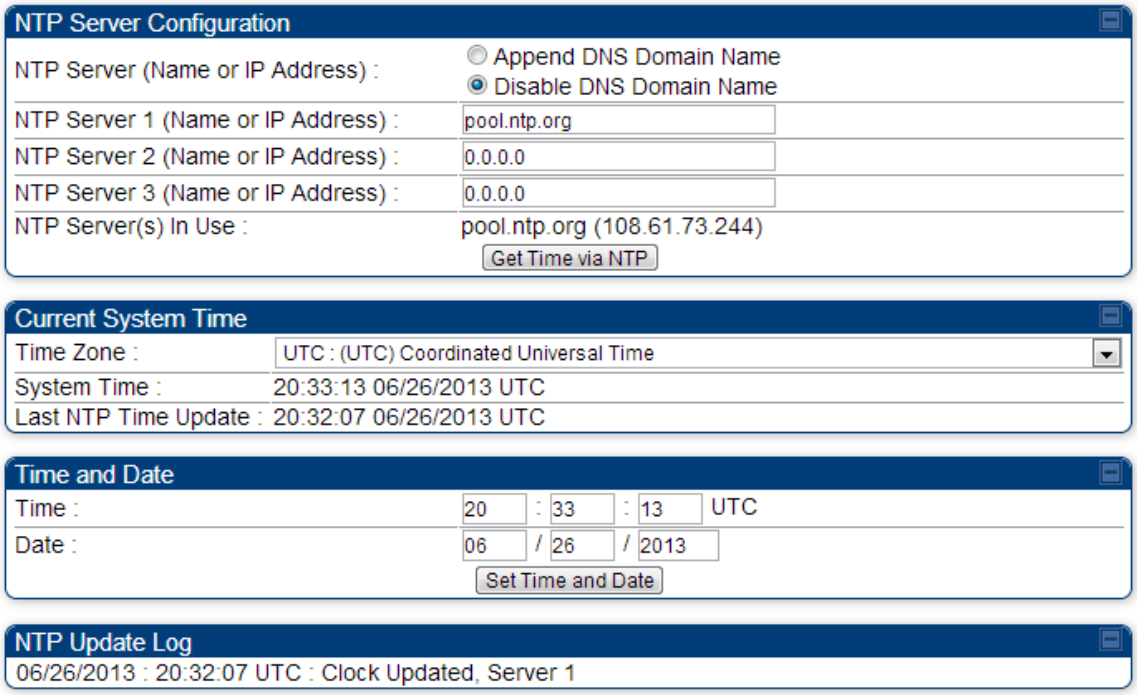
Setting up time and date

Time page of 450 Platform Family - AP/BHM

Applicable products	PMP: ☑ AP	PTP: ☑ BHM

The Time page of 450 Platform Family AP/BHM is explained in Table 32.

Table 32 450 Platform Family - AP/BHM Time attributes



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.

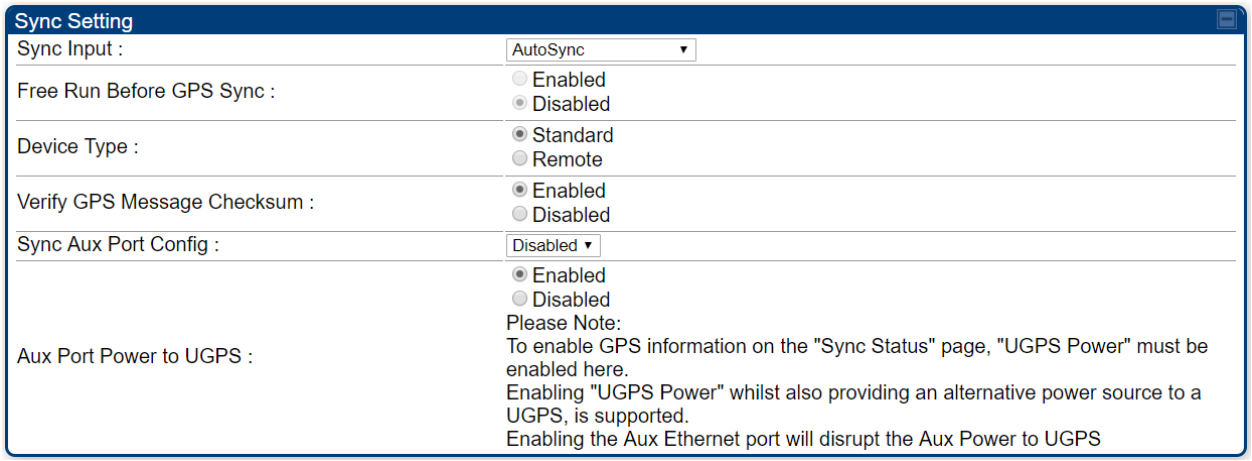
Configuring synchronization

Applicable products	**PMP:**	☑	AP	**PTP:** ☑	BHM

Sync Input

This section describes synchronization options for PMP and PTP configuration.

Figure 19 Sync Setting configuration



The **Sync Input** parameter can be configured under Sync Setting tab of **Configure > General** page (see General configuration on page 1-71).

PMP/PTP 450i Series has following synchronization input options:

- AutoSync
- AutoSync + Free Run
- Generate Sync

AutoSync

For 450i AP/BHM and 450m AP, the AP/BHM automatically receives sync from one of the following sources:

- GPS Sync over Timing Port (UGPS, cnPulse, co-located AP GPS sync output, or “Remote” Device feed from a registered SM’s GPS sync output)
- GPS Sync over Power Port (CMM4), CMM5, cnPulse module ODU Sync Port.

For 450 AP, the internal GPS is available in addition to the above sync sources. For a 450 BHM the only available sync source is the Timing Port, as GPS Sync Over Power Port is not supported. For a 450b BHM only GPS Sync Over Power Port is available.

Upon AP/BHM power on with the **Free Run Before GPS Sync** parameter set to disabled, 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 after sync is initially established, within two seconds the AP/BHM automatically attempts to source GPS signaling from another source.

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

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

Note

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

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.

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 BHS/SM registration is 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.

Note

In mode AutoSync + Free Run with the Free Run Before GPS Sync parameter set to disabled, 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/CMM5 or UGPS/cnPulse module, and there are no other APs/BHMs active within the link range. Using this option will not synchronize transmission of APs/BHMs that can “hear” each other; it will only generate a sync signal for the local AP/BHM and its associated SMs/BHS.

Note

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

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

Free Run Before GPS Sync

This option is available when the Sync Input parameter is configured for either AutoSync mode or AutoSync + Free Run mode. When **Free Run Before GPS Sync** is set to Enabled, if the radio does not detect a valid GPS synchronization pulse after booting up then it will operate in Generate Sync – Free Run mode until a valid source is detected. While the AP/BHM is in Generate Sync – Free Run mode SMs/BHS will be able to register, but 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 synchronization source is found, the AP/BHM automatically switches to receiving synchronization from the source and SM/BHS registration is maintained. If **Free Run Before GPS Sync** is set to Disabled, the AP/BHM does not transmit and SMs/BHS will be unable to register until a valid GPS synchronization source is connected.

Device Type

This parameter determines whether the device is configured as a Remote AP, receiving GPS sync from a co-located AP GPS sync output or Remote Device feed from a registered SM’s GPS sync output, or as a Standard AP. This parameter applies in AutoSync or AutoSync + Free Run modes only. Synchronization behavior is as follows:

Standard: The AutoSync mechanism will source GPS synchronization from the AP’s Aux/Timing port, the AP’s power port, or from the device on-board GPS module (if present).

Remote: The AutoSync mechanism will source GPS synchronization from the AP’s Aux/Timing port or from the device on-board GPS module (if present). GPS synchronization pulses on the Power Port are ignored.

Verify GPS Message Checksum

The Verify GPS Message Checksum parameter enables or disables validation of incoming GPS location messages from a UGPS or cnPulse module connected to the AP’s Aux Port. When enabled the AP will discard messages found to have an incorrect checksum and will increment the Invalid Message Count display of the Sync Status tab of the Home GUI page accordingly.

Sync Aux Port Config

The Sync Output to Aux Port parameter takes effect when the AP is operating in either AutoSync or AutoSync + Free Run modes. When enabled, the AP will output the GPS timing pulse on the Aux/Timing Port. In this configuration the AP may serve as a GPS synchronization source for a co-located AP.

Aux Port Power to UGPS

The 450 series APs are capable of supplying power to a connected UGPS or cnPulse module via the Aux/Timing Port. Enable the Aux Port Power to UGPS parameter to output power on the port.

Note

The AP is able to receive GPS sync pulses and satellite data via the Aux Port regardless of whether this parameter is Enabled or Disabled. However, on the 450m AP and 450i AP/BHM, the satellite data is displayed on the Sync Status page only when the Aux Port power is enabled.

Caution

When a UGPS module is used to provide GPS sync to two 450m or 450i APs simultaneously, it is recommended to install a separate power supply for the UGPS to prevent the possibility of sync interruption upon reboot of the APs.

Configuring security

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

- Managing module access by password on page 1-110: to configure the unit access password and access level
- See Radio Recovery on page 3-87
- Isolating from the internet on page 1-113: to ensure that APs are properly secured from external networks
- Encrypting radio transmissions on page 1-113: to configure the unit to operate with AES wireless link security
- Requiring SM Authentication on page 1-114: to set up the AP to require SMs to authenticate via the AP, WM, or RADIUS server
- Filtering protocols and ports on page 1-115: to filter (block) specified protocols and ports from leaving the system
- Encrypting downlink broadcasts on page 1-118: to encrypt downlink broadcast transmissions
- Isolating SMs on page 1-118: to prevent SMs in the same sector from directly communicating with each other
- Filtering management through Ethernet on page 1-119: to prevent management access to the SM via the radio's Ethernet port
- Allowing management only from specified IP addresses on page 1-119: to only allow radio management interface access from specified IP addresses
- Restricting radio Telnet access over the RF interface on page 1-119: to restrict Telnet access to the AP
- Configuring SNMP Access on page 1-123
- Configuring Security on page 1-125

Managing module access by password

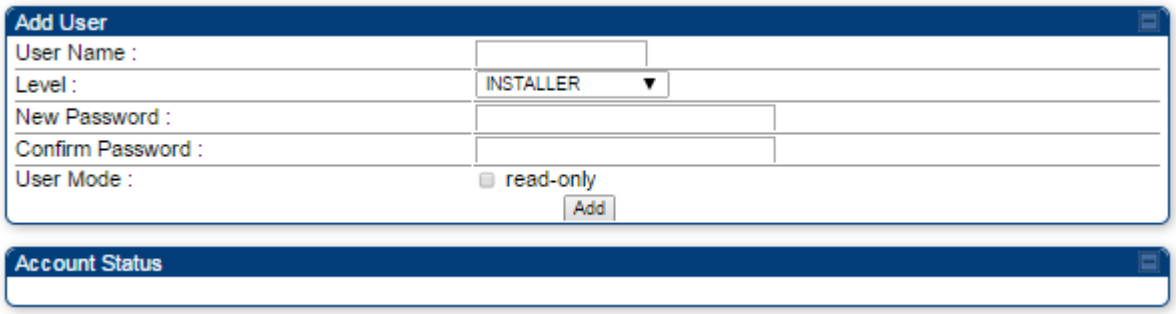
Applicable products	PMP: ☑ AP ☑ SM	PTP: ☑ BHM ☑ BMS

See Managing module access by password in Planning and installation Guide.

Adding a User for Access to a module

The **Account > Add User** page allows to create a new user for accessing 450 Platform Family - AP/SM/BHM/BHS. The Add User page is explained in Table 33.

Table 33 Add User page of account page - AP/ SM/BH



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

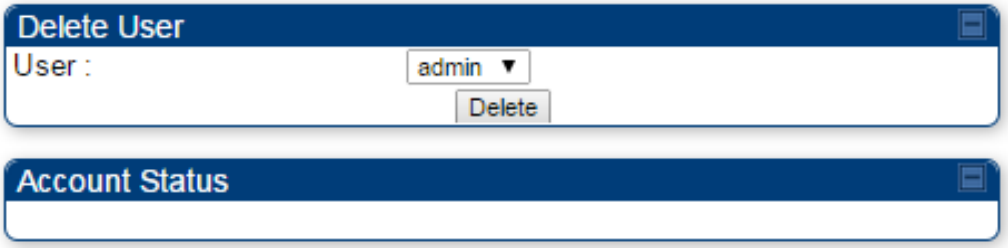
Note

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

Deleting a User from Access to a module

The **Account > Delete User** page provides a drop-down list of configured users from which to select the user you want to delete. The Delete User page is explained in Table 34.

Table 34 Delete User page - 450 Platform Family - AP/ SM/BH



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.

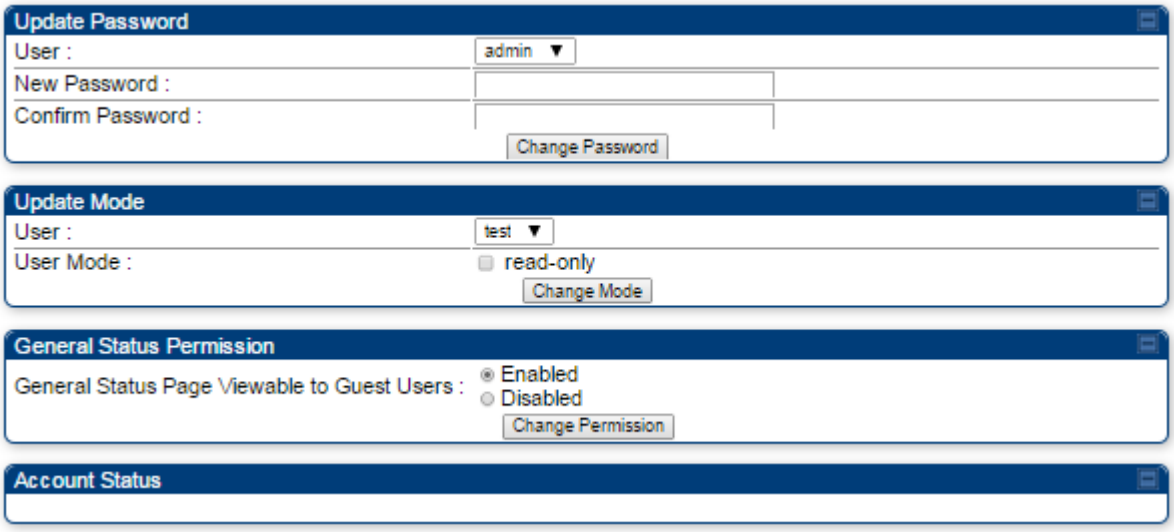
Changing a User Setting

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

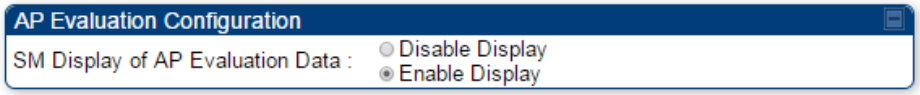
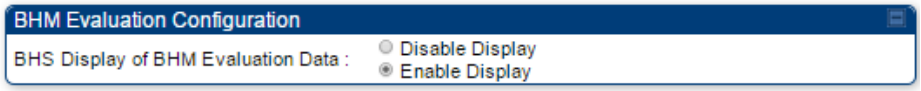
From the factory default state, configure passwords for both the root and admin account at the ADMINISTRATOR permission level, using **Update Password** tab of Change Users Setting page.

The Change User Setting page is explained in Table 35.

Table 35 Change User Setting page - 450 Platform Family AP/ SM/BH



Attribute	Meaning

Update Password tab	This tab provides a drop-down list of configured users from which a user is selected to change password.
Update Mode tab	This tab facilitates to convert a configured user to a Read-Only user.
General Status Permission tab	This tab enables and disables visibility of **General Status Page** for all Guest users. 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 20 AP Evaluation Configuration parameter of Security tab for PMP**  **Figure 21 BHM Evaluation Configuration parameter of Security tab for PTP** 

Users account

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

The Users page is explained in Table 36.

Table 36 User page –450 Platform Family 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 on page 3-89

Isolating from the internet – APs/BHMs

Applicable products	PMP:	☑ AP	PTP:	☑ BHM

See Isolating AP/BHM from the Internet in Planning and Installation Guide.

Encrypting radio transmissions

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

See Encryption radio transmission in Planning and Installation Guide.

Requiring SM Authentication

Applicable products	**PMP:**	☑	AP	☑	SM

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

For descriptions of each of the configurable security parameters on the AP, see Configuring Security on page 1-125. For descriptions of each of the configurable security parameters on the SM, see Security page – 450 Platform Family BHM on page 1-130.

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

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

  For more information on configuring the PMP 450 Platform network to utilize a RADIUS server, see Configuring a RADIUS server on page 1-275.

Filtering protocols and ports

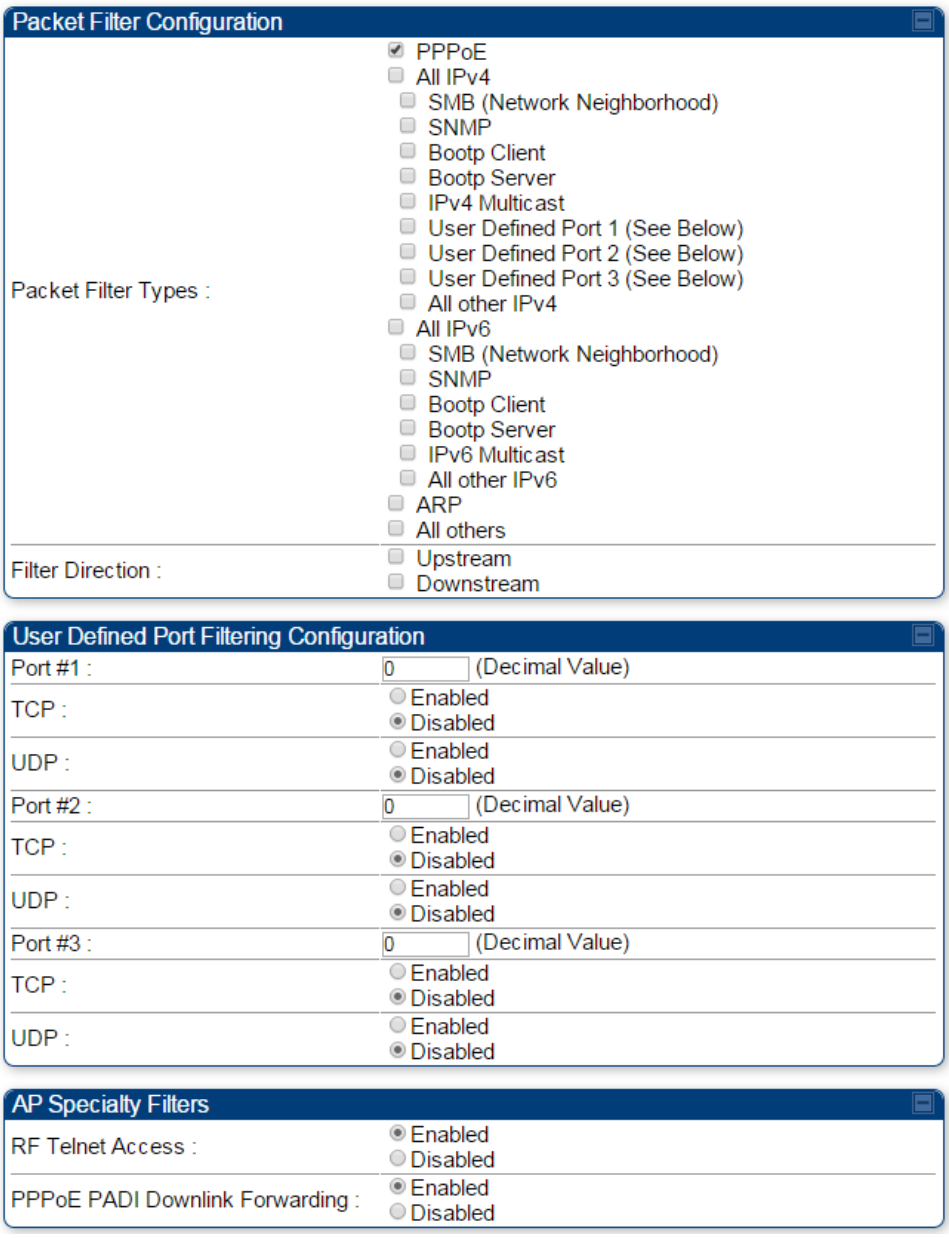
Applicable products	PMP: ☑ AP ☑ SM	PTP: ☑ BHM ☑ BMS

The filtering protocols and ports allows to configure filters for specified protocols and ports from leaving the AP/SM/BHM/BHS and entering the network. See Filtering protocols ans ports in Planning and Installation Guide.

Protocol filtering page of 450 Platform Family AP/BHM

The Protocol Filtering page of 450 Platform Family - AP/BHM is explained in Table 37.

Table 37 AP/BHM Protocol Filtering attributes

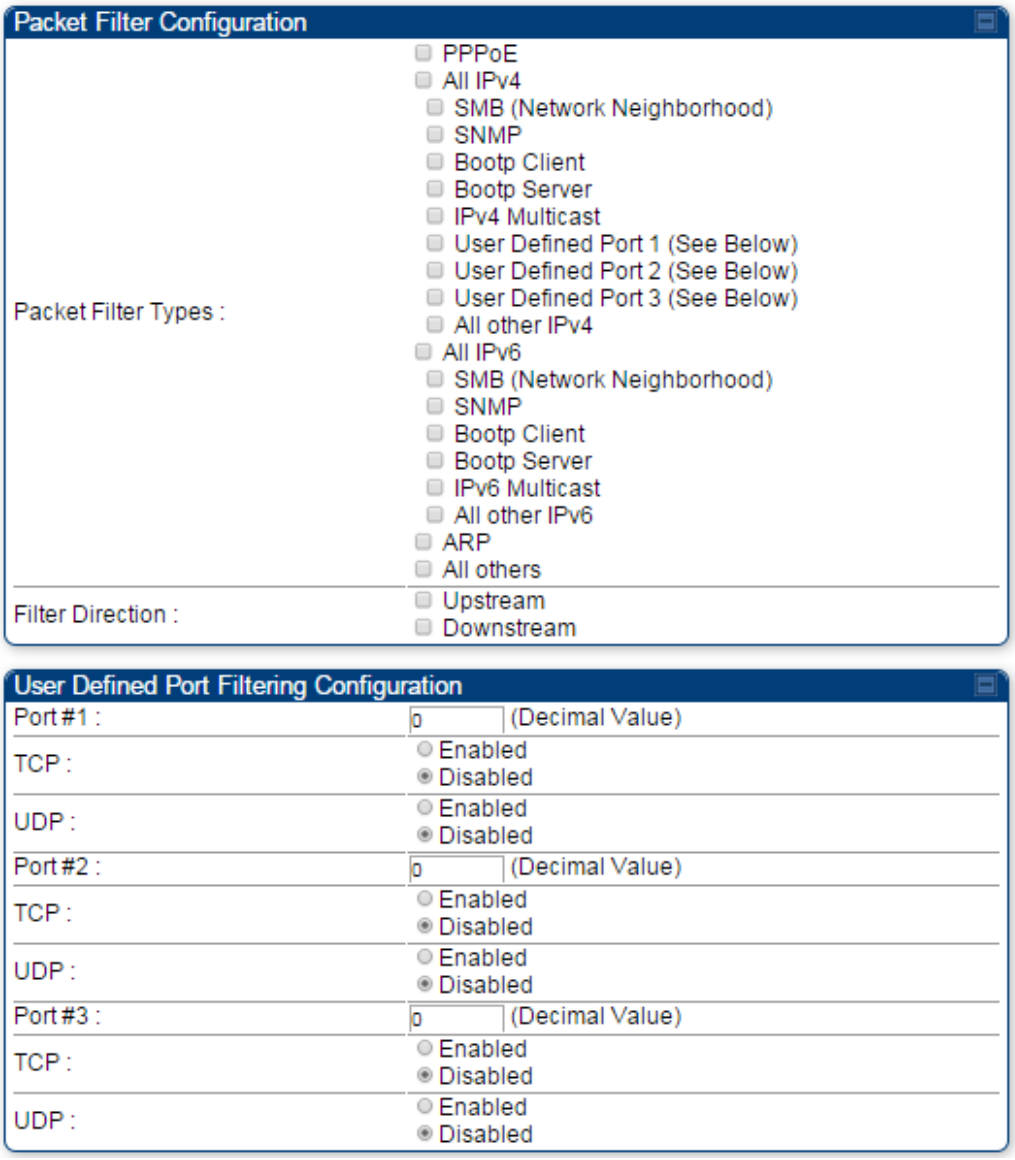


Attribute	Meaning
Packet Filter Types	For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type. To filter packets in any of the user-defined ports, must do all of the following: Check the box for **User Defined Port *n* (See Below)** in the **Packet Filter Types** 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 38.

Table 38 SM/BHS Protocol Filtering attributes



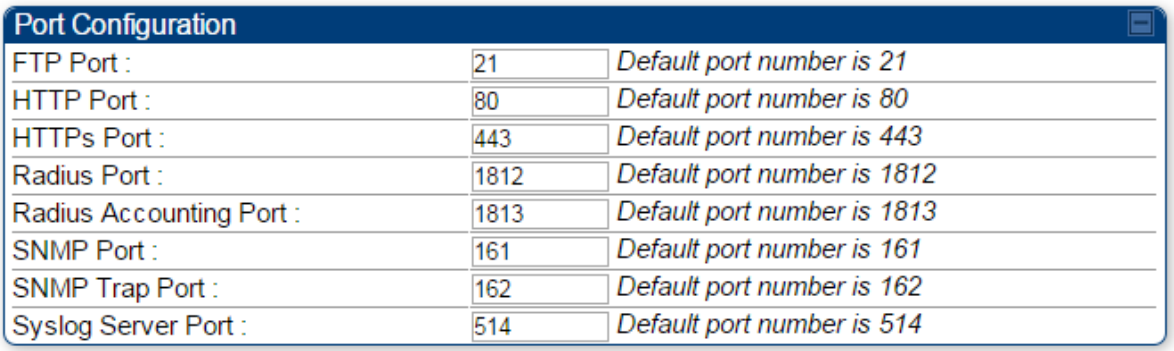
Attribute	Meaning
Packet Filter Configuration tab	See Table 37 AP/BHM Protocol Filtering attributes on page 1-115
User Defined Port Filtering Configuration tab	See Table 37 AP/BHM Protocol Filtering attributes on page 1-115

Port configuration

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

The **Port Configuration** page of the AP/SM/BHM/BHS is explained in Table 39.

Table 39 Port Configuration attributes – AP/SM/BHM/BMS



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

Encrypting downlink broadcasts

See Encryption downlink broadcast in Installation and Planning Guide.

Isolating SMs

See Isolating SMs in Installation and Planning Guide.

Filtering management through Ethernet

See Filtering management through Ethernet in Installation and Planning Guide.

Allowing management only from specified IP addresses

See Allowing management only from specified IP address in Installation and Planning Guide.

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.

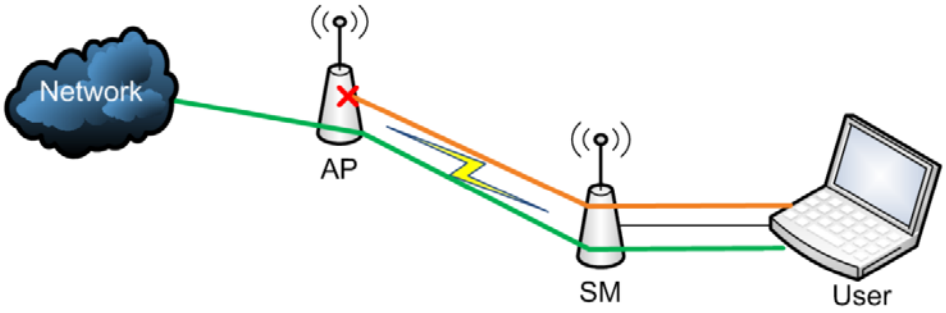
The RF Telnet Access may be configured via the AP GUI or via SNMP commands, and RF Telnet Access is set to “Enabled” by default. Once RF Telnet Access is set to “Disabled”, if there is a Telnet session attempt to the AP originating from a device situated below the SM (or any downstream device), the attempt 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 22).

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

Figure 22 RF Telnet Access Restrictions (orange) and Flow through (green)



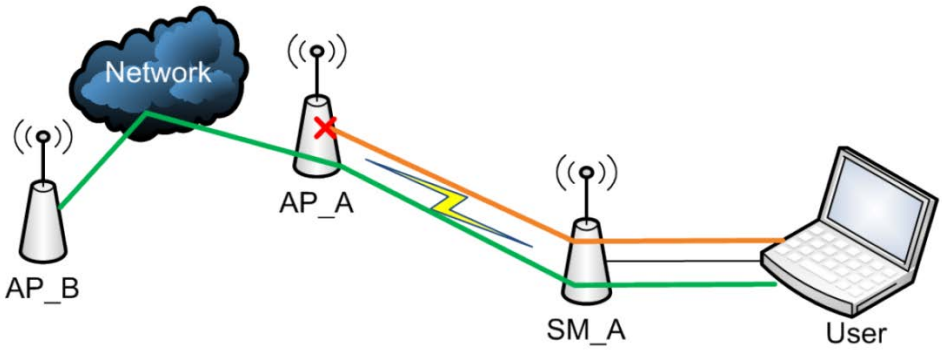
Key Security Considerations when using the RF Telnet Access Feature

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

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

Figure 23 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.

2. Restricting AP RF Telnet Access

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

3. Controlling RF Telnet Access via the AP GUI

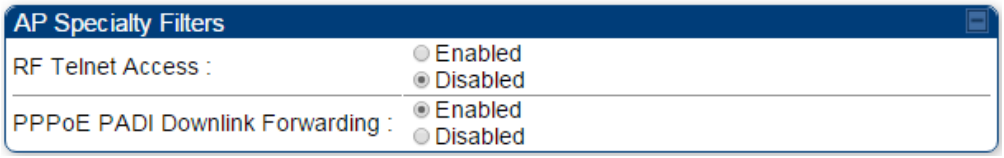
To restrict all Telnet access to the AP via the RF interface from downstream devices, follow these instructions using the AP GUI:

Procedure 12 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**



4 Click the **Save** button

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

Note

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

Configuring SNMP Access

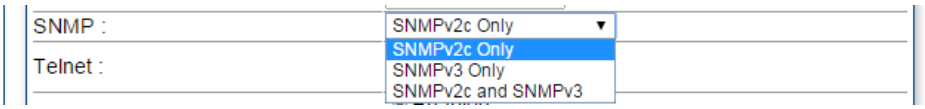
The SNMPv3 interface provides a more secure method to perform SNMP operations. This standard provides services for authentication, data integrity and message encryption over SNMP. Refer to Planning of SNMPv3 operation in Planning and Installation Guide.

Note

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

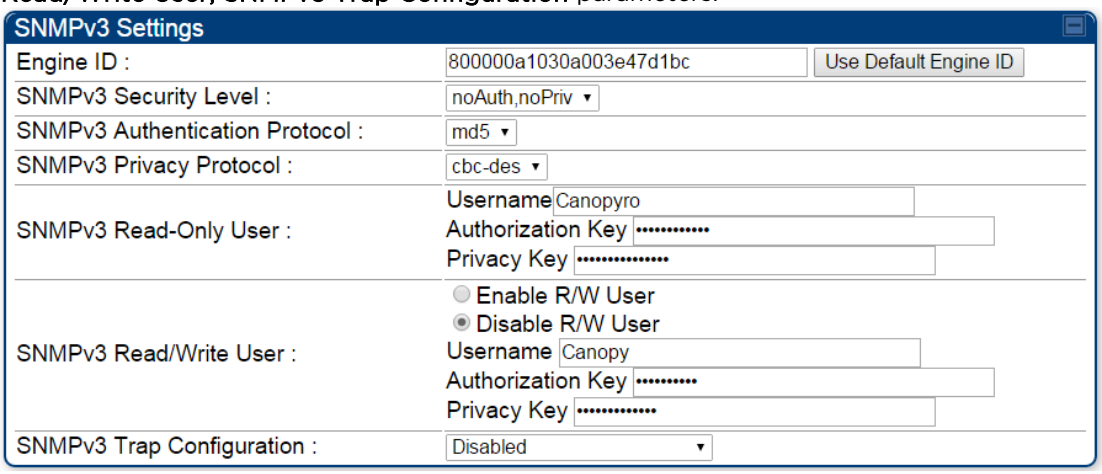
Procedure 13 Configuring SNMPv3

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**



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:



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 follows the guidelines of the SNMPEngineID defined in the SNMP-FRAMEWORK-MIB (RFC 3411). The default Engine ID is the MAC address of the device.

SNMPv3 security level, Authentication and Privacy Protocol

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

SNMPv3 Read-Only and Read/Write User

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

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

SNMPv3 Trap Configuration

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

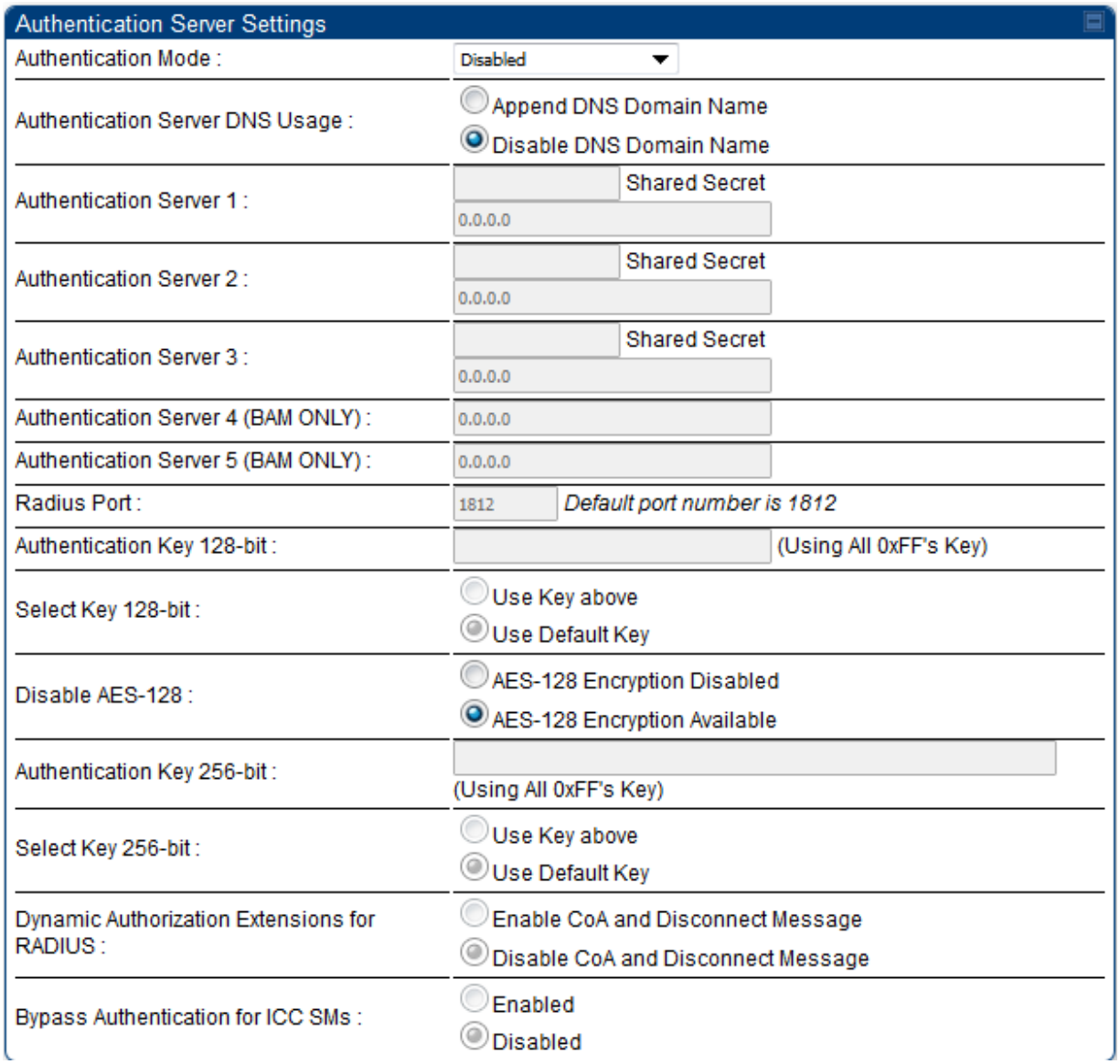
Configuring Security

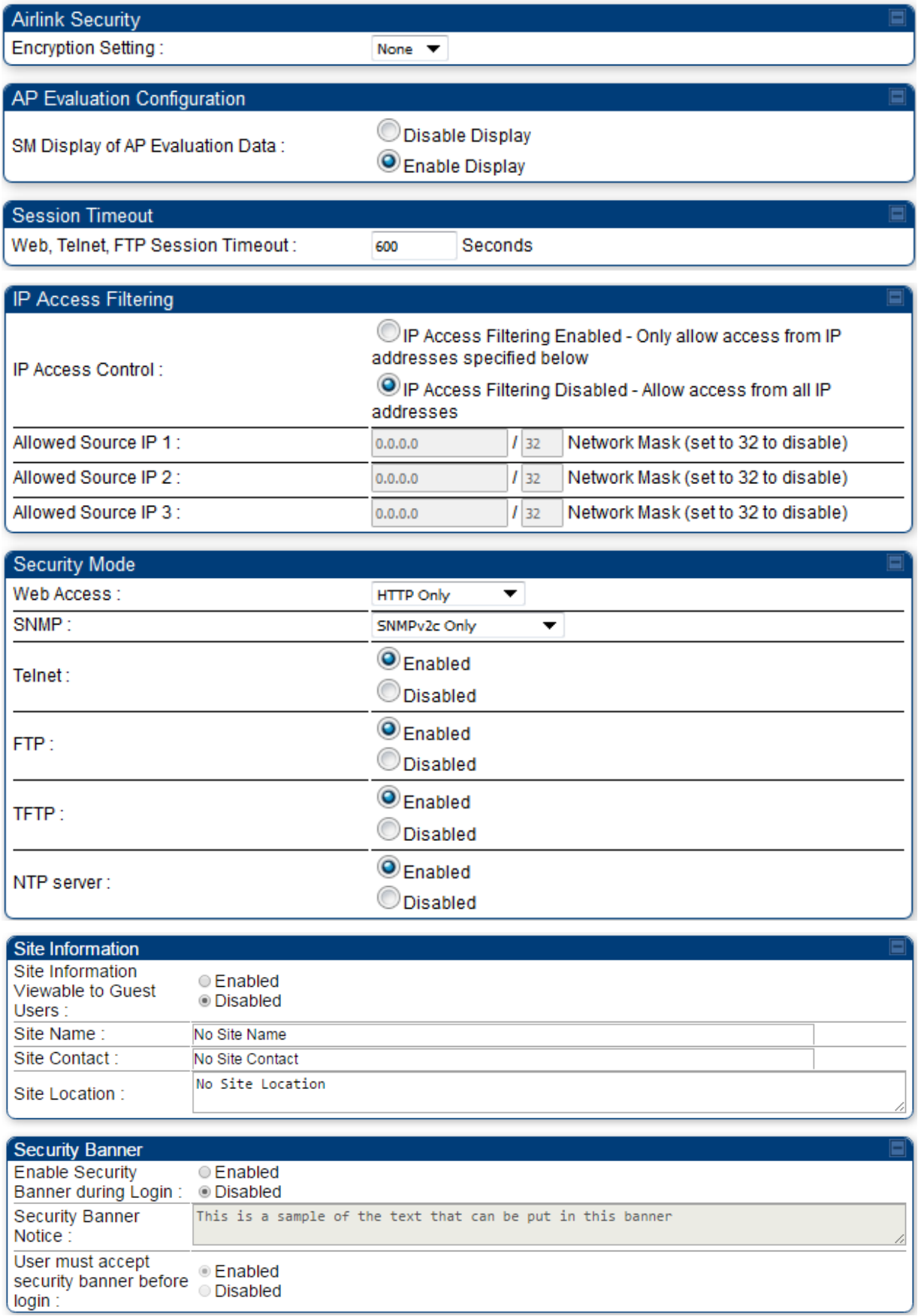
Applicable products	PMP: ☑ AP ☑ SM	PTP: ☑ BHM ☑ BMS

Security page – 450 Platform Family AP

The security page of AP is explained in Table 40.

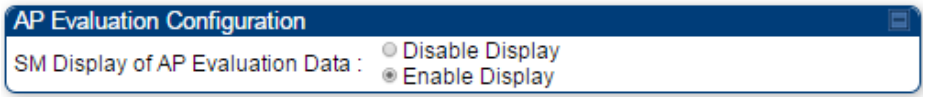
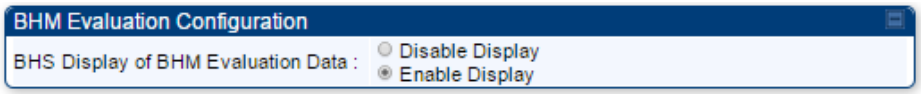
Table 40 Security attributes –450 Platform Family AP




Airlink Security
Encryption Setting :
None
AP Evaluation Configuration
SM Display of AP Evaluation Data :
Disable Display
Enable Display
Session Timeout
Web, Telnet, FTP Session Timeout :
600
Seconds
IP Access Filtering
IP Access Control :
IP Access Filtering Enabled - Only allow access from IP addresses specified below
IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :
0.0.0.0
/ 32
Network Mask (set to 32 to disable)
Allowed Source IP 2 :
0.0.0.0
/ 32
Network Mask (set to 32 to disable)
Allowed Source IP 3 :
0.0.0.0
/ 32
Network Mask (set to 32 to disable)
Security Mode
Web Access :
HTTP Only
SNMP :
SNMPv2c Only
Telnet :
Enabled
Disabled
FTP :
Enabled
Disabled
TFTP :
Enabled
Disabled
NTP server :
Enabled
Disabled
Site Information
Site Information Viewable to Guest Users :
Enabled
Disabled
Site Name :
No Site Name
Site Contact :
No Site Contact
Site Location :
No Site Location
Security Banner
Enable Security Banner during Login :
Enabled
Disabled
Security Banner Notice :
This is a sample of the text that can be put in this banner
User must accept security banner before login :
Enabled
Disabled

Attribute	Meaning
Authentication Mode	Operators may use this field to select from among the following authentication modes: **Disabled**—the AP requires no SMs to authenticate. (Factory default). **Authentication Server** —the AP/BHM requires any SM/BHS that attempts registration to be authenticated in Wireless Manager before registration. **AP PreShared Key** - The AP/BHM acts as the authentication server to its SMs/BHS and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP/BHM and all SMs/BHS desired to register to that AP/BHM. There is also an option of leaving the AP/BHM and SMs/BHS at their default setting of using the "Default Key". Due to the nature of the authentication operation, if you want to set a specific authentication key, then you MUST configure the key on all of the SMs/BHS and reboot them BEFORE enabling the key and option on the AP/BHM. Otherwise, if you configure the AP/BHM first, none of the SMs/BHS is able to register. **RADIUS AAA** - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.
Authentication Server DNS Usage	The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.
Authentication Server *1 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.
Radius Port	This field allows the operator to configure a custom port for RADIUS server communication. The default value is *1812*.
Authentication Key 128-bit	This 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.
Select Key 128-bit	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 the SM's MAC address) is used for authentication

Disable AES 128-bit	This option allows to disable the AES-128 encryption. When AES-128 Encryption is disabled, it prevents the use of AES-128 when encryption is enabled. Since changes to other attributes (e.g. PreSharedKey authentication settings) could cause a need for 128-bit Auth and AES-128 upon next registration, Disable AES 128-bit parameter is prevented from being changed on the "Security" webpage while the "Reboot Required" warning is present at the top of the Web GUI pages. The recommendation is to complete other changes first and to ensure that all links at an AP are running AES-256 before disabling the use of AES-128 on all units (AP and SMs) in the sector. When saving and loading a configuration file, Disable AES 128 is saved and loaded as a normal attribute. It will not take effect until a reboot is triggered. Since enabling this attribute could have the effect of preventing a link coming up, care should be taken on networks that enable this attribute on only some units. Select one of the following options to either disable or use AES-128 encryption. • AES-128 Encryption Disabled: • AES-128 Encryption Available
Authentication Key 256-bit	This authentication key is a 64-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF. **Note** The AES-256 parameters are visible only when the feature key is purchased.
Select Key 256-bit	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** The AES-256 parameters are visible only when the feature key is purchased.
Dynamic Authorization Extensions for RADIUS	**Enable CoA and Disconnect Message**: Allows to control configuration parameters of SM using RADIUS CoA and Disconnect Message feature. **Disable CoA and Disconnect Message**: Disables RADIUS CoA and Disconnect Message feature. To enable CoA and Disconnect feature, the Authentication Mode should be set to RADIUS AAA.

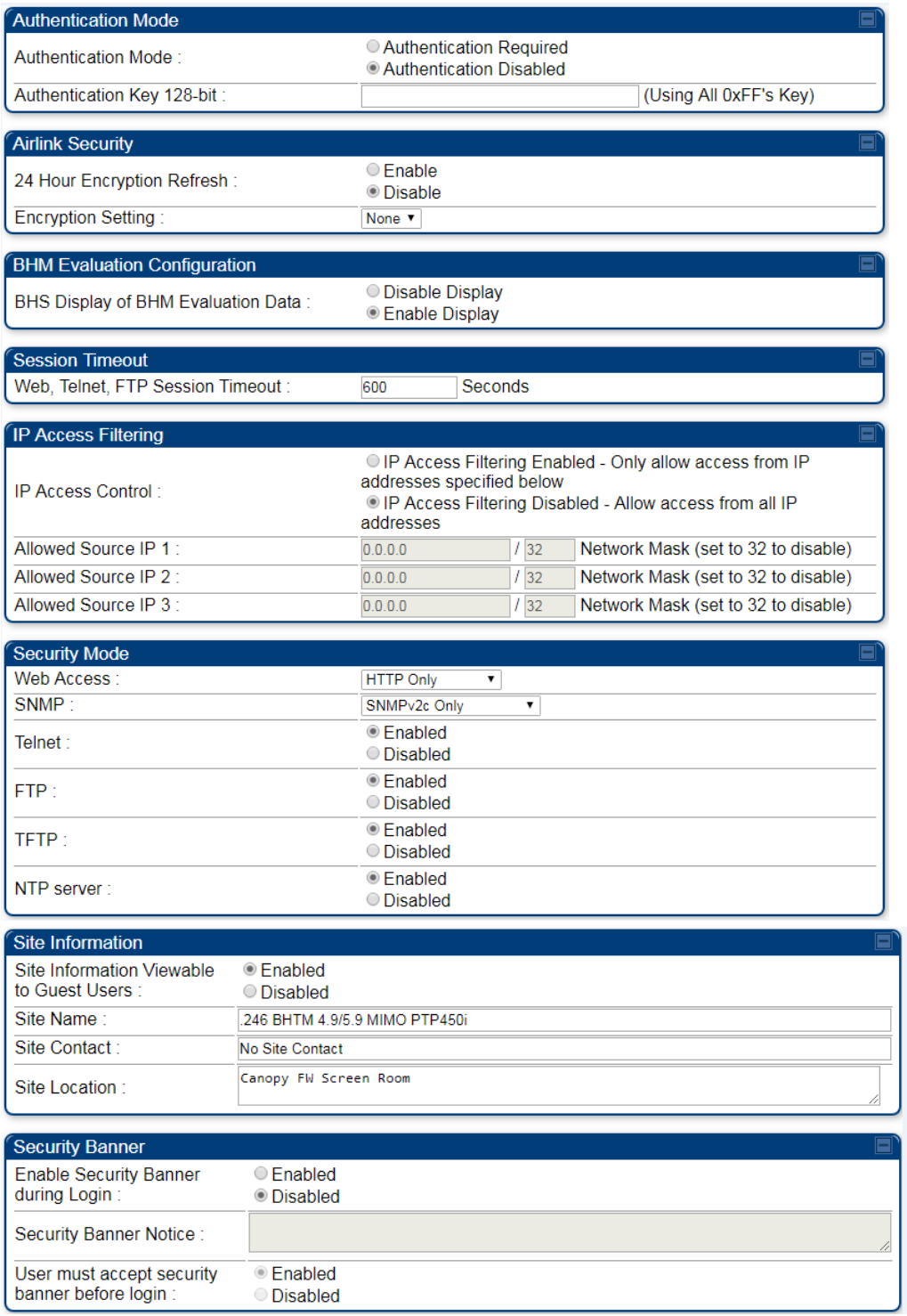
Bypass Authentication for ICC SMs	**Enabled**: SM authentication is disabled when SM connects via ICC (Installation Color Code). **Disabled**: SM authentication is enabled.
Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. **None** provides no encryption on the air link. **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. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A. **Note** This parameter is applicable to BHM.
SM Display of AP Evaluation Data Or BHS Display of BHM Evaluation Data	Allows operators to suppress the display of data about this AP/BHM on the AP/BHM Evaluation tab of the Tools page in all SMs/BHS that register. The factory default setting for SM Display of AP Evaluation Data or BHS Display of BHM Evaluation Data is enabled display. PMP 450/450i Series – SM display of AP Evaluation Data parameter  PTP 450/450i Series – BHS display of BHM Evaluation Data parameter 
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via **HTTP**, **telnet**, or **ftp** access to the AP/BHM.
IP Access Control	You can permit access to the AP/BHM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address
Allowed Source IP *1 to 3*	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop-down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop-down list: • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is a secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.
NTP Server	This option allows to **Enable** and **Disable** NTP server access to the Radio.
Site Information viewable to Guest Users	This option allows to Enable or Disable displaying site information with Guest users.
Site Name	Specify a string to associate with the physical module.
Site Contact	Enter contact information for the module administrator.
Site Location	Enter information about the physical location of the module.
Enable Security Banner during Login	**Enable**: The Security Banner Notice will be displayed before login. **Disable**: The Security Banner Notice will not be displayed before login.
Security Banner Notice	User can enter ASCII (0-9a-zA-Z newline, line-feed are allowed) text up-to 1300 characters.
User must accept security banner before login	**Enable**: login area (username and password) will be disabled unless user accepts the security banner. **Disable**: User can't login to radio without accepting security banner.

Security page – 450 Platform Family BHM

The security page of AP/BHM is explained in Table 41.

Table 41 Security attributes –450 Platform Family BHM



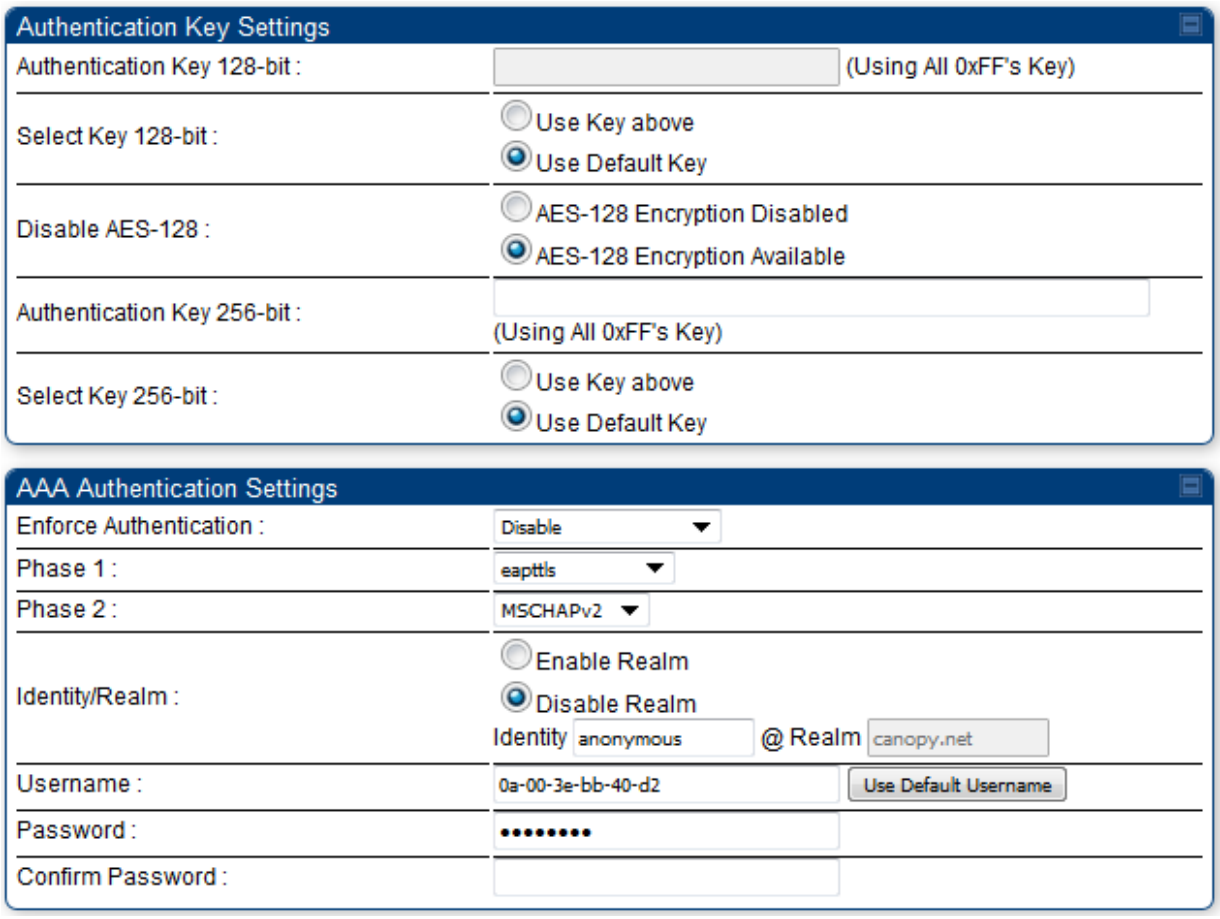
Attribute	Meaning
Authentication Mode	Operators may use this field to select from among the following authentication modes: Authentication Required: the BHS requires to be authenticated. Authentication Disabled: the BHM requires no BHS to authenticate. (Factory default).
Authentication Key 128-bit	Refer Table 40 Security attributes –450 Platform Family AP on page 1-125 for parameter details
24 Hour Encryption Refresh	Operators may use this field to select from among the following options: Enabled: Allows BHS re-registration every 24 hours. Disabled: Disables 24-hour encryption refresh. This parameter is disabled by default.
Encryption Setting	Refer Table 40 Security attributes –450 Platform Family AP on page 1-125 for parameter details
BHS Display of BHM Evaluation Data	
Web, Telnet, FTP Session Timeout	
IP Access Control	
Allowed Source IP 1 to 3	
Web Access	
SNMP	
Telnet	
FTP	
TFTP	
NTP Server	
Site Information viewable to Guest Users	Refer Table 40 Security attributes –450 Platform Family AP on page 1-125 for parameter details
Site Name	
Site Contact	
Site Location	
Enable Security Banner during Login	

Security Banner Notice	
User must accept security banner before login	

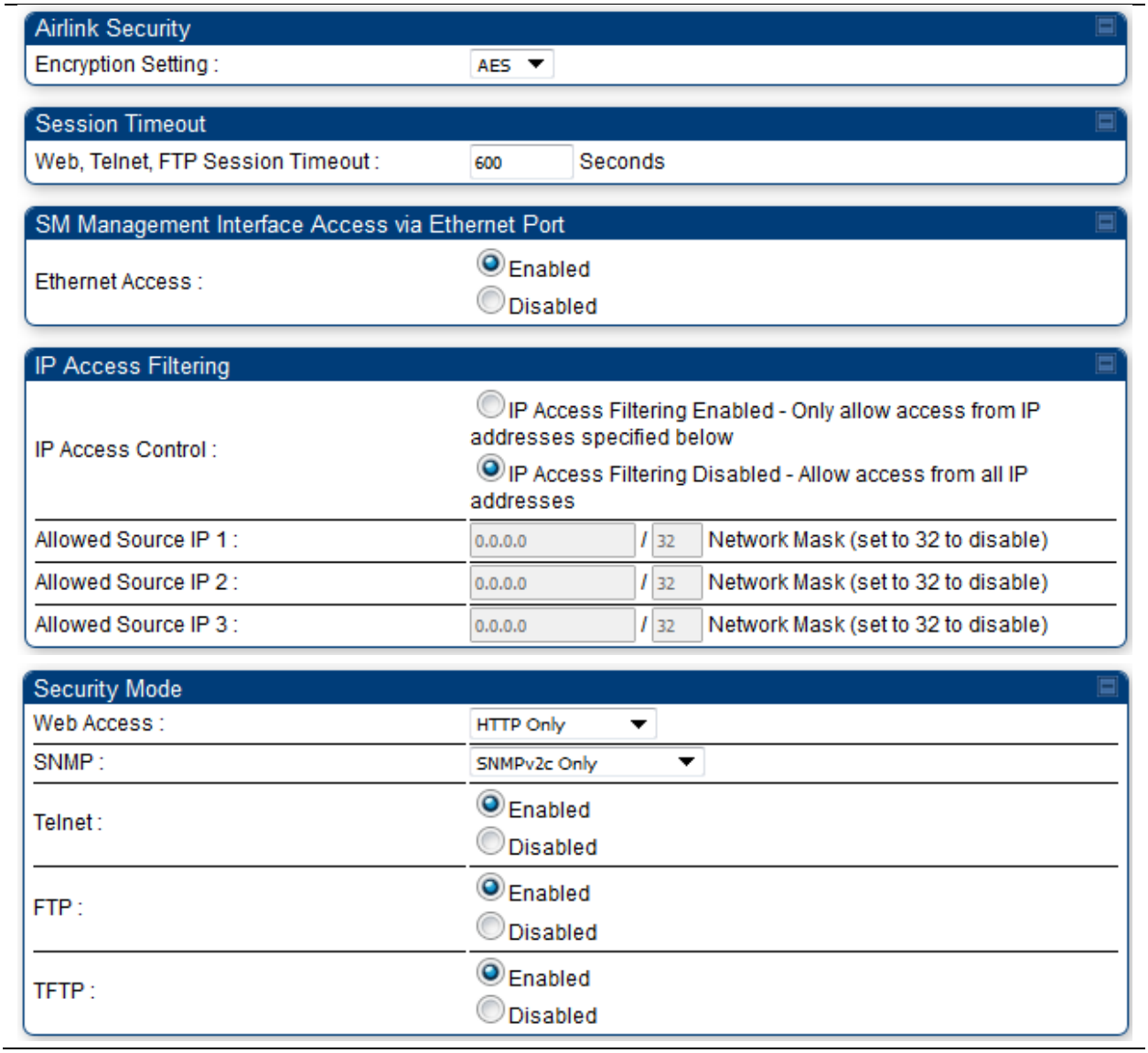
Security page - 450 Platform Family SM

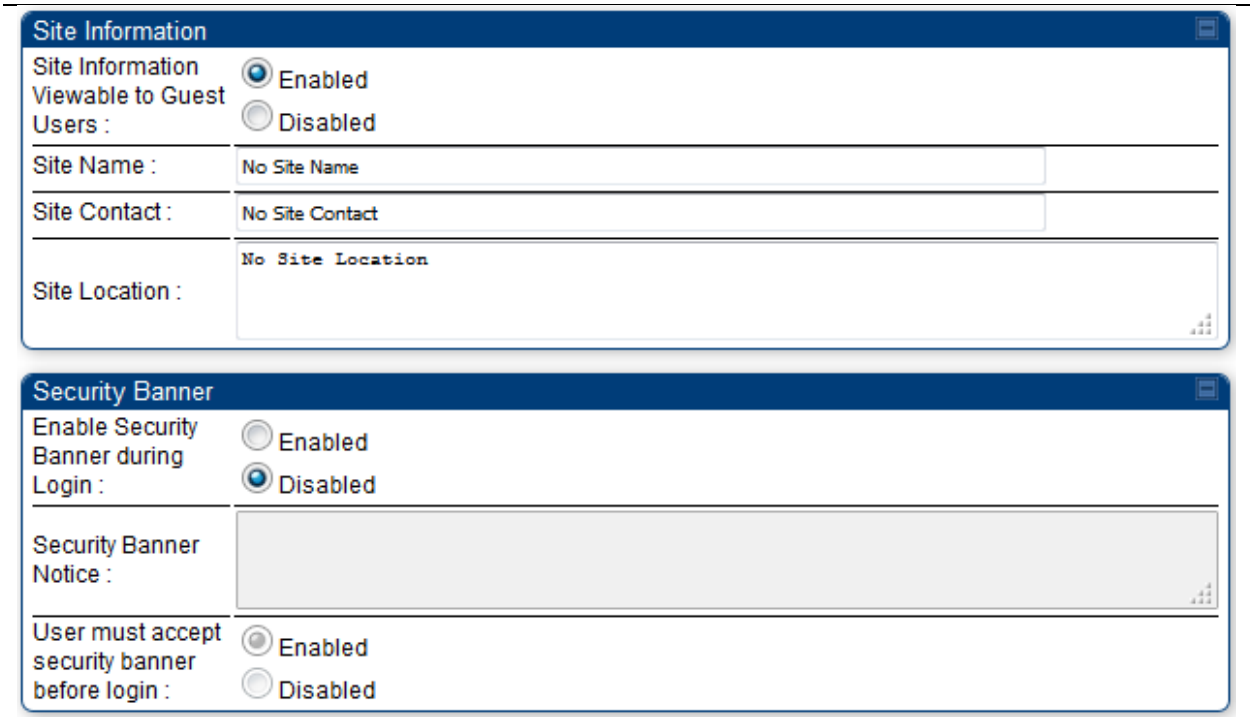
The security page of 450 Platform Family SM is explained in Table 42.

Table 42 Security attributes –450 Platform Family SM




RADIUS Certificate Settings
Upload Certificate File
File: Browse... No file selected.
Import Certificate
Use Default Certificates
This will delete all current certificates
Certificate 1
C =US
S =Illinois
O =Motorola Solutions, Inc.
OU =Canopy Wireless Broadband
CN =Canopy AAA Server Demo CA
E =technical-support@canopywireless.com
Valid From: 01/01/2001 00:00:00
Valid To: 12/31/2049 23:59:59
Delete
Certificate 2
C =US
S =Illinois
O =Motorola, Inc.
OU =Canopy Wireless Broadband
CN =PMP320 Demo CA
Valid From: 07/01/2009 06:00:00
Valid To: 12/31/2049 23:59:59
Delete


Airlink Security
Encryption Setting :
AES
Session Timeout
Web, Telnet, FTP Session Timeout :
600
Seconds
SM Management Interface Access via Ethernet Port
Ethernet Access :
Enabled
Disabled
IP Access Filtering
IP Access Control :
IP Access Filtering Enabled - Only allow access from IP addresses specified below
IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :
0.0.0.0
/ 32
Network Mask (set to 32 to disable)
Allowed Source IP 2 :
0.0.0.0
/ 32
Network Mask (set to 32 to disable)
Allowed Source IP 3 :
0.0.0.0
/ 32
Network Mask (set to 32 to disable)
Security Mode
Web Access :
HTTP Only
SNMP :
SNMPv2c Only
Telnet :
Enabled
Disabled
FTP :
Enabled
Disabled
TFTP :
Enabled
Disabled



Attribute	Meaning
Authentication Key 128-bit	Only if the AP to which this SM will register requires authentication, specify the 128-bit key that the SM will use when authenticating. For alpha characters in this 32-character hex key, use only upper case.
Select Key 128-bit	Refer Table 40 Security attributes –450 Platform Family AP on 1-125 for parameter details.
Disable AES 128-bit	
Authentication Key 256-bit	
Select Key 256-bit	
Enforce Authentication	The SM may enforce authentication types of **AAA** and **AP Pre-sharedKey**. The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM locks out the AP for 15 minutes).
Phase 1	The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

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

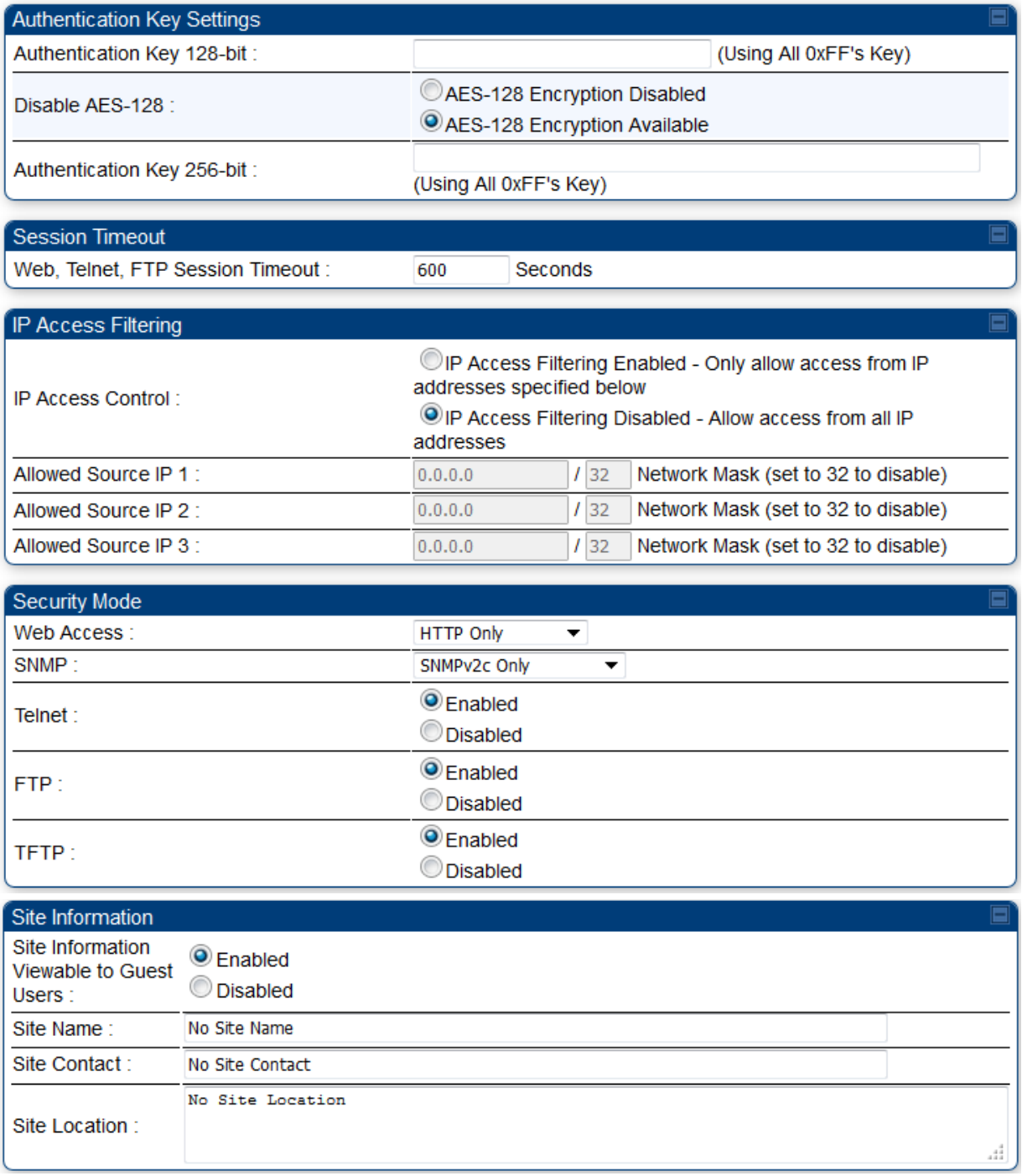
Encryption Setting	Specify the type of airlink security to apply to this SM. The encryption setting must match the encryption setting of the AP. **None** provides no encryption on the air link. **AES** (Advanced Encryption Standard)**:** An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet, or FTP access to the SM.
Ethernet Access	If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select **Ethernet Access Disabled**. This selection disables access through this port to via HTTP (the GUI), SNMP, telnet, FTP, and TFTP. With this selection, management access is available through only the RF interface via either an IP address (if **Network Accessibility** is set to **Public** on the SM) or the Session Status or Remote Subscribers tab of the AP.  **Note** This setting does not prevent a device connected to the Ethernet port from accessing the management interface of other SMs in the network. To prevent this, use the IP Access Filtering Enabled selection in the IP Access Control parameter of the SMs in the network. See IP Access Control below. If you want to allow management access through the Ethernet port, select **Ethernet Access Enabled**. This is the factory default setting for this parameter.
IP Access Control	You can permit access to the SM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address
Allowed Source IP *1 to 3*	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the SM from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop-down list:

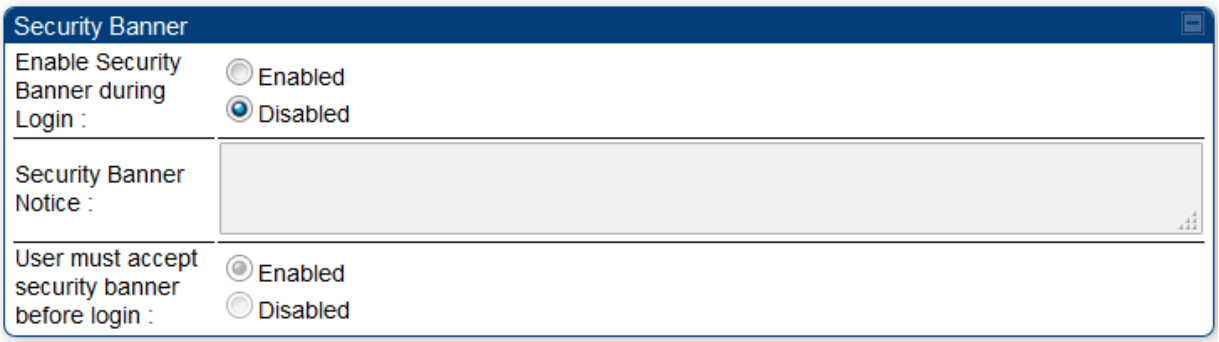
	• **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop-down list : • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.
Site Information viewable to Guest Users	This option allows to Enable or Disable displaying site information with Guest users.
Site Name	Specify a string to associate with the physical module.
Site Contact	Enter contact information for the module administrator.
Site Location	Enter information about the physical location of the module.
Enable Security Banner during Login	**Enable**: The Security Banner Notice will be displayed before login. **Disable**: The Security Banner Notice will not be displayed before login.
Security Banner Notice	User can enter ASCII (0-9a-zA-Z newline, line-feed are allowed) text up-to 1300 characters.
User must accept security banner before login	**Enable**: login area (username and password) will be disabled unless user accepts the security banner. **Disable**: User can't login to radio without accepting security banner.

Security page –450 Platform Family BHS

The Security page of 450 Platform Family BHS is explained in Table 43.

Table 43 Security attributes - 450 Platform Family BHS





Attribute	Meaning
Authentication Key	Only if the BHM to which this BHS registers requires an authentication, specify the key that the BHS will use when authenticating. For alpha characters in this hex key, use only upper case.
Disable AES 128-bit Authentication Key 256-bit	Refer Table 40 Security attributes –450 Platform Family AP on 1-125 for parameter details.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet, or FTP access to the BHS.
IP Access Control	You can permit access to the BHS from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address
Allowed Source IP *1 to 3*	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the BHS from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop-down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.

SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop-down list: • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.
Site Information viewable to Guest Users	Refer Table 40 Security attributes –450 Platform Family AP on 1-125 for parameter details.
Site Name	
Site Contact	
Site Location	
Enable Security Banner during Login	
Security Banner Notice	
User must accept security banner before login	

Configuring 802.1X authentication

IEEE 802.1x standard defines a client and server-based access control and authentication protocol. This protocol restricts unauthorized clients from connecting to a LAN through publicly accessible ports.

The authentication server authenticates each client connected to SM's ethernet port and enables the port before making available any services offered by the SM, AP, and the network. Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPoL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

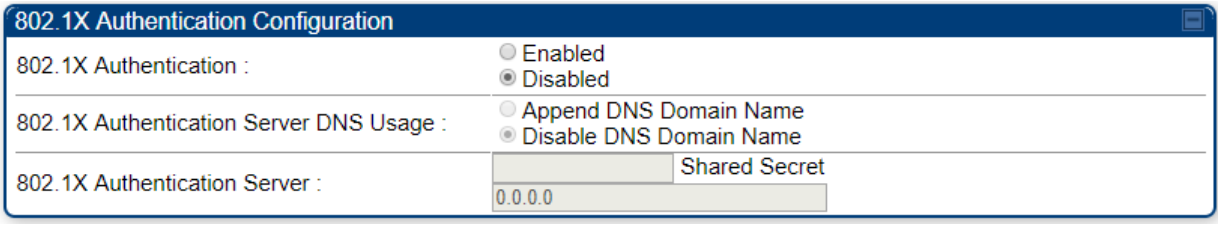
Two types of authentication mode are supported:

- **Port based authentication**: This mode needs to be used when single host is connected to the SM. If the authentication is successful by the host connected to the SM, SM port is enabled, and all traffic will pass through.
- **MAC Address Based Authentication:** This mode needs to be used when multiple hosts are connected to the SM. Each host needs to be authenticated by 802.1X protocol to access the network. The traffic is filtered based on the source MAC Address of the host, only the traffic from authenticated host will be allowed to access the network.

802.1X authentication page of AP

The 802.1X Authentication page of AP is explained in Table 44.

Table 44 802.1X authentication attributes –450 Platform Family AP

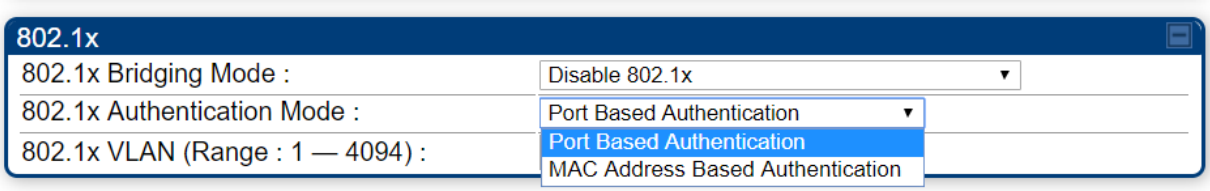


Attribute	Meaning
802.1X Authentication	This parameter is used to enable or disable 802.1Xauthentication. It is disabled by default.
802.1X Authentication Server DNS Usage	This parameter is enabled when server address is in fully qualified domain name format.
Shared Secret	This parameter specifies the the shared secret which is configured for this client on RADIUS server. Maximum length of this parameter is 32 characters.
802.1X Authentication Server	This parameter specifies either a dotted decimal notation (IP address) or fully qualified domain name (www.google.com). Maximum length of this parameter is 256 characters.

802.1x authentication page of SM

The 802.1X Authentication page of SM is explained in Table 45.

Table 45 802.1X authentication attributes –450 Platform Family SM



Attribute	Meaning
802.1x Bridging Mode	This parameter specifies the bridging mode used by SM. It is disabled by default. Following are the available options for this parameter. • **Disable 802.1x:** Disable 802.1x authentication. • **Require 802.1x for all traffic:** 802.1x authentication should be successful for any traffic to pass through the SM (i.e. Authenticator). • **Require 802.1x for all non-management traffic:** Management traffic will be allowed to pass through the SM without 802.1x Authentication.
802.1x Authentication Mode	This parameter specifies the authentication mode used by SM. • **Port Based Authentication:** SM port is activated once the 802.1x authentication is successful. This configuration needs to be used when single host is connected behind SM. If authentication is successful, SM port is enabled, and all traffic will pass through. • **MAC Address Based Authentication:** This option needs to be used when multiple hosts are connected behind an SM. Each host needs to be authenticated by 802.1x protocol to access the network. The traffic is filtered based on the source MAC address of the host, only the traffic from authenticated host will be allowed to access the network.
802.1x VLAN (Range : 1 — 4094)	This parameter specifies the number of VLAN configurations. It ranges from 1 to 4094. VLAN configuration is used for sending 802.1x packet on the configured VLAN. If a customer excepts EAPoL packets on a VLAN, customer needs to configure the VLAN. Once VLAN is configured, all EAPoL packets are exchanged on the configured VLAN. VLAN 1 is the default configuration which is equivalent to untagged traffic.

Configuring radio parameters

PMP 450m Series – configuring radio

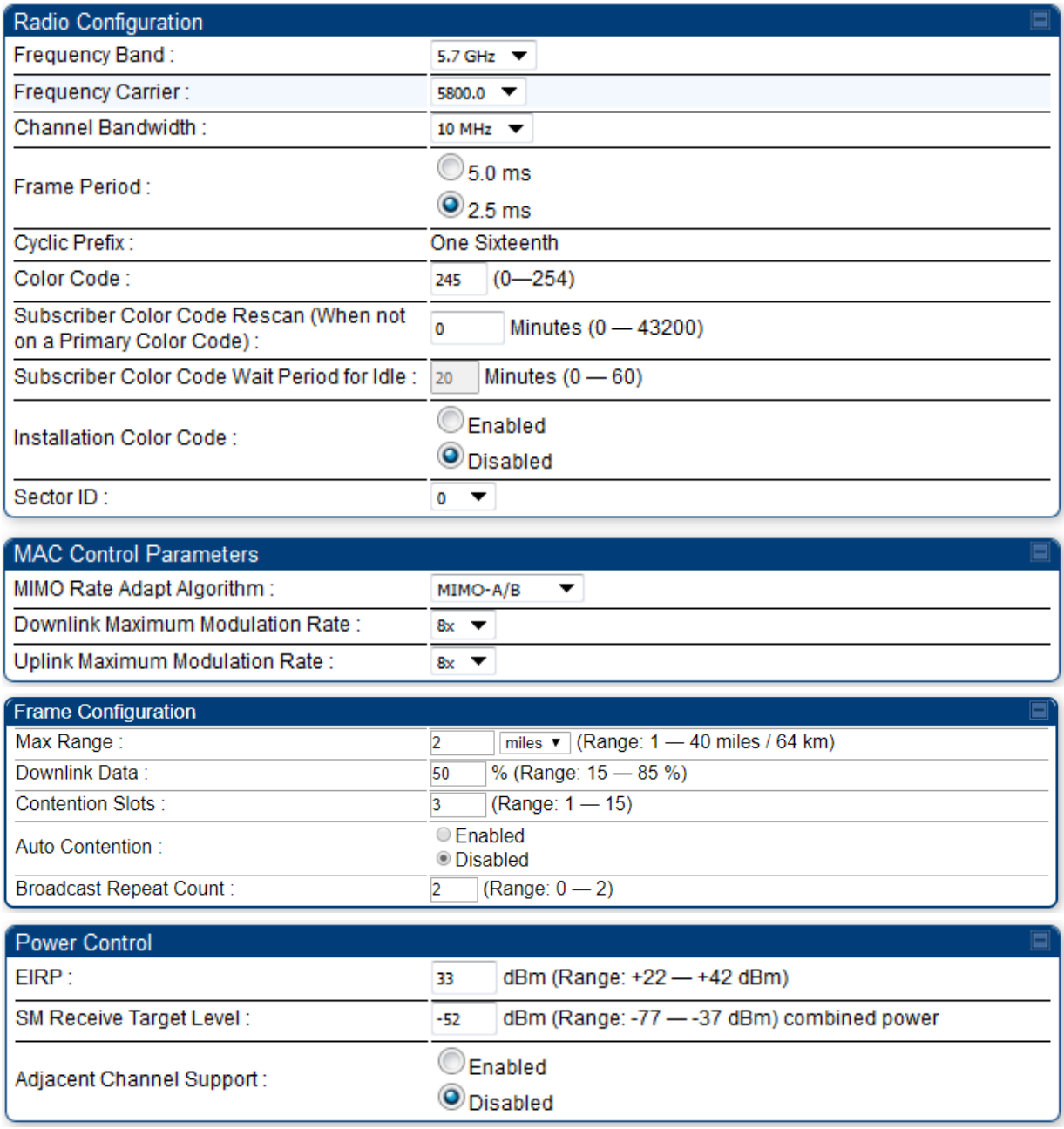
Radio page - PMP 450m AP 5 GHz

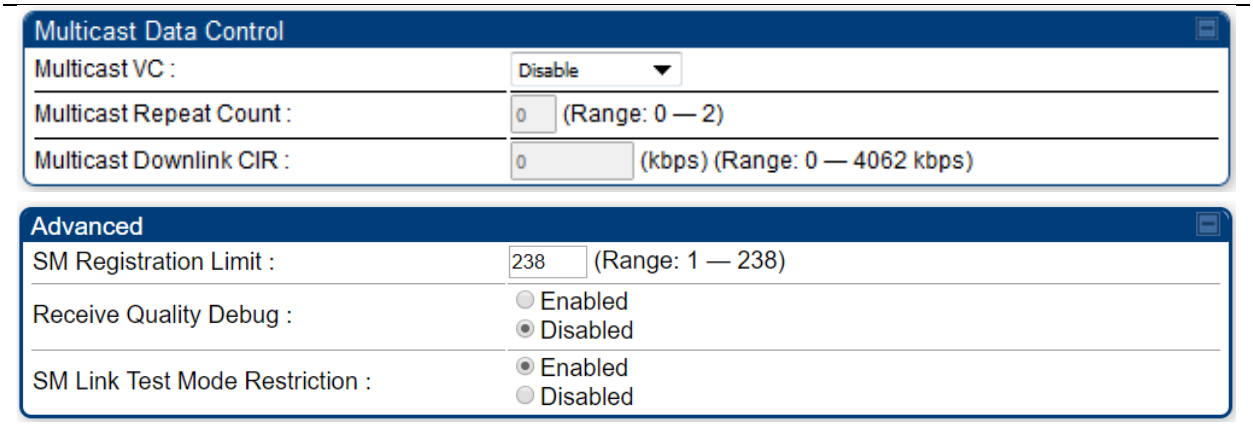
The **Radio** tab of the PMP 450m AP contains some of the configurable parameters that define how an AP operates.

Note

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

Table 46 PMP 450m AP Radio attributes - 5 GHz





Attribute	Meaning
Frequency Band	Select the desired operating frequency band.
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is **None**. For a list of channels in the band, see the drop-down list on the radio GUI.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM. The supported Channel Bandwidths are 5 MHz, 10 MHz, 15 MHz, 20 MHz, 30 MHz, and 40 MHz. **Note:** 40 MHz is not supported on PMP 450 AP, but is supported on PMP 450 SMs.
Frame Period	Select the Frame Period of the radio. The supported Frame Periods are: 5 ms and 2.5 ms.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Color Code	Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
Subscriber Color Code Rescan (When not on a Primary Color Code)	This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code.

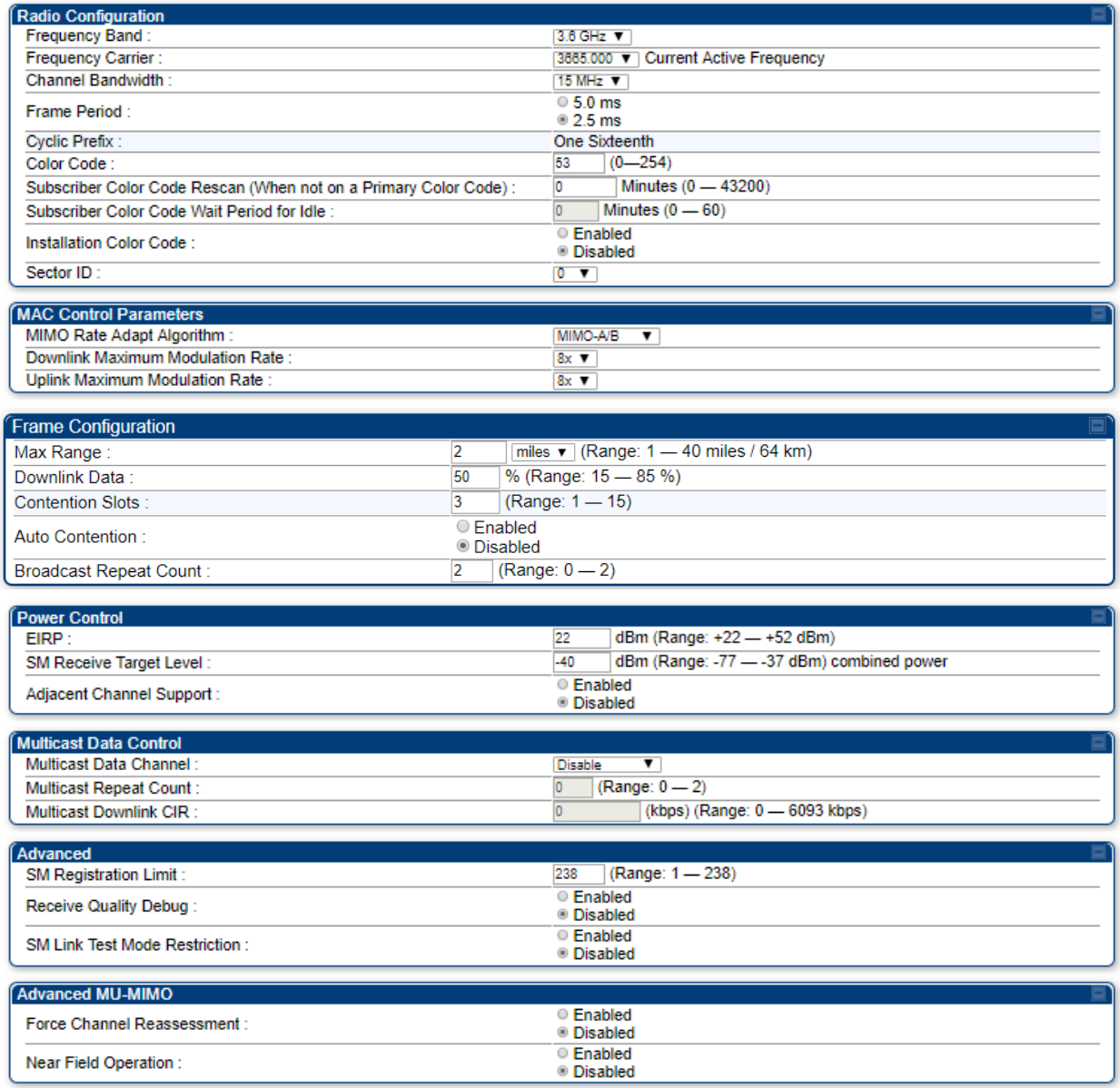
	The time (in minutes) for a subscriber to rescan (if this AP is not configured with the SM's primary color code). This timer will only fire once – if the **Subscriber Color Code Wait Period for Idle** timer is configured with a nonzero value and the **Subscriber Color Code Rescan** expires, the **Subscriber Color Code Wait Period for Idle** is started. If the **Subscriber Color Code Wait Period for Idle** timer is configured with a zero value and the **Subscriber Color Code Rescan** timer expires, the SM will immediately go into rescan mode
Subscriber Color Code Wait Period for Idle	The time (in minutes) for a subscriber to rescan while idle (if this AP is not configured with the SM's primary color code). This timer will fire periodic events. The fired event determines if any RF unicast traffic (either inbound or outbound) has occurred since the last event. If the results of the event determine that no RF unicast traffic has occurred (SM is idle), then the subscriber will rescan.
Installation Color Code	With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. When using the Installation Color Code feature, ensure that the SM is configured with the factory default Color Code configuration (Color Code 1 is "0", Color Code 2-10 set to "0" and "Disable"). The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message "SM is registered via ICC – Bridging Disabled!" is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If a SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using Rescan APs functionality on the AP Eval page).
Sector ID	This pull-down menu helps in configuring the Sector ID at a configurable value from 0 to 15.
MIMO Rate Adapt Algorithm	This pull-down menu helps in configuring the Rate Adapt Algorithm to MIMO-A/B, MIMO-B only, or MIMO-A only.
Downlink Maximum Modulation Rate	This pull-down menu helps in configuring the Downlink Maximum Modulation Rate at a configurable rate of 1X, 2X, 3X, 4X, 6X, or 8X. The default value is "8X". The Rate Adapt Algorithm does not allow the modulation to go beyond this limit.
Uplink Maximum Modulation Rate	This pull-down menu helps in configuring the Uplink Maximum Modulation Rate at a configurable rate of 1X, 2X, 3X, 4X, 6X, or 8X. The default value is "8X". The Rate Adapt Algorithm does not allow the modulation to go beyond this limit.
Max Range	Enter the number of miles or kilometers for the furthest distance from which a SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance

	• does not increase the power of transmission from the AP. • can reduce aggregate throughput. For example, with a 20 MHz channel and 2.5 ms frame, every additional 2.24 miles reduces the data air time by one symbol (around 1% of the frame). Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. The parameters have to be selected so that there is no overlap between one AP transmitting and another AP receiving. A co-location tool is provided to help with selecting sets of parameters that allow co-location. The default value of this parameter is 2 miles (3.2 km).
Downlink Data	Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 90 Mb, then 75% specified for this parameter allocates 67.5 Mb for the downlink and 22.5 Mb for the uplink. The default for this parameter is 75%. This parameter must be set in the range of 15% - 85%, otherwise the invalid input will not be accepted and the previously-entered valid setting is used.  **Note** In order to prevent self-interference, the frame configuration needs to align which includes Downlink Data, Max Range and Contention slots. For DFS regions, the maximum Downlink % for a 5.4 GHz radio is 75% only.
Contention Slots	This field indicates the number of (reserved) Contention slots configured by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page 1-208.
Broadcast Repeat Count	For PMP systems broadcast packets are not acknowledged. So, they are sent at the lowest modulation rate 1X. This setting adds an automatic retransmission to broadcast packets to give SMs that have poor signal a higher chance to get the packet.
Contention Slots	This field indicates the number of (reserved) Contention slots configured by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page 1-208.
Auto Contention	This filed eliminates the need to configure optimal number of contention slots. When this feature is enabled, AP dynamically adjusts the number of contention slots resulting in improved performance.
EIRP	This field indicates the combined power level at which the AP will transmit, based on the Country Code. It also includes the antenna gain and array gain.
SM Receive Target Level	Each SM's Transmitter Output Power is automatically set by the AP. The AP monitors the received power from each SM, and adjusts each SM's Transmitter Output Power so that the received power at the AP from that SM is not greater what is set in this field. This value represents the transmitted and received power (combined power) perceived on the SM.

Adjacent Channel Support	For some frequency bands and products, this setting is needed if AP is operating on adjacent channels with zero guard band.
Multicast VC	This pull-down menu of the Multicast VC screen helps in configuring multicast packets to be transmitted over a dedicated channel at a configurable rate of 2X, 4X or 6X. The default value is “Disable”. If set to the default value, all multicast packets are transmitted over the Broadcast VC data path. This feature is available only for the PMP 450 Series and is not backward compatible with PMP 430 series of radios.
Multicast Repeat Count	This value is the number of packets that are repeated for every multicast VC packet received on the AP (located under **Radio** tab of **Configuration**). Multicast (like Broadcast) packets go over a VC that is shared by all SMs, so there is no guaranteed delivery. The repeat count is an attempt to improve the odds of the packets getting over the link. If the user has issues with packets getting dropped, they can use this parameter to improve the performance at the cost of the overall throughput possible on that channel. The default value is *0*.
Multicast Downlink CIR	This value is the committed information rate for the multicast downlink VC (located under the **Radio** tab of **Configuration**). The default value is *0* kbps. The range of this parameter is based on the number of repeat counts. The higher the repeat count, the lower the range for the multicast downlink CIR.
Near Field Operation	This parameter is enabled by the Near Field Operation control. This is only available when the EIRP is set to 22 dBm or below. When Near Field Operation is enabled, the Near Field Range is used to apply compensation to the unit’s calibration to support operation in the near field.
SM Registration Limit	This parameter allows to configure the limit for maximum number of SMs that can register to a PMP AP. The configurable range is from 1 to 238.  **Note** SM trying to register after the maximum configured limit has been reached is locked out for 15 minutes and a message is displayed at the SM.
Receive Quality Debug	To aid in link performance monitoring, the AP and SM now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM) and per channel (polarization).  **Note** Due to CPU load, this will slightly degrade packet per second processing.

Radio page - PMP 450m AP 3 GHz

Table 47 PMP 450m AP Radio attributes - 3 GHz



Attribute	Meaning
Frequency Band	Refer Table 46 PMP 450m AP Radio attributes - 5 GHz for parameter details.
Frequency Carrier	
Channel Bandwidth	
Frame Period	
Cyclic Prefix	
Color Code	
Subscriber Color Code Rescan (When not on a Primary Color Code)	
Subscriber Color Code Wait Period for Idle	
Installation Color Code	
Sector ID	
MIMO Rate Adapt Algorithm	
Downlink Maximum Modulation Rate	
Uplink Maximum Modulation Rate	
Max Range	
Downlink Data	
Contention Slots (a.k.a. Control Slots)	
Broadcast Repeat Count	
Contention Slots	
Auto contention	
EIRP	
SM Receive Target Level	
Adjacent Channel Support	

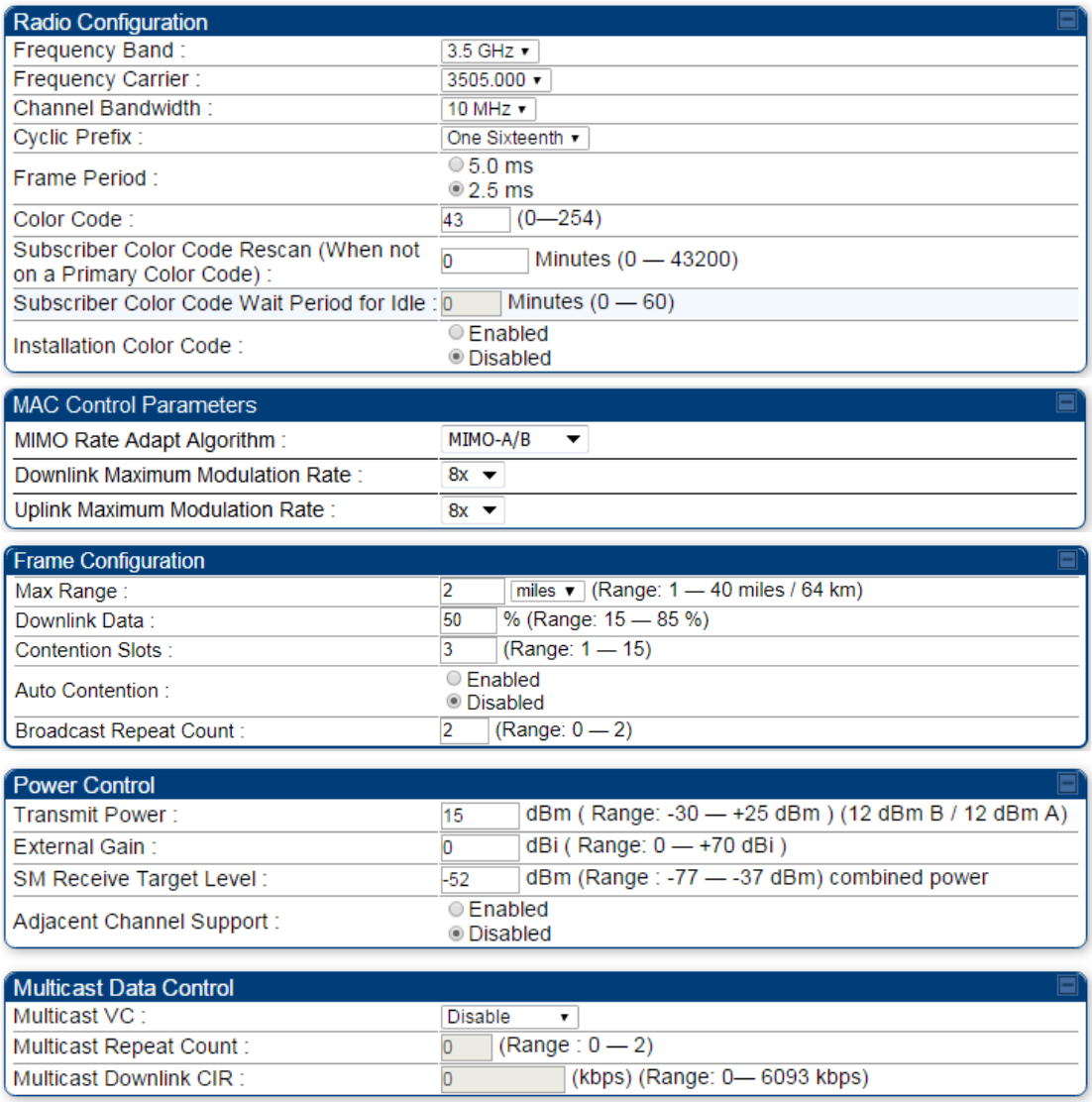
Multicast Data Channel	
Multicast Repeat Count	
Multicast Downlink CIR	Refer Table 46 PMP 450m AP Radio attributes - 5 GHz for parameter details.
SM Registration Limit	
Reieve Quality Debug	
SM Link Test Mode Restriction	
Force Channel Reassessment	
Near Field Operation	

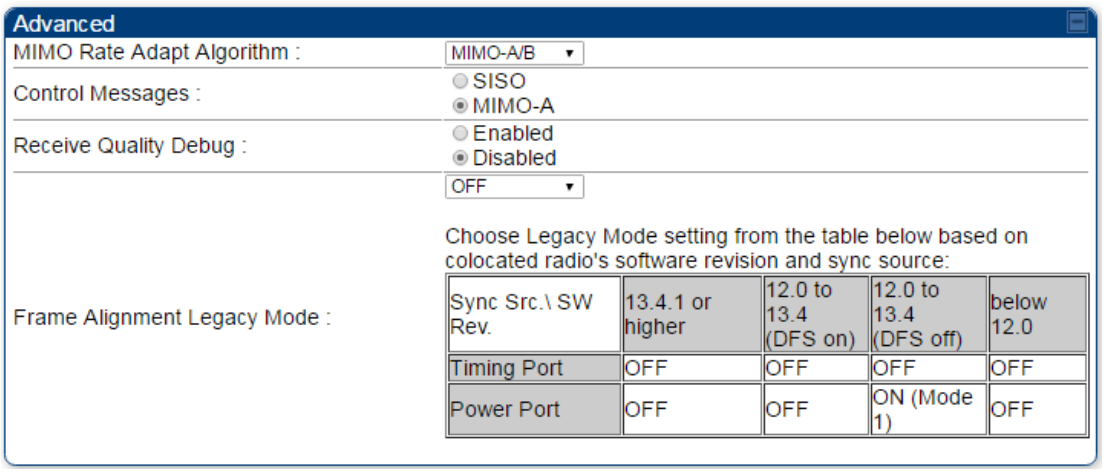
PMP/PTP 450i Series – configuring radio

Radio page - PMP 450i AP 3 GHz

The **Radio** tab of the PMP 450i AP 3 GHz is shown in Figure 24.

Figure 24 PMP 450i AP Radio attributes - 3 GHz





Note

Refer Table 48 PMP 450i AP Radio attributes - 5 GHz and Table 49 PMP 450i SM Radio attributes – 5 GHz on page 1-163 for parameter details

Note

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

Radio page - PMP 450i AP 5 GHz

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

Table 48 PMP 450i AP Radio attributes - 5 GHz