

Cambium PMP 450 Configuration and User Guide

System Release 12.0



Cambium Networks

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

Components, units, or 3rd Party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities). Cambium and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

© 2009 – 2012 Cambium Networks, Inc. All Rights Reserved.

Safety and regulatory information

This section describes important safety and regulatory guidelines that must be observed by personnel installing or operating PMP 450 equipment.

Important safety information

WARNING

To prevent loss of life or physical injury, observe the safety guidelines in this section.

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

Grounding and protective earth

PMP 450 units must be properly grounded to protect against lightning. It is the user's responsibility to install the equipment in accordance with national regulations. In the USA, follow Section 810 of the *National Electric Code, ANSI/NFPA No. 70-1984* (USA). In Canada, follow Section 54 of the *Canadian Electrical Code*. These codes describe correct installation procedures for grounding the outdoor unit, mast, lead-in wire and discharge unit, size of grounding conductors and connection requirements for grounding electrodes. Other regulations may apply in different countries and therefore it is recommended that installation of the outdoor unit be contracted to a professional installer.

Powering down before servicing

Always power down and unplug the equipment before servicing.

Primary disconnect device

The main power supply is the primary disconnect device.

External cables

Safety may be compromised if outdoor rated cables are not used for connections that will be exposed to the outdoor environment.

RF exposure near the antenna

Strong radio frequency (RF) fields will be present close to the antenna when the transmitter is on. Always turn off the power to the PMP 450 unit before undertaking maintenance activities in front of the antenna.

Minimum separation distances

Install the units so as to provide and maintain the minimum separation distances from all persons.

Important regulatory information

The PMP 450 product is 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).

Radar avoidance

In countries where radar systems are the primary band users, the regulators have mandated special requirements to protect these systems from interference caused by unlicensed devices. Unlicensed devices must detect and avoid co-channel operation with radar systems.

The PMP 450 system provides detect and avoid functionality for countries and frequency bands requiring protection for radar systems.

Installers and users must meet all local regulatory requirements for radar detection. To meet these requirements, users must set the correct region code during commissioning of the the PMP 450. If this is not done, installers and users may be liable to civil and criminal penalties.

Contact the Cambium helpdesk if more guidance is required.

USA and Canada specific information

The USA Federal Communications Commission (FCC) has asked 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.

In order to comply with these FCC requirements, Cambium supplies variants of the PMP 450 for operation in the USA or Canada. These variants are only allowed to operate with region codes that comply with FCC/IC rules.

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

Contents

Safety and regulatory information	I
Important safety information	I
Important regulatory information	II
About This Configuration and User Guide	1-8
General information.....	1-9
Version information.....	1-9
Contacting Cambium Networks	1-9
Problems and warranty	1-11
Security advice	1-13
Warnings, cautions, and notes	1-14
Caring for the environment	1-15
Chapter 1: Legal information	1-1
Cambium Networks end user license agreement	1-2
Acceptance of this agreement	1-2
Definitions	1-2
Grant of license.....	1-2
Conditions of use	1-3
Title and restrictions	1-4
Confidentiality.....	1-4
Right to use Cambium’s name.....	1-5
Transfer	1-5
Updates	1-5
Maintenance	1-5
Disclaimer	1-6
Limitation of liability	1-6
U.S. government	1-7
Term of license.....	1-7
Governing law	1-7
Assignment	1-7
Survival of provisions.....	1-8
Entire agreement.....	1-8
Hardware warranty	1-9
Limit of liability	1-10
Chapter 2: Configuration and alignment	2-1
Preparing for configuration and alignment	2-2
Safety precautions during configuration and alignment	2-2
Regulatory compliance during configuration and alignment	2-2

Task 1: Connecting to the unit.....	2-3
Configuring the management PC.....	2-3
Connecting to the PC and powering up	2-5
Logging into the web interface	2-5
Task 2: Configuring IP and Ethernet interfaces	2-6
Configuring the AP IP interface	2-6
NAT tab of the SM with NAT disabled	2-10
IP tab of the SM with NAT disabled	2-14
NAT tab of the SM with NAT enabled.....	2-16
IP tab of the SM with NAT enabled.....	2-21
Reconnecting to the management PC	2-21
VLAN Tab of the AP	2-22
VLAN Membership Tab of the AP.....	2-26
VLAN Tab of the SM	2-27
VLAN Membership Tab of the SM.....	2-31
PPPoE Tab of the SM	2-32
NAT Port Mapping Tab of the SM.....	2-36
Task 3: Upgrading the software version and using CNUT	2-37
Checking the installed software version.....	2-37
Upgrading to a new software version	2-37
Task 4: Configuring General and Unit settings.....	2-41
General Tab of the AP	2-41
Unit Settings Tab of the AP	2-46
General Tab of the SM.....	2-47
Unit Settings Tab of the SM.....	2-51
Time tab of the AP	2-53
Task 5: Configuring security	2-56
Isolating APs from the internet.....	2-56
Encrypting radio transmissions.....	2-57
Managing module access by passwords.....	2-58
Requiring SM Authentication	2-61
Filtering protocols and ports	2-62
Encrypting downlink broadcasts.....	2-64
Isolating SMs.....	2-64
Filtering management through Ethernet	2-65
Allowing management only from specified IP addresses	2-65
Configuring management IP by DHCP.....	2-65
Denying All Remote Access.....	2-65
Reinstating Remote Access Capability.....	2-66
Security Tab of the AP	2-67
Protocol Filtering tab of the AP	2-70
Port configuration tab of the AP.....	2-71
Security Tab of the SM.....	2-72

Protocol Filtering Tab of the SM.....	2-76
Port configuration tab of the SM	2-77
Task 6: Configuring radio parameters.....	2-79
Task 7: Setting up SNMP agent	2-92
SNMP Tab of the AP	2-93
SNMP Tab of the SM	2-96
Task 8: Configuring syslog	2-100
Configuring AP system logging (syslog)	2-100
Configuring SM system logging (syslog)	2-101
Task 9: Configuring remote access	2-102
Configuring SM IP over-the-air access	2-102
Accessing SM over-the-air by LUID	2-102
Denying All Remote Access.....	2-103
Reinstating Remote Access Capability.....	2-104
Task 10: Monitoring the AP-SM Link	2-105
Monitoring the AP-SM Link.....	2-105
Task 11: Configuring quality of service	2-106
Maximum Information Rate (MIR) Parameters	2-106
Token Bucket Algorithm.....	2-106
MIR Data Entry Checking.....	2-107
Committed Information Rate.....	2-107
Bandwidth from the SM Perspective.....	2-108
Interaction of Burst Allocation and Sustained Data Rate Settings	2-108
High-priority Bandwidth	2-108
Traffic Scheduling	2-109
Setting the Configuration Source	2-110
Quality of Service (QoS) Tab of the AP.....	2-113
DiffServ Tab of the AP	2-116
Quality of Service (QoS) Tab of the SM	2-118
DiffServ Tab of the SM	2-120
Task 12: Configuring a RADIUS server	2-122
Understanding RADIUS for PMP 450	2-122
Choosing Authentication Mode and Configuring for Authentication Servers - AP	2-123
SM Authentication Mode – Require RADIUS or Follow AP	2-124
Handling Certificates.....	2-126
Configuring your RADIUS servers for SM authentication.....	2-127
Configuring your RADIUS server for SM configuration	2-129
Using RADIUS for centralized AP and SM user name and password management.....	2-131
RADIUS Device Data Accounting.....	2-134
RADIUS Device Re-Authentication	2-138
RADIUS Attribute Framed-IP-Address	2-138
Chapter 3: Reference information.....	3-1
FCC and ICC Information	3-2

Transmitter Output Power 3-5

Exposure Separation Distances 3-1

 Details of Exposure Separation Distances Calculations and Power Compliance Margins 3-1

Appendix A: Glossary A-1

List of Figures

Figure 1 NAT tab of the SM with NAT disabled	2-10
Figure 2 IP tab of the SM with NAT disabled	2-14
Figure 3 NAT tab of the SM with NAT enabled	2-16
Figure 4 IP tab of SM with NAT enabled	2-21
Figure 5 VLAN tab of the AP	2-22
Figure 6 VLAN Membership tab of the SM	2-31
Figure 7 General Status tab view for GUEST-level account	2-59
Figure 8 SM Add User tab.....	2-59
Figure 9 Delete User tab of the SM	2-60
Figure 10 RJ-11 pinout for the override plug.....	2-61
Figure 11 Categorical protocol filtering.....	2-63
Figure 12 Ports filtered per protocol selection.....	2-63
Figure 13 Security tab of the AP	2-67
Figure 14 Port Configuration tab of the SM.....	2-77
Figure 15 Radio tab of the AP	2-79
Figure 16 AP Syslog Configuration page.....	2-100
Figure 17 SM Syslog Configuration page.....	2-101
Figure 18 SM IP Configuration page.....	2-102
Figure 19 AP Session Status page	2-103
Figure 20 AP Remote Subscribers page	2-103
Figure 21 AP Session Status page	2-105
Figure 22 Uplink and downlink rate caps adjusted to apply aggregate cap	2-107
Figure 23 Uplink and downlink rate cap adjustment example.....	2-107
Figure 24 Quality of Service (QoS) tab of the AP	2-113
Figure 25 Diffserv tab of the AP	2-116
Figure 26 Quality of Service (QoS) tab of the SM	2-118
Figure 27 Diffserv tab of the SM.....	2-120
Figure 28 Security tab of the AP	2-124
Figure 29 Security tab of the SM	2-125
Figure 30 SM Certificate Management	2-127
Figure 31 AP display of RADIUS accept for SM	2-128
Figure 32 AP display of RADIUS rejected SM	2-129
Figure 33 SM display of RADIUS accept	2-129
Figure 34 User Authentication tab of the AP	2-132
Figure 35 User Authentication tab of the SM	2-134

List of Tables

Table 1	IP interface attributes.....	2-8
Table 2	SM DNS Options with NAT Disabled.....	2-11
Table 3	SM with NAT disabled - NAT attributes	2-11
Table 4	SM with NAT disabled - IP attributes	2-14
Table 5	SM DNS Options with NAT Enabled	2-17
Table 6	SM with NAT enabled - NAT attributes	2-17
Table 7	SM with NAT enabled - IP attributes.....	2-21
Table 8	SM with NAT enabled - IP attributes.....	2-22
Table 9	VLAN Membership tab of the AP	2-26
Table 10	AP VLAN Membership attributes	2-26
Table 11	VLAN tab of the SM	2-27
Table 12	SM VLAN attributes.....	2-27
Table 13	SM VLAN Membership attributes	2-32
Table 14	PPPoE tab of the SM.....	2-32
Table 15	SM PPPoE attributes	2-33
Table 16	NAT Port Mapping tab of the SM.....	2-36
Table 17	SM PPPoE attributes	2-36
Table 18	General tab of the AP	2-41
Table 19	SM PPPoE attributes	2-42
Table 20	Unit Settings tab of the AP.....	2-46
Table 21	AP Unit Settings attributes	2-46
Table 22	General tab of the SM	2-47
Table 23	AP Unit Settings attributes	2-47
Table 24	Unit Settings tab of the SM.....	2-51
Table 25	SM Unit Settings attributes	2-52
Table 26	Unit Settings tab of the SM.....	2-53
Table 27	AP Time attributes	2-53
Table 28	AP Security attributes	2-68
Table 29	Protocol Filtering tab of the AP	2-70
Table 30	AP Protocol Filtering attributes	2-70
Table 31	Port configuration tab of the AP	2-71
Table 32	AP Port Configuration attributes	2-71
Table 33	Security tab of the SM	2-72
Table 34	AP Security attributes	2-73
Table 35	Protocol Filtering tab of the SM	2-76
Table 36	AP Protocol Filtering attributes	2-76
Table 37	SM Port Configuration attributes	2-78

Table 38 AP Radio attributes	2-79
Table 39: Control slot settings for all OFDM APs in cluster	2-85
Table 40 Radio tab of SM	2-88
Table 41 SM Radio attributes	2-88
Table 42 SNMP tab of the AP	2-93
Table 43 AP SNMP attributes	2-94
Table 44 SNMP tab of SM	2-96
Table 45 SM SNMP attributes	2-97
Table 46 Syslog Configuration attributes	2-101
Table 47 Syslog Configuration attributes	2-101
Table 48 Characteristics of traffic scheduling	2-109
Table 49 Recommended combined settings for typical operations	2-111
Table 50 Where feature values are obtained for an SM with authentication required	2-112
Table 51 Where feature values are obtained for an SM with authentication disabled	2-112
Table 52 AP QoS attributes	2-113
Table 53 Broadcast Downlink CIR achievable per Broadcast Repeat Count	2-115
Table 54 AP Diffserv attributes	2-116
Table 55 AP Quality of Service attributes	2-118
Table 56 SM Diffserv attributes	2-121
Table 57 RADIUS Vendor Specific Attributes (VSAs)	2-130
Table 58 Device data accounting RADIUS attributes	2-134
Table 59 RADIUS accounting messages configuration	2-137
Table 60 RADIUS data accounting message interval	2-137
Table 61 Device re-authentication configuration	2-138
Table 62 US FCC IDs and Industry Canada Certification Numbers and Covered Configurations	3-2
Table 63 PMP 450 AP transmitter output power	3-5
Table 64 Exposure Separation Distances	3-1
Table 65 Calculated Exposure Distances and Power Compliance Margins	3-2

About This Configuration and User Guide

This guide describes the configuration of the Cambium PMP 450 Series of point-to-multipoint wireless equipment deployment. It is intended for use by the system administrator.

General information

Version information

The following shows the issue status of this document since it was first released:

Issue	Date of issue	Remarks
000v001	Jan 2012	System Release 12.0

Contacting Cambium Networks

PMP support website: <http://www.cambiumnetworks.com/support>

PMP main website: <http://www.cambiumnetworks.com/pmp>

Sales enquiries: solutions@cambiumnetworks.com

Email support: support@cambiumnetworks.com

Telephone numbers:

North America: +1 866-961-9288

Latin/Central America: +420 533 336 946

Europe, Middle East or Africa: +44 203 0277499

Asia/Pacific: +420 533 336 946

For full list of Cambium support telephone numbers, see:

<http://www.cambiumnetworks.com/support/technical.php>

Address:

Cambium Networks Limited,
1299 E Algonquin Road
Schaumburg, IL 60196

Purpose

Cambium Networks Point-To-Multipoint (PMP) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium PMP equipment and ancillary devices. 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.

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. Send feedback to email support (see 'Contacting Cambium Networks').

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:
 - The IP addresses and MAC addresses.
 - The software releases.
 - The configuration of software features.
 - Any available diagnostic downloads.
- 5** Escalate the problem by emailing or telephoning support.

See ‘Contacting Cambium Networks’ for URLs, email addresses and telephone numbers.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Warranty

Cambium’s standard hardware warranty is for one (1) year from date of shipment from Cambium or a Cambium distributor. Cambium 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 products or activate warranties, visit the support website.

For warranty assistance, contact the reseller or distributor.

CAUTION

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

 **CAUTION**

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 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 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 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 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. In the EU, Cambium in conjunction with a recycling partner ensures that equipment is collected and recycled according to the requirements of EU environmental law.

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: Legal information

This chapter provides legal notices including software license agreements.



CAUTION

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

The following topics are described in this chapter:

- [Cambium Networks end user license agreement](#) on page 1-2
- [Hardware warranty](#) on page 1-9
- [Limit of liability](#) on page 1-10

Cambium Networks end user license agreement

Acceptance of this agreement

In connection with Cambium’s delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both, Cambium is willing to license this certain proprietary software and the accompanying documentation to you only on the condition that you accept all the terms in this End User License Agreement (“Agreement”).

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT OR INSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE PRODUCT, WILL CONSTITUTE YOUR ACCEPTANCE TO THE TERMS OF THIS AGREEMENT.

Definitions

In this Agreement, the word “Software” refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word “Documentation” refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word “Product” refers to Cambium’s fixed wireless broadband devices for which the Software and Documentation is licensed for use.

Grant of license

Cambium Networks Limited (“Cambium”) grants you (“Licensee” or “you”) a personal, nonexclusive, non-transferable license to use the Software and Documentation subject to the Conditions of Use set forth in “Conditions of use” and the terms and conditions of this Agreement. Any terms or conditions relating to the Software and Documentation appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

Conditions of use

Any use of the Software and Documentation outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.
2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.
3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.
4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.
5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

Title and restrictions

If you transfer possession of any copy of the Software and Documentation to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Software and Documentation and any copies made by you remain with Cambium and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Cambium's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Software and Documentation be equipped with such a protection device. If the Software and Documentation is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Cambium's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

Confidentiality

You acknowledge that all Software and Documentation contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Software and Documentation will result in irreparable harm to Cambium for which monetary damages would be inadequate and for which Cambium will be entitled to immediate injunctive relief. If applicable, you will limit access to the Software and Documentation to those of your employees and agents who need to use the Software and Documentation for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Software and Documentation, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Cambium prior to such disclosure and provide Cambium with a reasonable opportunity to respond.

Right to use Cambium's name

Except as required in “Conditions of use”, you will not, during the term of this Agreement or thereafter, use any trademark of Cambium, or any word or symbol likely to be confused with any Cambium trademark, either alone or in any combination with another word or words.

Transfer

The Software and Documentation may not be transferred to another party without the express written consent of Cambium, regardless of whether or not such transfer is accomplished by physical or electronic means. Cambium's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

Updates

During the first 12 months after purchase of a Product, or during the term of any executed Maintenance and Support Agreement for the Product, you are entitled to receive Updates. An “Update” means any code in any form which is a bug fix, patch, error correction, or minor enhancement, but excludes any major feature added to the Software. Updates are available for download at the support website.

Major features may be available from time to time for an additional license fee. If Cambium makes available to you major features and no other end user license agreement is provided, then the terms of this Agreement will apply.

Maintenance

Except as provided above, Cambium is not responsible for maintenance or field service of the Software under this Agreement.

Disclaimer

CAMBIUM DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. CAMBIUM SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED “AS IS.” CAMBIUM DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of liability

THE TOTAL LIABILITY OF CAMBIUM UNDER THIS AGREEMENT FOR DAMAGES WILL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PRODUCT LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL CAMBIUM BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER CAMBIUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you.

U.S. government

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Software and Documentation is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

Term of license

Your right to use the Software will continue in perpetuity unless terminated as follows. Your right to use the Software will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Cambium in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Cambium, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

Governing law

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

Assignment

This agreement may not be assigned by you without Cambium's prior written consent.

Survival of provisions

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

Entire agreement

This agreement contains the parties' entire agreement regarding your use of the Software and may be amended only in writing signed by both parties, except that Cambium may modify this Agreement as necessary to comply with applicable laws.

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium or a Cambium Point-To-Point Distributor. Cambium 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.

Limit of liability

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

Chapter 2: Configuration and alignment

This chapter describes all configuration and alignment tasks that are performed when a PMP 450 link is deployed.

Observe the precautions in [Preparing for configuration and alignment](#) on page 2-2.

Preparing for configuration and alignment

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

Safety precautions during configuration and alignment

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 as soon as they are powered up.

Observe the following guidelines:

- Never work in front of the antenna when the AP or SM is powered.
- Always power down the AP or SM before connecting or disconnecting the drop cable from the unit.

Regulatory compliance during configuration and alignment

All applicable radio regulations must be followed while configuring the units and aligning the antennas.

CAUTION

USA only: if the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred during staging, before the units are allowed to radiate on site, otherwise FCC rules will be infringed.

Task 1: Connecting to the unit

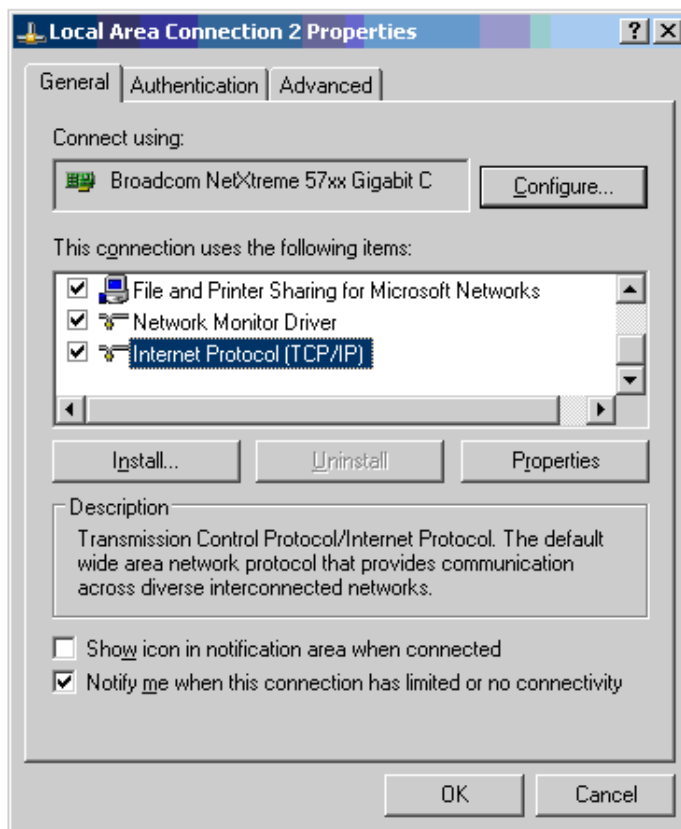
This task consists of the following procedures:

- [Configuring the management PC](#) on page 2-3
- [Connecting to the PC and powering up](#) on page 2-5
- [Logging into the web interface](#) on page 2-5

Configuring the management PC

To configure the local management PC to communicate with the PMP 450 AP or SM, proceed as follows:

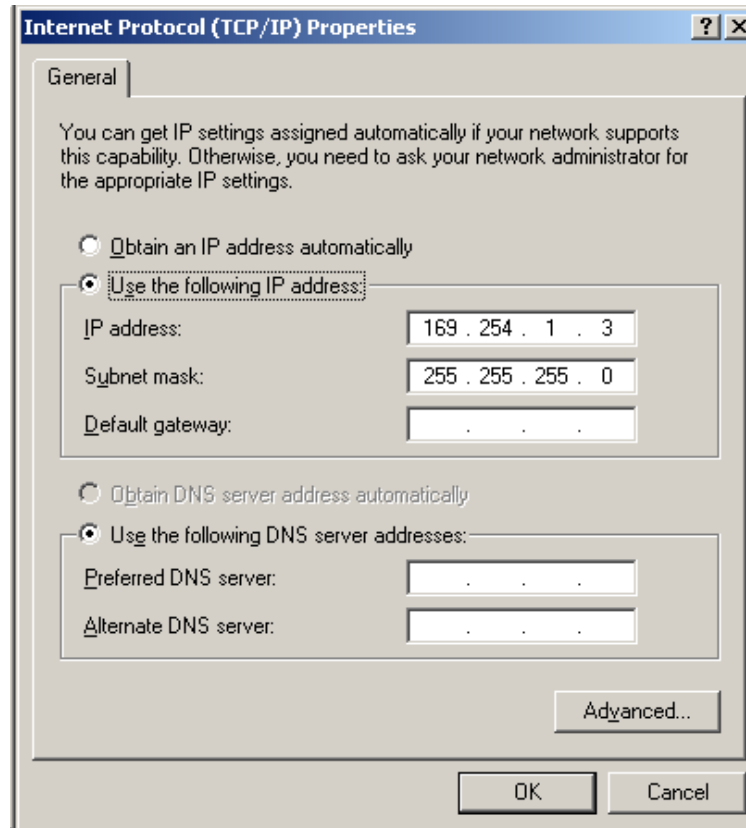
- 1** Select **Properties** for the Ethernet port.
- 2** Select the Internet Protocol (TCP/IP) item:



- 3** Click on **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 and 169.254.1.2

A good example is 169.254.1.3:



- 5** Enter a subnet mask of 255.255.255.0.
Leave the default gateway blank.

Connecting to the PC and powering up

To connect the PMP 450 AP or SM to the PC and power up the unit, proceed as follows:

- 1 Check that the AP/SM and the associated power supply are correctly connected.
- 2 Connect the PC Ethernet port to the LAN port of the power supply using a standard (not crossed) Ethernet cable.
- 3 Apply power to the radio power supply. The green Power LED should illuminate continuously.

Logging into the web interface

To log into the web interface as a system administrator, proceed as follows:

- 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 General Status page is displayed:

The screenshot shows the Cambium Networks web interface. The left sidebar contains a navigation menu with options: Home, Configuration, Statistics, Tools, Logs, Accounts, Quick Start, and Copyright. Below the menu, it shows the user account as 'none' and the level as 'ADMINISTRATOR'. The main content area is titled 'General Status' and shows the device type as '5.7GHz OFDM - Access Point - 0a-00-3e-3f-ff-53'. A red error message states: 'Region Code not Configured - Transmit Disabled!'. Below this, a table provides detailed device information.

Device Information	
Device Type :	5.7GHz OFDM - Access Point - 0a-00-3e-3f-ff-53 No valid accounts configured. Using default user account
Software Version :	CANOPY 11.2 AP-DES
Board Type :	P11
FPGA Version :	112211
FPGA Type :	C120
PLD Version :	1
Uptime :	00:01:04
System Time :	00:01:04 01/01/2011 UTC
Last NTP Time Update :	00:00:00 00/00/0000 UTC
Ethernet Interface :	100Base-TX Half Duplex
Regulatory :	Invalid Region Setting - Unit will not transmit until valid region has been configured.
DFS :	Idle
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/4
Temperature :	31 °C / 88 °F

Task 2: Configuring IP and Ethernet interfaces

This task consists of the following procedures:

- [Configuring the AP IP interface on page 2-6](#)

Configuring the AP IP interface

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



NOTE

To configure the Ethernet link to run at a fixed speed and duplex, leave Ethernet Auto Negotiation set to 'Enabled' and set Auto Neg Advertisement to the required speed.

To configure the IP interface, proceed as follows

- 1** Select menu option **System, Configuration, LAN Configuration**. The LAN configuration page is displayed:

Configuration → IP
5.7GHz OFDM - Access Point - 0a-00-3e-3f-ff-53

Save Changes Reboot

LAN1 Network Interface Configuration

IP Address :	188.254.1.1
Subnet Mask :	255.255.0.0
Gateway IP Address :	188.254.0.0
DHCP state :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

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

IP Address :	192.168.101.1
--------------	---------------

Save Changes

Reboot

- 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 required ([Table 1](#)).

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

Configuration → IP
5.7GHz OFDM - Access Point - 0a-00-3e-3f-ff-53

Reboot Required

Save Changes Reboot

LAN1 Network Interface Configuration

IP Address : 169.254.1.2

Subnet Mask : 255.255.0.0

Gateway IP Address : 169.254.0.0

DHCP state : Enabled
 Disabled

DNS IP Address : Obtain Automatically
 Set Manually

Preferred DNS Server : 0.0.0.0

Alternate DNS Server : 0.0.0.0

Domain Name : example.com

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

IP Address : 192.168.101.1

Save Changes

Reboot

Reboot Required

5 Select **Reboot**.

Table 1 IP interface attributes

Attribute	Meaning
IP Address	Internet protocol (IP) address. This address is used by the 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, but not settable, 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.

Attribute	Meaning									
Alternate DNS Server	Upon failure to reach the Preferred DNS server, the Alternate DNS Server is used.									
Domain Name	The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.									
LAN2 Network Interface Configuration (Radio Private Interface) – IP Address	<p>It is recommended to not change this parameter from the default <i>AP</i> private IP address of 192.168.101.1. A /24 CIDR subnet is used to communicate with each of the SMs that are registered. The <i>AP</i> uses a combination of the private IP and the LUID (logical unit ID) of the SM.</p> <p>For example, if an SM is the first to register in an <i>AP</i>, and another SM registers later, then the <i>AP</i> whose Private IP address is 192.168.101.1 uses the following <i>SM</i> Private IP addresses to communicate to each:</p> <table border="1" data-bbox="688 737 1313 907"> <thead> <tr> <th data-bbox="695 745 984 793">SM</th> <th data-bbox="984 745 1102 793">LUID</th> <th data-bbox="1102 745 1307 793">Private IP</th> </tr> </thead> <tbody> <tr> <td data-bbox="695 793 984 846">First SM registered</td> <td data-bbox="984 793 1102 846">2</td> <td data-bbox="1102 793 1307 846">192.168.101.2</td> </tr> <tr> <td data-bbox="695 846 984 898">Second SM registered</td> <td data-bbox="984 846 1102 898">3</td> <td data-bbox="1102 846 1307 898">192.168.101.3</td> </tr> </tbody> </table>	SM	LUID	Private IP	First SM registered	2	192.168.101.2	Second SM registered	3	192.168.101.3
SM	LUID	Private IP								
First SM registered	2	192.168.101.2								
Second SM registered	3	192.168.101.3								

NAT tab of the SM with NAT disabled

Figure 1 NAT tab of the SM with NAT disabled

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

Configuration => NAT

5.2GHz - Subscriber Module - 0a-00-3e-04-99-42

NAT Enable

NAT Enable/Disable : Enabled
 Disabled

WAN Interface

Connection Type : DHCP

IP Address : 0.0.0.0

Subnet Mask : 255.255.255.0

Gateway IP Address : 0.0.0.0

Reply to Ping on WAN Interface : Enabled
 Disabled

LAN Interface

IP Address : 192.168.1.28

Subnet Mask : 255.255.255.xxx

DMZ Enable : Enabled
 Disabled

DMZ IP Address : xxx.xxx.xxx.52

LAN DHCP Server

DHCP Server Enable/Disable : Enabled
 Disabled

DHCP Server Lease Timeout : 30 Days (Range : 1 — 30)

DHCP Start IP : xxx.xxx.xxx.2

Number of IP's to Lease : 50

DNS IP Address : Obtain Automatically (From WAN DHCP or PPPoE)
 Set Manually

Preferred DNS IP Address : 0.0.0.0

Alternate DNS IP Address : 0.0.0.0

Remote Configuration Interface

Interface Enable/Disable : Enabled
 Disabled

Connection Type : DHCP
 Static IP

IP Address : 0.0.0.0

Subnet Mask : 255.255.255.0

Gateway IP Address : 0.0.0.0

NAT Protocol Parameters

ARP Cache Timeout : 20 Minutes (Range : 1 — 30)

TCP Session Garbage Timeout : 120 Minutes (Range : 4 — 1440)

UDP Session Garbage Timeout : 4 Minutes (Range : 1 — 1440)

SM NAT DNS Considerations

SM DNS behavior is different depending on the accessibility of the SM. When NAT is disabled the DNS configuration that is discussed in this document is tied to LAN1 interface, and only functions if the device is publicly accessible. 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 2 SM DNS Options with NAT Disabled

NAT Configuration	Management Interface Accessibility	DHCP Status	DNS Status
NAT Disabled	Local	DHCP Disabled	DNS Disabled
		DHCP Enabled	DNS Disabled
	Public	DHCP Disabled	DNS Static Configuration
		DHCP Enabled	DNS from DHCP or DNS Static Configuration

In the NAT tab of an SM with NAT disabled, you may set the following parameters.

Table 3 SM with NAT disabled - NAT attributes

Attribute	Meaning
NAT Enable/Disable	<p>This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an 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/wired side of the SM</p> <p>When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design</p>
WAN Interface, Connection Type	This parameter is not configurable when NAT is disabled.
WAN Interface, IP Address	This field displays the IP address for the SM. DHCP Server <i>will not</i> automatically assign this address when NAT is disabled.

Attribute	Meaning
WAN Interface, Subnet Mask	This field displays the subnet mask for the SM. DHCP Server <i>will not</i> automatically assign this address when NAT is disabled.
WAN Interface, Gateway IP Address	This field displays the gateway IP address for the SM. DHCP Server <i>will not</i> automatically assign this address when NAT is disabled.
WAN Interface, Reply to Ping on WAN Interface	This parameter is not configurable when NAT is disabled.
LAN Interface, IP Address	This parameter is not configurable when NAT is disabled.
LAN Interface, Subnet Mask	This parameter is not configurable when NAT is disabled.
LAN Interface, DMZ Enable	This parameter is not configurable when NAT is disabled.
LAN Interface, DMZ IP Address	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, DHCP Server Enable/Disable	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, DHCP Server Lease Timeout	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, DHCP Start IP	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, Number of IPs to Lease	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, DNS Server Proxy	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, DNS IP Address	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, Preferred DNS IP Address	This parameter is not configurable when NAT is disabled.
LAN DHCP Server, Alternate DNS IP Address	This parameter is not configurable when NAT is disabled.
Remote Configuration Interface, Interface Enable/Disable	This parameter is not configurable when NAT is disabled.
Remote Configuration Interface, Connection Type	This parameter is not configurable when NAT is disabled.
Remote Configuration Interface, IP Address	This parameter is not configurable when NAT is disabled.

Attribute	Meaning
Remote Configuration Interface, Subnet Mask	This parameter is not configurable when NAT is disabled.
Remote Configuration Interface, Gateway IP Address	This parameter is not configurable when NAT is disabled.
Remote Configuration Interface, DNS IP Address	This parameter is not configurable when NAT is disabled.
Remote Configuration Interface, Preferred DNS Server	This parameter is not configurable when NAT is disabled.
Remote Connection Interface, Alternate DNS Server	This parameter is not configurable when NAT is disabled.
Remote Connection Interface, Domain Name	This parameter is not configurable when NAT is disabled.
NAT Protocol Parameters, 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.
NAT Protocol Parameters, TCP Session Garbage Timeout	Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates.
NAT Protocol Parameters, 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.


IP tab of the SM with NAT disabled

Figure 2 IP tab of the SM with NAT disabled

LAN1 Network Interface Configuration	
IP Address :	192.168.2.57
Network Accessibility :	<input checked="" type="radio"/> Public <input type="radio"/> Local
Subnet Mask :	255.255.255.0
Gateway IP Address :	192.168.2.1
DHCP state :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
Domain Name :	example.com

In the IP tab of an SM with NAT disabled, you may set the following parameters.

Table 4 SM with NAT disabled - IP attributes

Attribute	Meaning
LAN1 Network Interface Configuration, IP Address	<p>Enter the <i>non-routable</i> 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 set and then forget this parameter, then you must both</p> <ul style="list-style-type: none"> physically access the module. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP on Page 2-60. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> NOTE</p> <p>Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.</p> </div>
LAN1 Network Interface Configuration, Network Accessibility	Specify whether the IP address of the SM should be visible to only a device connected to the SM by Ethernet (Local) or should be visible to the AP as well (Public).
LAN1 Network Interface Configuration, Subnet Mask	Enter an appropriate subnet mask for the SM to communicate on the network. The default subnet mask is 255.255.0.0.
LAN1 Network Interface Configuration, Gateway IP Address	Enter the appropriate gateway for the SM to communicate with the network. The default gateway is 169.254.0.0.

Attribute	Meaning
LAN1 Network Interface Configuration, DHCP state	<p>If you select Enabled, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable, but not settable, in the Network Interface tab of the Home page.</p> <p>In this tab, DHCP State is settable only if the Network Accessibility 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.</p> <p>If the DHCP state parameter is set to Enabled in the Configuration => IP tab of the SM, <i>do not</i> check the BootpClient option for Packet Filter Types in its Protocol Filtering tab, because doing so would 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.</p>
LAN1 Network Interface Configuration, DNS IP Address	<p>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.</p>
LAN1 Network Interface Configuration, Preferred DNS Server	<p>The first DNS server used for DNS resolution.</p>
LAN1 Network Interface Configuration, Alternate DNS Server	<p>The second DNS server used for DNS resolution.</p>
LAN1 Network Interface Configuration, Domain Name	<p>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.</p>

NAT tab of the SM with NAT enabled

Figure 3 NAT tab of the SM with NAT enabled

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

Configuration => NAT

5.2GHz - Subscriber Module - 0a-00-3e-04-99-42

NAT Enable	
NAT Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Save Changes	
WAN Interface	
Connection Type :	DHCP
IP Address :	0.0.0.0
Subnet Mask :	255.255.255.0
Gateway IP Address :	0.0.0.0
Reply to Ping on WAN Interface :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
LAN Interface	
IP Address :	169.254.1.1
Subnet Mask :	255.255.255.0
DMZ Enable :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DMZ IP Address :	169.254.1.52
LAN DHCP Server	
DHCP Server Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DHCP Server Lease Timeout :	30 Days (Range : 1 — 30)
DHCP Start IP :	169.254.1.2
Number of IP's to Lease :	50
DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically (From WAN DHCP or PPPoE) <input type="radio"/> Set Manually
Preferred DNS IP Address :	0.0.0.0
Alternate DNS IP Address :	0.0.0.0
Remote Configuration Interface	
Interface Enable/Disable :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Connection Type :	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address :	192.168.1.28
Subnet Mask :	255.255.255.0
Gateway IP Address :	192.168.1.1
NAT Protocol Parameters	
ARP Cache Timeout :	20 Minutes (Range : 1 — 30)
TCP Session Garbage Timeout :	120 Minutes (Range : 4 — 1440)
UDP Session Garbage Timeout :	4 Minutes (Range : 1 — 1440)
Save Changes	
Reboot	

SM NAT DNS Considerations

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 5 SM DNS Options with NAT Enabled

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

In the NAT tab of an SM with NAT enabled, you may set the following parameters.

Table 6 SM with NAT enabled - NAT attributes

Attribute	Meaning
NAT Enable/Disable	<p>This parameter enables or disabled the Network Address Translation (NAT) feature for the SM. NAT isolates devices connected to the Ethernet/wired side of an 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/wired side of the SM.</p> <p>When NAT is enabled, VLANs are not supported on the wired side of that SM. You can enable NAT in SMs within a sector where VLAN is enabled in the AP, but this may constrain network design.</p>
WAN Interface	The WAN interface is the RF-side address for transport traffic.

Attribute	Meaning
WAN Interface, Connection Type	<p>This parameter may be set to</p> <p>Static IP—when this is the selection, the following three parameters (IP Address, Subnet Mask, and Gateway IP Address) must all be properly populated.</p> <p>DHCP—when this is the selection, the information from the DHCP server configures the interface.</p> <p>PPPoE—when this is the selection, the information from the PPPoE server configures the interface.</p>
WAN 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.
WAN Interface, 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.
WAN Interface, Reply to Ping on WAN Interface	By default, the radio interface <i>does not</i> respond to pings. If you use a management system (such as Prizm or 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.
LAN Interface, IP Address	Assign an IP address for SM management through Ethernet access to the SM. This address becomes the base for the range of DHCP-assigned addresses.
LAN Interface, 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.
LAN Interface, DMZ Enable	Either enable or disable DMZ for this SM.
LAN Interface, 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 should receive 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.
LAN 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.
WAN 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.

Attribute	Meaning
LAN DHCP Server, DHCP Server Enable/Disable	Select either Enabled to <ul style="list-style-type: none"> • allow this SM to assign IP addresses, subnet masks, and gateway IP addresses to attached devices. • assign a start address for DHCP. • designate how many IP addresses may be temporarily used (leased). Disabled to disallow the SM to assign addresses to attached devices.
LAN DHCP Server, 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.
LAN DHCP Server, DHCP Start IP	If you will be enabling DHCP Server below, set the last byte of the starting IP address that the DHCP server will assign. The first three bytes are identical to those of the NAT private IP address.
LAN DHCP Server, Number of IPs to Lease	Enter how many IP addresses the DHCP server is allowed to assign. The default value is 50 addresses.
LAN DHCP Server, DNS Server Proxy	This parameter enables or disables advertisement of the SM as the DNS server. On initial boot up of an SM with the NAT WAN interface configured as DHCP or PPPoE, the SM module will not immediately have DNS information. 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.
LAN DHCP Server, DNS IP Address	Select either Obtain Automatically to allow the system to set the IP address of the DNS server. Set Manually to enable yourself to set both a preferred and an alternate DNS IP address.
LAN DHCP Server, Preferred DNS IP Address	Enter the preferred DNS IP address to use when the DNS IP Address parameter is set to Set Manually .
LAN DHCP Server, 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 Configuration Interface, Interface Enable/Disable	If you want over-the-air management capability for the SM, select Enabled . If you want to limit management of the SM to its Ethernet interface, select Disabled .

Attribute	Meaning
Remote Configuration Interface	The Remote Configuration interface is the RF-side address for management by an EMS or NMS (Prizm or WM, for example).
Remote Configuration Interface, Interface Enable/Disable	<p>When this interface is Disabled, the SM is not directly accessible by IP address, and management access is only through either the LAN (Ethernet) interface or a link from an AP web page into the WAN (RF-side) interface.</p> <p>When this interface is Enabled, you can configure management access through either</p> <ul style="list-style-type: none"> a Static IP address an IP address that DHCP provides for the WAN interface.
Remote Configuration Interface, Connection Type	<p>This parameter may be set to</p> <p>Static IP—when this is the selection, the following three parameters (IP Address, Subnet Mask, and Gateway IP Address) must all be properly populated.</p> <p>DHCP—when this is the selection, the information from the DHCP server configures the interface.</p>
Remote Configuration 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.
Remote Configuration 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 management traffic.
Remote Configuration Interface, Gateway IP Address	<p>If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the gateway IP address for the SM for RF management traffic.</p> <p>Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.</p>
NAT Protocol Parameters, 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.
NAT Protocol Parameters, TCP Session Garbage Timeout	Where a large network exists behind the SM, you can set this parameter to lower than the default value of 1440 minutes (24 hours). This action makes additional resources available for greater traffic than the default value accommodates. The default value of this parameter is 120 minutes.
NAT Protocol Parameters, 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.

IP tab of the SM with NAT enabled

Figure 4 IP tab of SM with NAT enabled

The screenshot shows the configuration page for the IP tab of a Subscriber Module (SM) with NAT enabled. The page title is "Configuration => IP" and the device is identified as "2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48". The "NAT Network Interface Configuration" section contains the following fields:

- IP Address : 169.254.1 .1
- Subnet Mask : 255.255.255.0

Buttons for "Save Changes" and "Reboot" are visible at the bottom of the configuration area.

In the IP tab of an SM with NAT enabled, you may set the following parameters.

Table 7 SM with NAT enabled - IP attributes

Attribute	Meaning
NAT Network Interface Configuration, IP Address	Assign an IP address for SM management through Ethernet access to the SM. 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.
NAT Network Interface Configuration, 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.

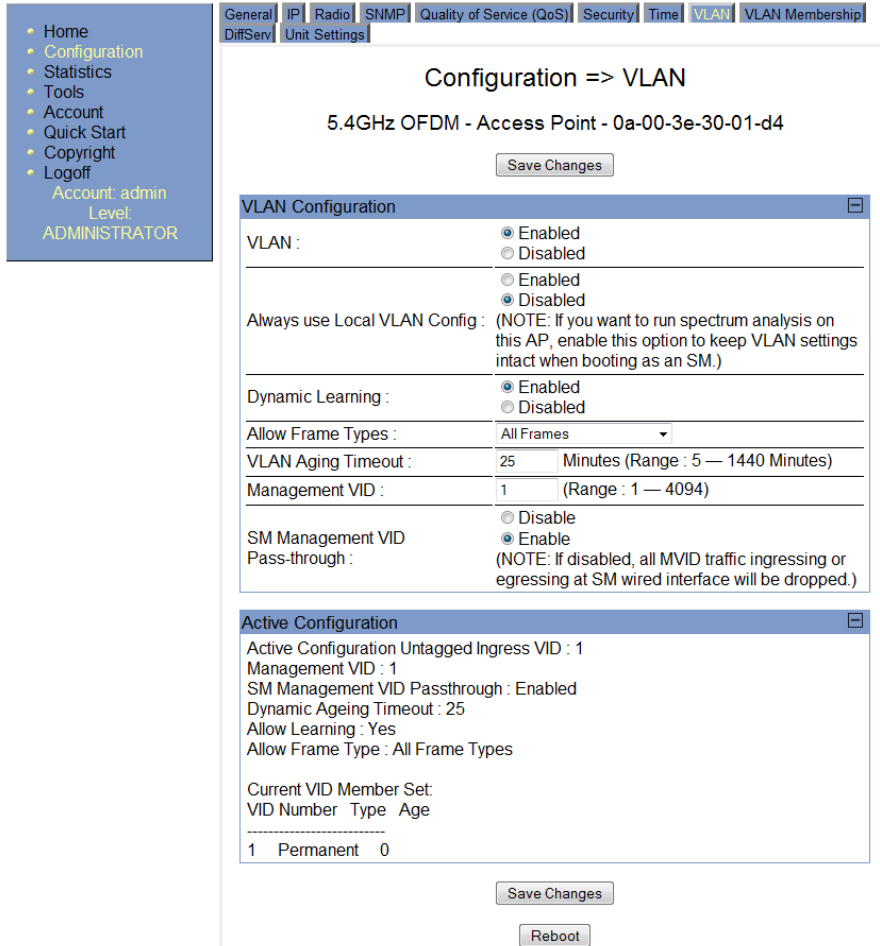
Reconnecting to the management PC

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. Refer to [Configuring the management PC](#) on page 2-3.

When the unit has rebooted, log in using the new IP address. Refer to [Logging into the web interface](#) on page 2-5.

VLAN Tab of the AP



Figure 5 VLAN tab of the AP




In the VLAN tab of the AP, you may set the following parameters.

Table 8 SM with NAT enabled - IP attributes

Attribute	Meaning
VLAN	Specify whether VLAN functionality for the AP and all linked SMs should (Enabled) or should not (Disabled) be allowed. The default value is Disabled .
Always use Local VLAN Config	Enable this option before you reboot this AP as an SM to use it to perform spectrum analysis. After the spectrum analysis is completed and before you reboot this module as an AP, disable this option.

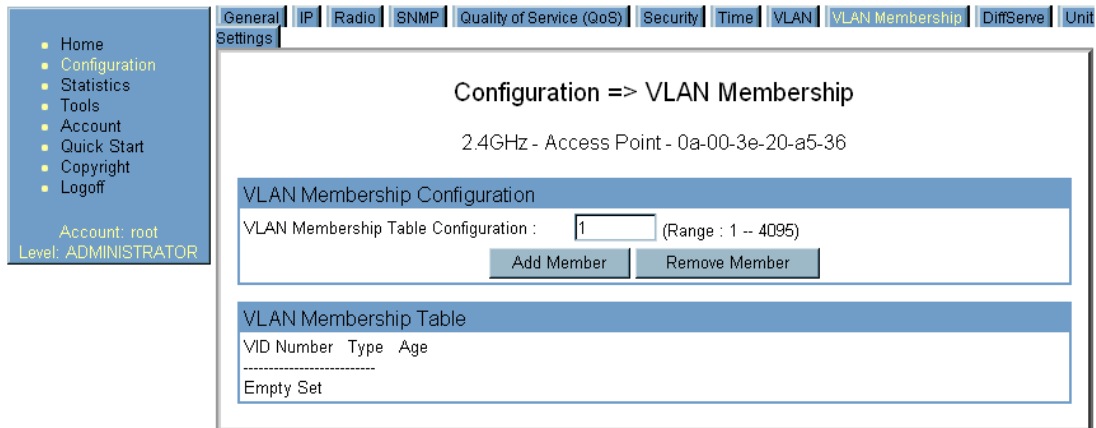
Attribute	Meaning
Dynamic Learning	Specify whether the AP should (Enabled) or should not (Disabled) add the VLAN IDs (VIDs) of upstream frames to the VID table. (The AP passes frames with VIDs that are stored in the table both upstream and downstream.) The default value is Enabled .
Allow Frame Types	Select the type of arriving frames that the AP should tag, using the VID that is stored in the Untagged Ingress VID parameter. The default value is All Frames .
VLAN Aging Timeout	Specify how long the AP should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is 25 (minutes). <div data-bbox="618 737 1313 873" style="border: 1px solid black; padding: 5px;">  NOTE VIDs that you enter for the Management VID and VLAN Membership parameters do not time out. </div>
Management VID	Enter the VID that the operator wishes to use to communicate with the module manager. The range of values is 1 to 4095. The default value is 1 .
SM Management VID Pass-through	Specify whether to allow the SM (Enable) or the AP (Disable) to control the VLAN settings of the SM. The default value is Enable . <div data-bbox="618 1157 1313 1507" style="border: 1px solid black; padding: 5px;">  CAUTION Do not set this parameter to Enable where both a BAM release earlier than 2.1 is implemented. The Configuration Source parameter in the AP is set to BAM. This combination causes the SMs to become unmanageable, until you gain direct access with an override plug and remove this combination from the AP configuration. </div>
QinQ EtherType	This parameter is the outer S-VLAN EtherType that may be configured to interoperate with other networks that use a different EtherType than the default.
Active Configuration	When VLAN is enabled in the AP, the Active Configuration block provides the following details as read-only information in this tab. In the Motorola 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.

Attribute	Meaning
Port VID	This is the VID that the AP will use for tagging frames of the type specified by Allow Frame Types .
Management VID	This is the value of the parameter of the same name, configured above.
SM Management VID Pass-Through	This is the value of the parameter of the same name, configured above.
Dynamic Ageing Timeout	This is the value of the VLAN Aging Timeout parameter configured above.
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 .
Allow Frame Type	This displays the selection that was made from the drop-down list at the Allow Frame Types parameter above.
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.
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 an SM behind it in the network, or from a customer equipment that is behind the SM in this case, was read.

Attribute	Meaning
Current VID Member Set, Age	<p>For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:</p> <ul style="list-style-type: none"> • for Permanent type—the number will never time out, and this is indicated by the digit 0. • for Dynamic type—the 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. <div data-bbox="618 829 1313 1220" style="border: 1px solid black; padding: 5px;"> <p> NOTE</p> <p>Values in this Active Configuration block can differ from attempted values in configurations:</p> <p>A VLAN profile administered by the BAM subsystem in Prizm is capable of overriding any configured VLAN value, if the Configuration Source parameter in the AP is set to Authentication Server.</p> <p>The AP itself can override the value that the SM has configured for SM Management VID Pass-Through.</p> </div>

VLAN Membership Tab of the AP

Table 9 VLAN Membership tab of the AP



You may set the VLAN Membership tab parameter as follows.

Table 10 AP 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 Tab of the SM

Table 11 VLAN tab of the SM

Configuration → VLAN

5.7GHz OFDM - Subscriber Module - 0a-00-3e-3f-fe-48

Save Changes

VLAN Configuration

Dynamic Learning : Enabled
 Disabled

Allow Frame Types : All Frames

VLAN Aging Timeout : 25 Minutes (Range : 5 — 1440 Minutes)

Untagged Ingress VID : 770 (Range : 1 — 4094)

Management VID : 1 (Range : 1 — 4094)

SM Management VID Pass-through : Enable
 Disable
 (NOTE: If disabled, all MVID traffic ingressing or egressing at SM wired interface will be dropped.)

Active Configuration

Active Configuration Untagged Ingress VID : 770
 Management VID : 1
 SM Management VID Passthrough : Enabled
 Dynamic Ageing Timeout : 25
 Allow Learning : Yes
 Allow Frame Type : All Frame Types


Current VID Member Set

VID Number	Type	Age
1	Permanent	0
770	Permanent	0

In the VLAN tab of an SM, you may set the following parameters.


Table 12 SM VLAN attributes

Attribute	Meaning
Always use Local VLAN Config	Enable this option before you reboot this AP as an SM to use it to perform spectrum analysis. After the spectrum analysis is completed and before you reboot this module as an AP, disable this option.

Attribute	Meaning
VLAN Port Type	By default this will be simply Q, indicating that it is to operate in the existing manner. The other option is Q-in-Q, which indicates that it should 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. 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 will be dropped and a filter entry will show up on the VLAN Statistics page as DVLAN Egress or DVLAN Ingress.
Dynamic Learning	Specify whether the SM should (Enable) or should 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 .
Allow Frame Types	Select the type of arriving frames that the SM should tag, using the VID that is stored in the Untagged Ingress VID parameter. The default value is All Frames .
VLAN Aging Timeout	Specify how long the SM should keep dynamically learned VIDs. The range of values is 5 to 1440 (minutes). The default value is 25 (minutes). <div data-bbox="613 1251 1307 1388" style="border: 1px solid black; padding: 5px;">  NOTE VIDs that you enter for the Untagged Ingress VID and Management VID parameters do not time out. </div>
Management VID	Enter the VID that the SM should share with the AP. The range of values is 1 to 4095. The default value is 1 .
SM Management VID Pass-through	Specify whether to allow the SM (Enable) or the AP (Disable) to control the VLAN settings of this SM. The default value is Enable . 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 Motorola 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.

Attribute	Meaning
Default Port VID	This is the VID that will be 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 will be 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 will be 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 would 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 would 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 will be 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 will be 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 will be the S-tag and the Default Port VID (or Port VID MAC Address Mapping , if valid) will be used for the C-tag.
Active Configuration, Default Port VID	This is the value of the parameter of the same name, configured above.
Active Configuration, MAC Address VID Map	This is the listing of the MAC address VIDs configured in Port VID MAC Address Mapping .
Active Configuration, Management VID	This is the value of the parameter of the same name, configured above.

Attribute	Meaning
Active Configuration, SM Management VID Pass-Through	This is the value of the parameter of the same name, configured above.
Active Configuration, Dynamic Ageing Timeout	This is the value of the VLAN Aging Timeout parameter configured above.
Active Configuration, Allow Learning	Yes is displayed if the value of the Dynamic Learning parameter above is Enabled . No is displayed if the value of Dynamic Learning is Disabled .
Active Configuration, Allow Frame Type	This displays the selection that was made from the drop-down list at the Allow Frame Types parameter above.
Active Configuration, QinQ	This is set to Enabled if VLAN Port Type is set to QinQ , and is set to Disabled if VLAN Port Type is set to Q .
Active Configuration, QinQ EthType	This is the value of the QinQ EtherType configured in the AP.
Active Configuration, Allow QinQ Tagged Frames	This is the value of Accept QinQ Frames , configured above.
Active Configuration, Current VID Member Set, VID Number	This column lists the ID numbers of the VLANs in which this module is a member, whether through assignment or through dynamic learning.
Active Configuration, Current VID Member Set, Type	<p>For each VID number in the first column, the entry in this column correlates the way in which the module became and continues to be a member:</p> <p>Permanent—This indicates that the module was assigned the VID number through direct configuration by the operator.</p> <p>Dynamic—This indicates that the module adopted the VID number through enabled dynamic learning, when a tagged packet from an SM behind it in the network, or from a customer equipment that is behind the SM in this case, was read.</p>

Attribute	Meaning
Active Configuration, Current VID Member Set, Age	<p>For each VID number in the first column of the table, the entry in this column reflects whether or when the VID number will time out:</p> <p>for Permanent type—the number will never time out, and this is indicated by the digit 0.</p> <p>for Dynamic type—the Age reflects what is configured in the VLAN Aging Timeout parameter in the Configuration => VLAN tab of the AP or reflects a fewer number of minutes that represents the difference between what was configured and what has elapsed since the VID was learned. Each minute, the Age decreases by one until, at zero, the AP deletes the learned VID, but can it again from packets sent by elements that are beneath it in the network.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> NOTE</p> <p>Values in this Active Configuration block can differ from attempted values in configurations:</p> <p>A VLAN profile administered by the BAM subsystem in Prizm is capable of overriding any configured VLAN value, if the Configuration Source parameter in the AP is set to BAM.</p> <p>The AP can override the value that the SM has configured for SM Management VID Pass-Through.</p> </div>

VLAN Membership Tab of the SM

Figure 6 VLAN Membership tab of the SM

Account: root
Level: ADMINISTRATOR

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | VLAN | **VLAN Membership** | DiffServe | Protocol
Filtering | NAT | NAT Port Mapping | Unit Settings

Configuration => VLAN Membership

2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

VLAN Membership Configuration

VLAN Membership Table Configuration : (Range : 1 -- 4095)

Add Member Remove Member

VLAN Membership Table

VID Number	Type	Age
10	Static	

In the VLAN Membership tab, you may set the following parameter.

Table 13 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.

PPPoE Tab of the SM

Table 14 PPPoE tab of the SM

The screenshot displays the 'Configuration => PPPoE' interface for a subscriber module (5.4GHz - Subscriber Module - 0a-00-3e-52-14-8b). The 'PPPoE Configuration' section includes the following fields and options:

- PPPoE:** Enabled, Disabled
- Access Concentrator:** [Empty field]
- Service Name:** [Empty field]
- Authentication Type:** [None] (dropdown menu)
- User Name:** [None] (dropdown menu)
- Password:** [PAP] (dropdown menu)
- MTU:** Use MTU Received from PPPoE Server, Use User Defined MTU (1492)
- Timer Type:** [None] (dropdown menu)
- Timer Period:** [None] (dropdown menu)
- TCP MSS Clamping:** Keep Alive, Idle Timeout, Disabled

Below the configuration section is the 'PPPoE Manual Connect/Disconnect' area with 'Connect' and 'Disconnect' buttons. At the bottom, there are 'Save Changes' and 'Reboot' buttons.

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 will be 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. This is because the NAT Public IP will be received through the IPCP process of the PPPoE discovery stages.

The pre-requisites required are:

- NAT MUST be enabled on the SM
 - NAT DHCP Client will be disabled automatically. The NAT public IP will be received from the PPPoE Server.
 - NAT Public Network Interface Configuration will not be used and should be left to defaults. Also NAT Public IP DHCP will be 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 following PPPoE configuration parameters are available:

Table 15 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 will be implemented CHAP/PAP means that CHAP authentication will be attempted first, then PAP authentication. The same password is used for both types.
User Name	This is the CHAP/PAP user name that will be used if CHAP/PAP authentication is selected. If None is selected for authentication then this field is unused. This is limited to 32 characters.

Attribute	Meaning
Password	<p>This is the CHAP/PAP password that will be used if PAP authentication is selected. If None is selected for authentication then this field is unused. This is limited to 32 characters.</p>
MTU	<p>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.</p> <p>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 will be 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.</p>
Timer Type	<p>Keep Alive is the default timer type. This timer will enable a keepalive that will check the status of the link periodically. The user can set a keepalive period. If no data is seen from the PPPoE server for that period, the link will be taken down and a reconnection attempt will be started. For marginal links, the keep alive timer can be useful so that the session will stay alive over periodic dropouts. The keepalive timer should 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 should be in sync so that one side does not drop the session prematurely.</p> <p>Idle Timeout enables an idle timer that will check 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 will be dropped. Once data starts flowing from the customer again, the session will be 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 will be reestablished automatically.</p>

Attribute	Meaning
TCP MSS Clamping	<p>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 will be 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.</p>

NAT Port Mapping Tab of the SM

An example of the NAT Port Mapping tab in an SM is displayed in **Error! Reference source not found.**.

Table 16 NAT Port Mapping tab of the SM

The screenshot shows the 'Configuration => NAT Port Mapping' page for a 2.4GHz Subscriber Module (0a-00-3e-20-a5-48). The page has a navigation menu on the left and a main configuration area. The configuration area contains a table with 10 rows, each representing a port map. The columns are 'Port Map', 'Port Number', 'Protocol', and 'IP'. The 'Port Number' column contains values from 0 to 9. The 'Protocol' column contains 'All Protocols'. The 'IP' column contains values: 169.254.1.1, 169.254.1.2, 169.254.1.3, and 0.0.0.0. Below the table are 'Save Changes' and 'Reboot' buttons.

Port Map	Port Number	Protocol	IP
Port Map 1	0	All Protocols	169.254.1.1
Port Map 2	1	All Protocols	169.254.1.2
Port Map 3	2	All Protocols	169.254.1.3
Port Map 4	3	All Protocols	0.0.0.0
Port Map 5	4	All Protocols	0.0.0.0
Port Map 6	5	All Protocols	0.0.0.0
Port Map 7	6	All Protocols	0.0.0.0
Port Map 8	7	All Protocols	0.0.0.0
Port Map 9	8	All Protocols	0.0.0.0
Port Map 10	9	All Protocols	0.0.0.0

In the NAT Port Mapping tab of the SM, you may set the following parameters.

Table 17 SM PPPoE attributes

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

Task 3: Upgrading the software version and using CNUT

This task consists of the following procedures:

- [Checking the installed software version](#) on page 2-37
- [Upgrading to a new software version](#) on page 2-37

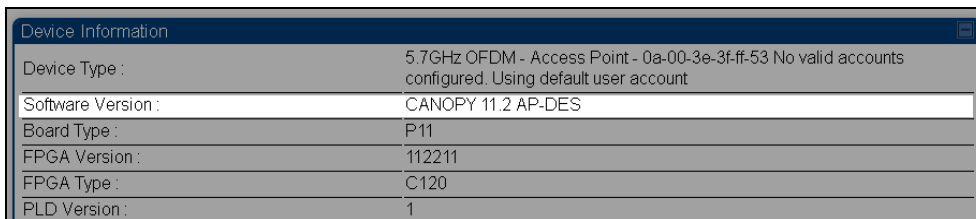
CAUTION

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.

Checking the installed software version

To check the installed software version, proceed as follows:

- 1** Select **Home** menu tab **General**.
- 2** Note the installed Software Version (near the top of the page):



Device Information	
Device Type :	5.7GHz OFDM - Access Point - 0a-00-3e-3f-ff-53 No valid accounts configured. Using default user account
Software Version :	CANOPY 11.2 AP-DES
Board Type :	P11
FPGA Version :	112211
FPGA Type :	C120
PLD Version :	1

- 3** Go to the support website (see [Contacting Cambium Networks](#) on page 1-9) and find Point-to-Multipoint software updates. Check that the latest PMP 450 software version (for example 13.0) is the same as the installed Software Version.
- 4** If the software needs to be upgraded to the latest version, perform [Upgrading to a new software version](#) on page 2-37.

Upgrading to a new software version

PMP 450 modules are upgraded using the Canopy Network Updater Tool (CNUT). The Canopy Network Updater Tool (CNUT) manages and automates the software and firmware upgrade process for a Canopy radio, CMMmicro, 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 while using the Autoupdate feature) to upgrade the modules.

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 1-9).

CNUT functions

The Canopy Network Updater Tool

- automatically discovers all network elements
 - executes a UDP command that initiates and terminates the Autoupdate mode within APs. This command is both secure and convenient:
 - For security, the AP accepts this command from only the IP address that you specify in the Configuration page of the AP.
 - For convenience, Network Updater automatically sets this Configuration parameter in the APs to the IP address of the Network Updater server when the server performs any of the update commands.
- allows you to choose 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.
 - Motorola supplies.

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

- organizes the display of elements (for example, by region or by AP cluster).
- allows you to
 - perform an operation on all elements in the group simultaneously.
 - set group-level defaults for telnet or 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 are behind an AP and thus, in this context, at a lower layer than the AP. Correctly portraying these layers in Network Updater is essential so that Network Updater can perform radio and AP cluster upgrades in an appropriate order.

NOTE

Correct layer information ensures that Network Updater does not command an AP that is behind another AP/SM pair (such as in a remote AP installation) to perform an upgrade at the same time as the SM that is feeding the AP. If this occurs, then the remote AP loses network connection during the upgrade (when the SM in front of the AP completes its upgrade and reboots).

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
- Set SNMP Accessibility
- Reset Unit

Software dependencies for CNUT

CNUT functionality requires

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

CNUT download

CNUT can be downloaded from the Cambium support website (see [Contacting Cambium Networks](#) on page 1-9).

Upgrading a module prior to deployment

To upgrade to a new software version, proceed as follows:

- 1** Go to the support website (see [Contacting Cambium Networks](#) on page 1-9) and find Point-to-Multipoint software updates. Download and save the required software image (for example CANOPY130BUILDOFFICIAL_DES.pkg3).
- 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 should 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.

Task 4: Configuring General and Unit settings

General Tab of the AP


Table 18 General tab of the AP

General	IP	Radio	SNMP	Quality of Service (QoS)	Security	Time	VLAN	VLAN Membership	DiffServ	Unit Settings
<p>Home Configuration Statistics Tools Account Quick Start Copyright Logoff Account: admin Level: ADMINISTRATOR</p>										
<p>Configuration => General</p> <p>5.7GHz - Access Point - 0a-00-3e-d5-b9-97</p> <p>Save Changes</p>										
<p>Device Type</p> <p>Device Setting : <input checked="" type="radio"/> AP <input type="radio"/> SM</p>										
<p>Link Speeds</p> <p>Link Speed : Auto 100F/100H/10F/10H</p>										
<p>Bandwidth Configuration Source</p> <p>Configuration Source : SM</p>										
<p>Sync Setting</p> <p>Sync Input : Sync to Received Signal (Power Port)</p>										
<p>Regional Settings</p> <p>Region Code : Europe</p>										
<p>Web Page Configuration</p> <p>Webpage Auto Update : 1 Seconds (0 = Disable Auto Update)</p>										
<p>Bridge Configuration</p> <p>Bridge Entry Timeout : 25 Minutes (Range : 25—1440 Minutes)</p> <p>Translation Bridging : <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>Send Untranslated ARP : <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>SM Isolation : Disable SM Isolation</p>										
<p>Update Application Information</p> <p>Update Application Address : 192.168.1.205</p>										
<p>MAC Control Parameters</p> <p>Dynamic Rate Adapt : 1x/2x</p>										
<p>TCP Settings</p> <p>Prioritize TCP ACK : <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</p>										
<p>Layer 2 Discovery Destination Address</p> <p>Multicast Destination Address : <input type="radio"/> Broadcast <input checked="" type="radio"/> LLDP Multicast</p> <p>Save Changes</p> <p>Reboot</p>										

The General tab of the AP contains many of the configurable parameters that define how the AP and the SMs in the sector operate.

Table 19 SM PPPoE attributes

Attribute	Meaning
Device Setting	You can temporarily transform an AP into an SM and thereby use the spectrum analyzer functionality. Otherwise, the selection for this parameter is AP .
Link Speeds	From the drop-down list of options, select the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected: Auto 100F/100H/10F/10H . In this setting, the two ends of the link automatically negotiate with each other whether the speed that they will use is 10 Mbps or 100 Mbps and whether the Ethernet traffic will be full duplex or half duplex. However, Ethernet links work best when either both ends are set to the same forced selection both ends are set to auto-negotiate and both have capability in least one common speed and traffic type combination.
Configuration Source	See Setting the Configuration Source
Sync Input	Specify the type of synchronization for this AP to use: Select Sync to Received Signal (Power Port) to set this AP to receive sync from a connected CMMmicro or CMM4. Select Sync to Received Signal (Timing Port) to set this AP to receive sync from a connected CMM2, an AP in the cluster, or an SM. Select Generate Sync Signal where the AP does not receive sync, and no other AP is active within the link range.

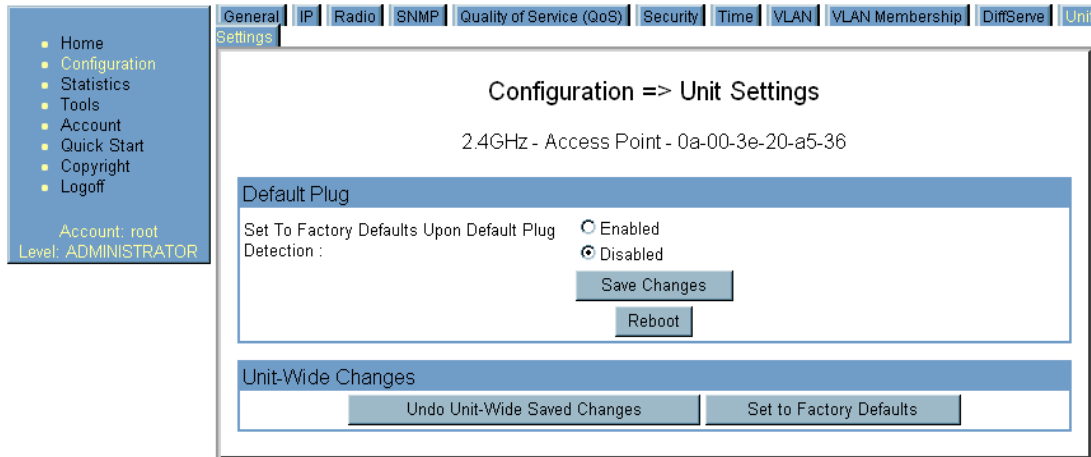
Attribute	Meaning
Region Code	<p>From the drop-down list, select the region in which the radio is operating. Selectable regions are:</p> <ul style="list-style-type: none"> • Australia • Brazil • Canada • Europe • India • Indonesia • Russia • Spain • Unites States • Other <p>When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard.</p> <p>Unlike selections in other parameters, your Region Code 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). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative Save Changes and Reboot cycles: one after the Region Code is set, and a second after related options are set.</p>
Webpage Auto Update	<p>Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.</p>
Bridge Entry Timeout	<p>Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> CAUTION</p> <p>An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.</p> </div>
Translation Bridging	<p>If you want the Translation Bridging feature, select Enabled. This has numerous implications.</p>

Attribute	Meaning
Send Untranslated ARP	<p>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.</p> <p>enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.</p> <p>If the Translation Bridging parameter is set to Disabled, then the Send Untranslated ARP parameter has no effect.</p>
SM Isolation	<p>Prevent or allow SM-to-SM communication by selecting from the following drop-down menu items:</p> <p>Disable SM Isolation (the default selection). This allows full communication between SMs.</p> <p>Block SM Packets from being forwarded. This prevents both multicast/broadcast and unicast SM-to-SM communication.</p> <p>Block and Forward SM Packets to Backbone. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.</p>
Update Application Address	<p>Enter the address of the server to access for software updates on this AP and registered SMs.</p>
2X Rate	<p>This parameter is present in only PMP 100 Series APs. You should generally keep this parameter set to Enabled to allow the module to automatically the operation rate. For troubleshooting, you may lock the rate down (Disabled), but be aware that this locks down the operation rate for all uplinks and downlinks across the sector.</p>
Dynamic Rate Adapt	<p>This parameter is present in only PMP 400 Series APs. You should generally keep this parameter set to Enabled to allow the module to automatically the operation rate. For troubleshooting, you may lock the rate down (Disabled), but be aware that this locks down the operation rate for all uplinks and downlinks across the sector.</p>
Prioritize TCP ACK	<p>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.</p>

Attribute	Meaning
Multicast Destination Address	<p>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 (CMMmicro, 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.</p> <p>In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to LLDP Multicast. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.</p> <p>Where the AP is not behind another device, the Broadcast mode will allow discovery of the AP.</p>
DHCP Relay Agent	<p>The AP may act as a DHCP relay for SMs and CPEs underneath it. The AP will make use of the DHCP Option 82 (DHCP Relay Agent Information) from RFC 3046 when performing relay functions. The AP offers two types of DHCP relay functionality:</p> <p>Full Relay Information. Configuring the DHCP Full Relay Operation will take broadcast DHCP packets and send them to a Unicast server in unicast mode. This way the DHCP requests and replies can be routed like any other UDP packet.</p> <p>Only Insert Option 82. This option leaves the DHCP request on its broadcast domain as opposed to DHCP Full Relay Operation which will turn it into a unicast packet.</p> <p>In order to accommodate setting up pools or classes for different VLANs, the Option 82 field will include information to tell the server what VLAN the client is on.</p>
DHCP Server (Name or IP Address)	<p>The DHCP relay server may be either a DNS name or a static IP address in dotted decimal notation. Additionally the management DNS domain name may be toggled such that the name of the DHCP relay server only needs to be specified and the DNS domain name is automatically appended to that name. The default DHCP relay server addresses is 255.255.255.255 with the appending of the DNS domain name disabled.</p>
Coordinates	<p>Physical radio location data may be configured via the Latitude, Longitude, and Height fields.</p>

Unit Settings Tab of the AP

Table 20 Unit Settings tab of the AP



The Unit Settings tab of the AP contains an option for how the AP should react when it detects a connected override plug. You may set this option as follows.

Table 21 AP Unit Settings attributes

Attribute	Meaning
Set to Factory Defaults Upon Default Plug Detection	<p>If Enabled is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, 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/default plug <i>cannot</i> see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.</p> <p>If Disabled is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug <i>can</i> see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.</p> <p>See Overriding Forgotten IP Addresses or Passwords on AP on Page 2-60.</p>

Attribute	Meaning
Undo Unit-Wide Saved Changes	When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.
Set to Factory Defaults	When you click this button, <i>all configurable parameters on all tabs</i> are reset to the factory settings.

General Tab of the SM

Table 22 General tab of the SM

The screenshot displays the 'Configuration => General' page for a 2.4GHz Subscriber Module (ID: 0a-00-3e-23-20-67). The interface includes a 'Save Changes' button at the top. The configuration sections are as follows:

- Link Speeds:** Link Speed is set to 'Auto 100F/100H/10F/10H'. Ethernet Link Enable/Disable is set to 'Enabled'.
- Regional Settings:** Region Code is set to 'United States'.
- Web Page Configuration:** Webpage Auto Update is set to '1' seconds.
- Bridge Configuration:** Bridge Entry Timeout is set to '25' minutes.
- MAC Control Parameters:** Power Up Mode With No 802.3 Link is set to 'Power up in Operational Mode'. Dynamic Rate Adapt is set to '1x/2x'.
- Frame Timing:** Frame Timing Pulse Gated is set to 'Enable (If SM out of sync then do not propagate the frame timing pulse)'.
- Layer 2 Discovery Destination Address:** Multicast Destination Address is set to 'LLDP Multicast'.


At the bottom of the configuration area, there are 'Save Changes' and 'Reboot' buttons.

In the General tab of the SM, you may set the following parameters.

Table 23 AP Unit Settings attributes

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.

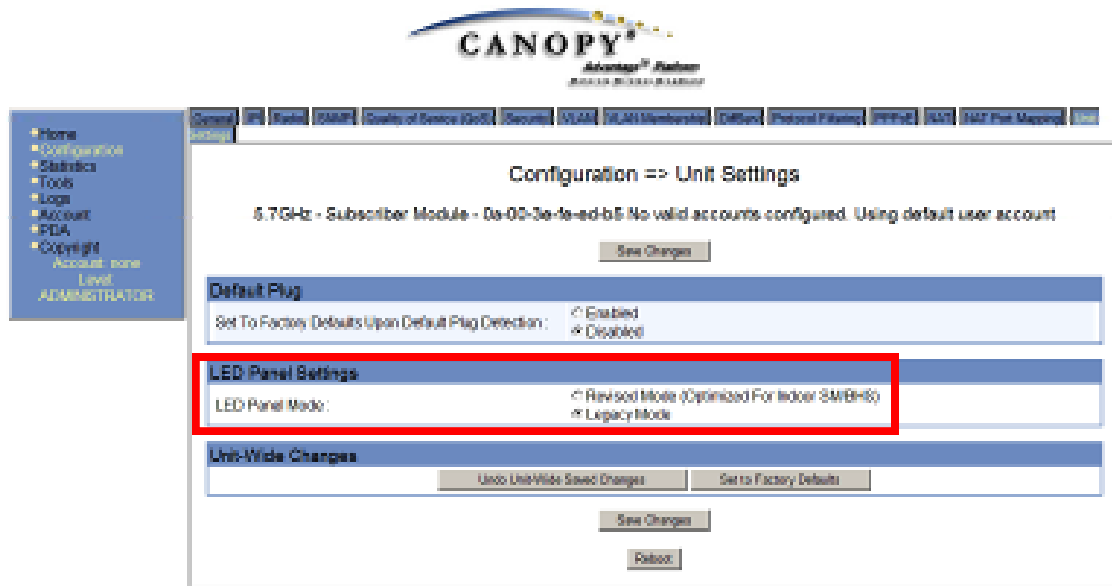
Attribute	Meaning
Ethernet Link Enable/Disable	<p>Specify whether to enable or disable Ethernet/802.3 connectivity on the wired port of the SM. This parameter has no effect on the wireless link. When you select Enable, this feature allows traffic on the Ethernet/802.3 port. This is the factory default state of the port. When you select Disable, this feature prevents traffic on the port. Typical cases of when you may want to select Disable include:</p> <ul style="list-style-type: none">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 Code	<p>This parameter allows you to set the region in which the radio will operate. When the appropriate region has been set, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard.</p> <p>The slave radio automatically inherits the DFS type of the master. This behavior ignores the value of the Region Code parameter in the slave, even when the value is None.</p> <p>Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), this parameter should always be set to the value that corresponds to the local region.</p>
Webpage Auto Update	<p>Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.</p>

Attribute	Meaning
Bridge Entry Timeout	<p>Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the AP encounters no activity with the SM (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.</p> <div data-bbox="654 552 1313 852" style="border: 1px solid black; padding: 5px;"> <p> CAUTION</p> <p>This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.</p> <p>An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.</p> </div>
SM Power Up Mode With No 802.3 Link	<p>This parameter is present in only PMP 100 Series SMs. Specify the default mode in which this SM will power up when the SM senses no Ethernet link. Select either</p> <p>Power Up in Aim Mode—the SM boots in an aiming mode. When the SM senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the module senses no Ethernet link within 15 minutes after power up, the SM carrier shuts off.</p> <p>Power Up in Operational Mode—the SM boots in Operational mode. The module attempts registration. This is the default selection.</p>
2X Rate	<p>This parameter is present in only PMP 100 Series (FSK) SMs. Whatever value that you set in this parameter is overridden by a lock-down to 1X operation, if that is configured in the AP. In some cases, disabling this parameter facilitates aiming. Be aware that a lock-down to 1X in the AP locks down the uplink and downlink between the AP and all SMs in its sector, and thus would affect traffic and performance across the entire sector. Hence, a temporary lock-down for aiming is better done in the individual SM.</p>

Attribute	Meaning
Dynamic Rate Adapt	<p>This parameter is present in only PMP 400 Series (OFDM) SMs. Whatever value that you set in this parameter is overridden by a lock-down to 1X or 2X operation, if that is configured in the AP. As with the 2X Rate parameter in a PMP 100 Series SM, a temporary lock-down to facilitate aiming may be helpful. Be aware that a lock-down to 1X or 2X in the AP locks down the uplink and downlink between the AP and all SMs in its sector, and thus would affect traffic and performance across the entire sector. Hence, a temporary lock-down for aiming is better done in the individual SM.</p>
Frame Timing Pulse Gated	<p>If this SM extends the sync pulse to a BH master or an AP, select either</p> <p>Enable—If this SM loses sync from the AP, then <i>do not</i> propagate a sync pulse to the BH timing master or other AP. This setting prevents interference in the event that the SM loses sync.</p> <p>Disable—If this SM loses sync from the AP, then propagate the sync pulse to the BH timing master or other AP.</p>
Multicast Destination Address	<p>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 (CMMmicro, 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.</p> <p>In this way, an SM can report to Prizm, for example, the multicast address of a connected remote AP, and thus allow Prizm to discover that AP. To allow this, set the message mode in the remote AP to LLDP Multicast. Set this parameter in the SM to Broadcast. The SM will pass this address in broadcast mode, and the CMMmicro will pass the address upward in the network, since it does not discard addresses that it receives in broadcast mode.</p> <p>Where the AP is not behind another device, the Broadcast mode will allow discovery of the AP.</p>
Coordinates	<p>Physical radio location data may be configured via the Latitude, Longitude, and Height fields.</p>

Unit Settings Tab of the SM

Table 24 Unit Settings tab of the SM



The Unit Settings tab of the SM contains an option for how the SM should react when it detects a connected override plug. You may set this option as follows.

Table 25 SM Unit Settings attributes

Attribute	Meaning
Set to Factory Defaults Upon Default Plug Detection	<p>If Enabled is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, 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/default plug <i>cannot</i> see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.</p> <p>If Disabled is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug <i>can</i> see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.</p> <p>See Overriding Forgotten IP Addresses or Passwords on AP on Page 2-60.</p>
Undo Unit-Wide Saved Changes	When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.
Set to Factory Defaults	When you click this button, <i>all configurable parameters on all tabs</i> are reset to the factory settings.

Time tab of the AP

Table 26 Unit Settings tab of the SM

NTP Server Configuration

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

NTP Server 1 (Name or IP Address) :

NTP Server 2 (Name or IP Address) :

NTP Server 3 (Name or IP Address) :

NTP Server(s) In Use : No NTP Server Configured

Current System Time

Time Zone :

System Time : 00:56:35 01/01/2011 UTC

Last NTP Time Update : 00:00:00 00/00/0000 UTC

Time and Date

Time : : : UTC

Date : / /

NTP Update Log

No entries.

You may set the time parameters as follows:

Table 27 AP 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.

Attribute	Meaning
NTP Server 1 (Name or IP Address) NTP Server 2 (Name or IP Address) NTP Server 3 (Name or IP Address)	<p>To have each log in the AP correlated to a meaningful time and date, either a reliable network element must pass time and date to the AP or you must set the time and date whenever a power cycle of the AP has occurred. A network element passes time and date in any of the following scenarios:</p> <ul style="list-style-type: none"> • A connected CMM2 or CMM4 passes time and date (GPS time and date, if received). • A connected CMMmicro passes the time and date (GPS time and date, if received), but only if both the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include NTP server functionality.) • A separate NTP server is addressable from the AP. <p>If the AP should obtain time and date from a CMMmicro, CMM4, or a separate NTP server, enter the IP address or DNS name of the CMM or NTP server on this tab. To force the AP to obtain time and date before the first (or next) 15-minute interval query of the NTP server, click Get Time through NTP.</p> <p>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.</p>
NTP Server(s) in Use	Lists the IP addresses of servers used for NTP retrieval.
Time Zone	<p>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, the offset will be set for the entire sector (SMs will be notified of the current Time Zone upon initial registration). If a Time Zone change is applied, the SMs will be notified of the change in a best effort fashion, meaning some SMs may not pick up the change until the next re-registration. Time Zone changes are noted in the Event Log of the AP and SM.</p>
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.

Attribute	Meaning
Date	This field may be used to manually set the system date of the radio.

Task 5: Configuring security

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

- [Isolating APs from the internet](#) on page 2-56: to ensure that APs are properly secured from external networks
- [Encrypting radio transmissions](#) on page 2-57: to configure the unit to operate with AES or DES wireless link security
- [Managing module access by passwords](#) on page 2-58: to set up the AP to require SMs to authenticate via the AP, Prizm, or RADIUS server
- [Filtering protocols and ports](#) on page 2-62: to filter (block) specified protocols and ports from leaving the system
- [Requiring SM Authentication](#) on page 2-61: to configure the network to only allow registration to authenticated SMs
- [Encrypting downlink broadcasts](#) on page 2-64: to encrypt downlink broadcast transmissions such as ARP and NetBIOS
- [Isolating SMs](#) on page 2-64: to prevent SMs in the same sector from directly communicating with each other
- [Filtering management through Ethernet](#) on page 2-65: to prevent management access to the SM via the radio's Ethernet port
- [Allowing management only from specified IP addresses](#) on page 2-65: to only allow radio management interface access from specified IP addresses
- [Configuring management IP by DHCP](#) on page 2-65: to allow the radio's management IP address to be assigned by a network DHCP server

Isolating APs from the internet

Ensure that the IP addresses of the APs in your network

- are not routable over the Internet.
- do not share the subnet of the IP address of your user.

RFC 1918, Address Allocation for Private Subnets, reserves for private IP networks three blocks of IP addresses that are not routable over the Internet:

- /8 subnets have one reserved network, 10.0.0.0 to 10.255.255.255.
- /16 subnets have 16 reserved networks, 172.16.0.0 to 172.31.255.255.
- /24 subnets have 256 reserved networks, 192.168.0.0 to 192.168.255.255.

Encrypting radio transmissions

Motorola fixed wireless broadband IP systems employ the following forms of encryption for security of the wireless link:

- DES–Data Encryption Standard, an over-the-air link option that uses secret 56-bit keys and 8 parity bits.
- AES–Advanced Encryption Standard, an extra-cost over-the-air link option that provides extremely secure wireless connections. AES uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.

DES Encryption

Standard modules provide DES encryption. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES Encryption does not affect the performance or throughput of the system.

AES Encryption

Motorola also offers fixed wireless broadband IP network products that provide AES encryption. AES uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. Because of this higher level of security, the government of the U.S.A. controls the export of communications products that use AES (among which the AES feature activation key is one) to ensure that these products are available in only certain regions and by special permit.

The distributor or reseller can advise service providers about current regional availability. AES products are certified as compliant with the Federal Information Processing Standards (FIPS) in the U.S.A. The National Institute of Standards and Technology (NIST) in the U.S.A. has specified AES for significantly greater security than that which DES provides. NIST selected the AES algorithm for providing the best combination of security, performance, efficiency, implementation, and flexibility. NIST collaborates with industry to develop and apply technology, measurements, and standards.

AES-DES Operability Comparisons

This section describes the similarities and differences between DES and AES products, and the extent to which they may interoperate.

Feature Availability

AES products run the same software as DES products. Thus feature availability and functionality are and will continue to be the same, regardless of whether AES encryption is enabled. All interface screens are identical. However, when encryption is enabled on the Configuration screen

- the AES product provides AES encryption.
- the DES product provides DES encryption.

AES and DES products use different FPGA (field-programmable gate array) loads. However, the AES FPGA will be upgraded as needed to provide new features or services similar to those available for DES products.

Canopy DES products cannot be upgraded to AES. To have the option of AES encryption, the operator must purchase AES products.

Interoperability

AES and DES products do not interoperate when enabled for encryption. For example, An AES AP with encryption enabled cannot communicate with DES SMs. Similarly, an AES Backhaul timing master module with encryption enabled cannot communicate with a DES Backhaul timing slave module.

However, if encryption is disabled, AES modules can communicate with DES modules.

Managing module access by passwords

Adding a User for Access to a Module

From the factory, each module has a preconfigured administrator-level account in the name `root`, which initially requires no associated password. This is the same `root` account that you may have used for access to the module by `telnet` or `ftp`. When you upgrade a module:

- an account is created in the name `admin`.
- both `admin` and `root` inherit the password that was previously used for access to the module:
 - the **Full Access** password, if one was set.
 - the **Display-Only Access** password, if one was set and no Full Access password was set.

NOTE

If you use Prizm, *do not* delete the `root` account from any module. If you use an NMS that communicates with modules through SNMP, *do not* delete the `root` account from any module unless you first can confirm that the NMS does not rely on the `root` account for access to the modules.

Each module supports four or fewer user accounts, regardless of account levels. The available levels are

- **ADMINISTRATOR**, who has full read and write permissions. This is the level of the `root` and `admin` users, as well as any other administrator accounts that one of them creates.
- **INSTALLER**, who has permissions identical to those of **ADMINISTRATOR** except that the installer cannot add or delete users or change the password of any other user.
- **GUEST**, who has no write permissions and only a limited view of General Status tab, and can log in as a user.

From the factory default state, configure passwords for both the `root` and `admin` account at the **ADMINISTRATOR** permission level, using the **Account, Change Users Password** tab. (If you configure only one of these, then the other will still require no password for access into it and thus remain a security risk.) If you are intent on configuring only one of them, delete the `admin` account. The `root` account is the only account that CNUT uses to update and Prizm uses to manage the module.

Figure 7 General Status tab view for GUEST-level account

- Home
- Copyright
- Login

Account: none
Level: GUEST

General Status

Home => General Status

5.7GHz - Access Point - 0a-00-3e-d5-b9-97

Device Information	
Device Type :	5.7GHz - Access Point - 0a-00-3e-d5-b9-97
Software Version :	CANOPY 9.4.2 AP-DES
Software BOOT Version :	CANOPYBOOT 1.0
Board Type :	P11
FPGA Version :	021909
FPGA Type :	C40
PLD Version :	1
Uptime :	01:38:17
System Time :	01:38:17 01/01/2001
Last NTP Time Update :	00:00:00 00/00/0000
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
DFS :	Normal Transmit
Antenna :	Vertical

Access Point Stats	
Registered SM Count :	1
GPS Sync Pulse Status :	Receiving Sync
Max Registered SM Count :	1

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Figure 8 SM Add User tab

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
- Login

Account: root
Level: ADMINISTRATOR

Change Users Password | **Add User** | Delete User

Account => Add User

5.7GHz - Subscriber Module - 0a-00-3e-f0-25-d9

Add User

User Name :	<input style="width: 80%;" type="text"/>
Level :	INSTALLER
New Password :	<input style="width: 80%;" type="password"/>
Confirm Password :	<input style="width: 80%;" type="password"/>

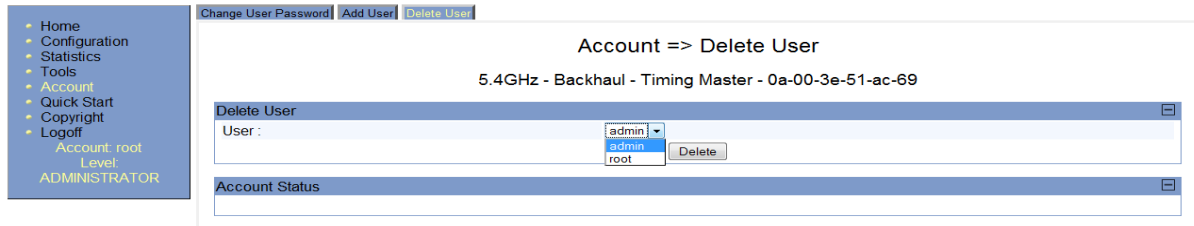
Account Status

After a password has been set for any ADMINISTRATOR-level account, initial access to the module GUI opens the view of GUEST level.

Deleting a User from Access to a Module

The Account => Delete User tab provides a drop-down list of configured users from which to select the user you want to delete.

Figure 9 Delete User tab of the SM



Accounts that cannot be deleted are

- the current user's own account.
- the last remaining account of ADMINISTRATOR level.

Overriding Forgotten IP Addresses or Passwords on AP and SM

A small adjunctive product allows you to temporarily override some AP/SM settings and thereby regain control of the module. This override plug is needed for access to the module in any of the following cases:

- You have forgotten either
 - the IP address assigned to the module.
 - the password that provides access to the module.
- The module has been locked by the No Remote Access feature.
- You want local access to a module that has had the 802.3 link disabled in the Configuration page.

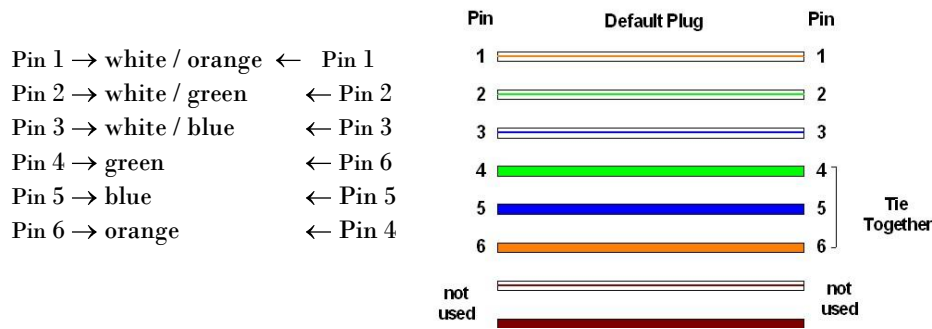
You can configure the module such that, when it senses the override plug, it responds by either

- resetting the LAN1 IP address to 169.254.1.1, allowing access through the default configuration without *changing* the configuration, whereupon you will be able to view and reset any non-default values as you wish.
- resetting all configurable parameters to their factory default values.

Acquiring the Override Plug

You can either purchase or fabricate an override plug as follows. To purchase an override plug for a nominal fee, order the plug at <http://www.best-tronics.com/motorola.htm>. To fabricate an override plug, perform the following steps.

- 1** Install an RJ-11 6-pin connector onto a 6-inch length of CAT 5 cable
- 2** Pin out all 6-pins.
- 3** Short (solder together) Pins 4 and 6 on the other end. Do not connect any other wires to anything.

Figure 10 RJ-11 pinout for the override plug

Using the Override Plug

NOTE

While the override plug is connected to a module, the module can neither register nor allow registration of another module.

To regain access to the module, perform the following steps.

- 1** Insert the override plug into the RJ-11 GPS utility port of the module.
- 2** Power cycle by removing, then re-inserting, the Ethernet cable.
RESULT: The module boots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.
- 3** Wait approximately 30 seconds for the boot to complete.
- 4** Remove the override plug.
- 5** Set passwords and IP address as desired.
- 6** Change configuration values if desired.
- 7** Click the Save Changes button.
- 8** Click the Reboot button.

Requiring SM Authentication

Through the use of Prizm, a shared AP key, a BAM (Bandwidth and Authentication Manager) server, or an external RADIUS (Remote Authentication Dial In User Service) server, you can enhance network security by requiring SMs to authenticate when they register. Three keys and a random number are involved in authentication as follows:

- factory-set key in each SM. Neither the subscriber nor the network operator can view or change this key.

- authentication key, also known as authorization key and skkey. This key matches in the SM and AP as the **Authentication Key** parameter, and in the Prizm database.
- random number, generated by Prizm or BAM and used in each attempt by an SM to register and authenticate. The network operator can view this number.
- session key, calculated separately by the SM and Prizm or BAM, based on both the authentication key (or, by default, the factory-set key) and the random number. Prizm or BAM sends the session key to the AP. The network operator cannot view this key.

None of the above keys is ever sent in an over-the-air link during an SM registration attempt. However, with the assumed security risk, the operator can create and configure the **Authentication Key** parameter. See **Authentication Key** on Page 2-73.

Filtering protocols and ports

You can filter (block) specified protocols and ports from leaving the SM 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.

Protocol and port filtering is set per SM. Except for filtering of SNMP ports, filtering occurs as packets leave the SM. If an SM is configured to filter SNMP, then SNMP packets are blocked from entering the SM and, thereby, from interacting with the SNMP portion of the protocol stack on the SM.

Port Filtering with NAT Enabled

Where NAT is enabled, you can filter only the three user-defined ports. The following are example situations in which you can configure port filtering where NAT is enabled.

- To block a subscriber from using FTP, you can filter Ports 20 and 21 (the FTP ports) for both the TCP and UDP protocols.
- To block a subscriber from access to SNMP, you can filter Ports 161 and 162 (the SNMP ports) for both the TCP and UDP protocols.



In only the SNMP case, filtering occurs before the packet interacts with the protocol stack.

Protocol and Port Filtering with NAT Disabled

Where NAT is disabled, you can filter both protocols and the three user-defined ports. Using the check boxes on the interface, you can either

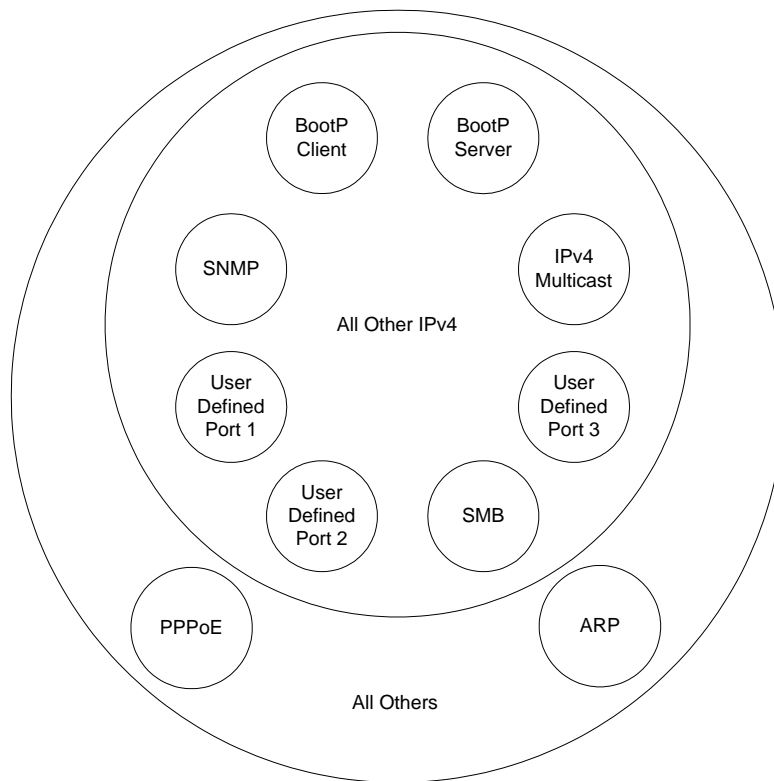
- allow all protocols except those that you wish to block.
- block all protocols except those that you wish to allow.

You can allow or block any of the following protocols:

- PPPoE (Point to Point Protocol over Ethernet)

- Any or all of the following IPv4 (Internet Protocol version 4) protocols:
 - SMB (Network Neighborhood)
 - SNMP
 - Up to 3 user-defined ports
 - All other IPv4 traffic
- Uplink Broadcast
- ARP (Address Resolution Protocol)
- All others

Figure 11 Categorical protocol filtering



The following are example situations in which you can configure protocol filtering where NAT is disabled:

- If you block a subscriber from only PPoE and SNMP, then the subscriber retains access to all other protocols and all ports.
- If you block PPoE, IPv4, and Uplink Broadcast, and you also check the **All others** selection, then only Address Resolution Protocol is not filtered.

. Further information is provided under **Protocol Filtering Tab of the SM** on Page [2-76](#).

Figure 12 Ports filtered per protocol selection

Protocol Selected	Port Filtered (Blocked)
SMB	Destination Ports 137 TCP and UDP, 138 UDP, 139 TCP, 445 TCP

Protocol Selected	Port Filtered (Blocked)
SNMP	Destination Ports 161 TCP and UDP, 162 TCP and UDP
Bootp Client	Source Port 68 UDP
Bootp Server	Source Port 67 UDP

Encrypting downlink broadcasts

An AP can be enabled to encrypt downlink broadcast packets such as the following:

- ARP
- NetBIOS
- broadcast packets containing video data on UDP.

The encryption used is DES for a DES module, and AES for an AES module. Before the Encrypt Downlink Broadcast feature is enabled on the AP, air link security should be enabled on the AP.

Isolating SMs

In an AP, you can prevent SMs in the sector from directly communicating with each other. In CMMmicro Release 2.2 or later and the CMM4, you can prevent connected APs from directly communicating with each other, which prevents SMs that are in different sectors of a cluster from communicating with each other.

In the AP, the **SM Isolation** parameter is available in the General tab of the Configuration web page. In the drop-down menu for that parameter, you can configure the SM Isolation feature by any of the following selections:

- **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 would have been handled SM to SM, through the Ethernet port of the AP.

In the CMMmicro and the CMM4, SM isolation treatment is the result of how you choose to manage the port-based VLAN feature of the embedded switch, where you can switch all traffic from any AP to an uplink port that you specify. However, this is not packet level switching. It is not based on VLAN IDs. See the **VLAN Port Configuration** parameter in the dedicated user guide that supports the CMM product that you are deploying.

Filtering management through Ethernet

You can configure the SM to disallow any device that is connected to its Ethernet port from accessing the IP address of the SM. If you set the **Ethernet Access Control** parameter to **Enabled**, then

- no attempt to access the SM management interface (by http, SNMP, telnet, ftp, or tftp) through Ethernet can succeed.
- any attempt to access the SM management interface over the air (by IP address, presuming that **LAN1 Network Interface Configuration, Network Accessibility** is set to **Public**, or by link from the Session Status or Remote Subscribers tab in the AP) is unaffected.

Allowing management only from specified IP addresses

The Security tab of the Configuration web page in the AP and SM includes the **IP Access Control** parameter. You can specify one, two, or three IP addresses that should be allowed to access the management interface (by http, SNMP, telnet, ftp, or tftp).

If you select

- **IP Access Filtering Disabled**, then management access is allowed from any IP address, even if the **Allowed Source IP 1 to 3** parameters are populated.
- **IP Access Filtering Enabled**, and specify at least one address in the **Allowed Source IP 1 to 3** parameter, then management access is limited to the specified address(es). If you intend to use Prizm to manage the element, then you must ensure that the IP address of the Prizm server is listed here.

Configuring management IP by DHCP

The IP tab in the Configuration web page of every radio contains a **LAN1 Network Interface Configuration, DHCP State** parameter that, if enabled, causes the IP configuration (IP address, subnet mask, and gateway IP address) to be obtained through DHCP instead of the values of those individual parameters. The setting of this DHCP state parameter is also viewable, but is not settable, in the Network Interface tab of the Home page.

In the SM, this parameter is settable

- in the NAT tab of the Configuration web page, but only if NAT is enabled.
- in the IP tab of the Configuration web page, but only if the **Network Accessibility** parameter in the IP tab is set to **Public**.

Denying All Remote Access

Wherever the No Remote Access feature is enabled by the following procedure, physical access to the module is required for

- any change in the configuration of the module.
- any software upgrade in the module.

Where additional security is more important than ease of network administration, you can disable all remote access to a module as follows. After this procedure, no access to the module is possible through HTTP, SNMP, FTP, or telnet over an RF link.

To deny remote access to the module, perform the following steps:

- 1** Insert the override plug into the RJ-11 GPS utility port of the module
- 2** Power up or power cycle the module
- 3** Access the web page <http://169.254.1.1/lockconfig.html>
- 4** Click the checkbox
- 5** Save the changes
- 6** Remove the override plug
- 7** Reboot the module

Reinstating Remote Access Capability

Where ease of network administration is more important than the additional security that the No Remote Access feature provides, this feature can be disabled as follows. After this procedure, access to the module is possible through HTTP, SNMP, FTP, or telnet over an RF link.

To reinstate all remote access to the module, perform the following steps:

- 1** Insert the override plug into the RJ-11 GPS utility port of the module
- 2** Power up or power cycle the module
- 3** Access the web page <http://169.254.1.1/lockconfig.html>
- 4** Click the check box to uncheck the field
- 5** Save the changes
- 6** Remove the override plug
- 7** Reboot the module

Security Tab of the AP

Figure 13 Security tab of the AP

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

Airlink Security	
Encryption :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

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

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

IP Access Filtering	
IP Access Control :	<input type="radio"/> IP Access Filtering Enabled - Only allow access from IP addresses specified below <input checked="" type="radio"/> IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0
Allowed Source IP 2 :	0.0.0.0
Allowed Source IP 3 :	0.0.0.0

In the Security tab of the AP, you may set the following parameters.

Table 28 AP Security attributes

Attribute	Meaning
Authentication Mode	<p>If the AP has authentication capability, then you can use this field to select from among the following authentication modes:</p> <p>Disabled—the AP requires no SMs to authenticate.</p> <p>Authentication Server —the AP requires any SM that attempts registration to be authenticated in BAM or Prizm before registration.</p> <p>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 will be able to register.</p> <p>RADIUS AAA - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(es) configured here must match the IP address(es) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.</p>
Authentication Server DNS Usage	<p>The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.</p>
Authentication Server 1 to 5	<p>Enter the IP address of the authentication server (RADIUS, Prizm, or BAM) and the Shared Secret configured in the authentication server.</p> <p>When Authentication Mode RADIUS AAA is selected, the default value of Shared Secret is “CanopySharedSecret”. The Shared Secret may consist of up to 32 ASCII characters.</p>
Radius Port	<p>This field allows the operator to configure a custom port for RADIUS server communication. The default value is 1812.</p>
Authentication Key	<p>The authentication key is a 32-character hexadecimal string used when Authentication Mode is set to AP PreShared Key. By default, this key is set to 0xFF.</p>

Attribute	Meaning
Select Key	<p>This option allows operators to choose which authentication key is used:</p> <p>Use Key above means that the key specified in Authentication Key is used for authentication</p> <p>Use Default Key means that a default key (based off of the SM's MAC address) will be used for authentication</p>
Encryption	<p>Specify the type of airlink security to apply to this AP:</p> <p>Encryption Disabled provides no encryption on the air link. This is the default mode.</p> <p>Encryption Enabled provides encryption, using a factory-programmed secret key that is unique for each module.</p>
Encrypt Downlink Broadcast	<p>When Encryption Enabled is selected in the Airlink Security parameter (described above) and Enable is selected in the Encrypt Downlink Broadcast parameter, the AP encrypts downlink broadcast packets as DES where the AP is DES capable.</p> <p>AES where the AP is AES capable.</p>
SM Display of AP Evaluation Data	<p>You can use this field to suppress the display of data about this AP on the AP Evaluation tab of the Tools page in all SMs that register.</p>
Web, Telnet, FTP Session Timeout	<p>Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the AP.</p>
IP Access Control	<p>You can permit access to the AP from any IP address (IP Access Filtering Disabled) or limit it to access from only one, two, or three IP addresses that you specify (IP Access Filtering Enabled). If you select IP Access Filtering Enabled, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted from any IP address, including access and management by Prizm.</p>
Allowed Source IP 1 to 3	<p>If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the AP from any IP address. You may populate as many as all three.</p> <p>If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.</p>

Protocol Filtering tab of the AP

Table 29 Protocol Filtering tab of the AP

The image shows two screenshots of the AP configuration interface. The top screenshot is titled "Packet Filter Configuration" and shows a list of "Packet Filter Types" with checkboxes. The "Filter Direction" is set to "Upstream". The bottom screenshot is titled "User Defined Port Filtering Configuration" and shows three rows for "Port #1", "Port #2", and "Port #3". Each row has a text input field for the port number (all set to 0) and radio buttons for "Enabled" and "Disabled" for both TCP and UDP protocols. In all cases, "Disabled" is selected.

Packet Filter Configuration

Packet Filter Types :

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

Filter Direction :

- Upstream
- Downstream

User Defined Port Filtering Configuration

Port #1 : (Decimal Value)

TCP : Enabled Disabled

UDP : Enabled Disabled

Port #2 : (Decimal Value)

TCP : Enabled Disabled

UDP : Enabled Disabled

Port #3 : (Decimal Value)

TCP : Enabled Disabled

UDP : Enabled Disabled

In the Protocol Filtering tab of the AP, you may set the following parameters.

Table 30 AP Protocol Filtering attributes

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

Port configuration tab of the AP

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

Table 31 Port configuration tab of the AP

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

In the Port Configuration tab of the AP, you may set the following parameters.

Table 32 AP Port Configuration attributes

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.
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.

Security Tab of the SM

Table 33 Security tab of the SM

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

AAA Authentication Settings	
Enforce Authentication :	Disable
Phase 1 :	eapTls
Phase 2 :	MSCHAPv2
Identity/Realm :	<input type="radio"/> Enable Realm <input checked="" type="radio"/> Disable Realm Identity <input type="text"/> @ Realm <input type="text"/>
Username :	0a-00-3e-3f-f53 <input type="button" value="Use Default Username"/>
Password :	*****
Confirm Password :	<input type="text"/>

RADIUS Certificate Settings	
Upload Certificate File	
File: <input type="text"/>	<input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	
<input type="button" value="Import Certificate"/> <input type="button" value="Use Default Certificates"/> <i>This will delete all current certificates</i>	

Certificate 1	
C =US S =Illinois O =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 <input type="button" value="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 <input type="button" value="Delete"/>	


Session Timeout	
Web, Telnet, FTP Session Timeout :	<input type="text"/> 600 <input type="text"/> Seconds

SM Management Interface Access via Ethernet Port	
Ethernet Access :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled


IP Access Filtering	
IP Access Control :	<input type="radio"/> IP Access Filtering Enabled - Only allow access from IP addresses specified below <input checked="" type="radio"/> IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	<input type="text"/> 0.0.0.0
Allowed Source IP 2 :	<input type="text"/> 0.0.0.0
Allowed Source IP 3 :	<input type="text"/> 0.0.0.0

In the Security tab of the SM, you may set the following parameters.

Table 34 AP Security attributes

Attribute	Meaning
Authentication Key	Only if the AP to which this SM will register requires authentication, specify the key that the SM should use when authenticating. For alpha characters in this hex key, use only upper case.
Select Key	<p>The Use Default Key selection specifies the predetermined key for authentication in BAM or Prizm.</p> <p>The Use Key above selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the BAM or Prizm database.</p> <div data-bbox="646 661 1450 890" style="border: 1px solid black; padding: 5px;"> <p> NOTE</p> <p>The SM and BAM or Prizm pad the key of any length by the addition of leading zeroes, and if the entered keys match, authentication attempts succeed. However, Motorola recommends that you enter 32 characters to achieve the maximal security from this feature.</p> </div>
Enforce Authentication	The SM may enforce authentication types of AAA and BAM/PreSharedKey . The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM will lockout 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.

Attribute	Meaning
Identity/Realm	<p>If Realms are being used, select Enable Realm and configure an outer identity in the Identity field and a Realm in the Realm field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default Identity is “anonymous”. The Identity can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default Realm is “canopy.net”. The Realm can also be up to 128 non-special alphanumeric characters.</p> <p>Configure an outer Identity in the Username field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity Username is “anonymous”. The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.</p>
Username	<p>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.</p>
Password	<p>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</p>
Upload Certificate File	<p>To upload a certificate manually to an SM, first load it in a known place on your PC or network drive, then click on a Delete button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on Choose File, browse to the location of the certificate, and click the Import Certificate button, and then reboot the radio to use the new certificate.</p> <p>When a certificate is in use, after the SM successfully registers to an AP, an indication of In Use will appear in the description block of the certificate being used.</p> <p>The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system.</p> <p>Up to 2 certificates can be resident on an SM. An installed certificate can be deleted by clicking the Delete button in the certificate’s description block on the Configuration > Security tab. To restore the 2 default certificates, click the Use Default Certificates button in the RADIUS Certificate Settings parameter block and reboot the radio.</p>
Web, Telnet, FTP Session Timeout	<p>Enter the expiry in seconds for remote management sessions via HTTP, telnet, or FTP access to the SM.</p>

Attribute	Meaning
Ethernet Access Control	<p>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.</p> <div data-bbox="646 590 1450 852" style="border: 1px solid black; padding: 5px;"> <p> NOTE</p> <p>This setting does not prevent a device connected to the Ethernet port from accessing the management interface of <i>other SMs</i> in the network. To prevent this, use the IP Access Filtering Enabled selection in the IP Access Control parameter of the SMs in the network. See IP Access Control below.</p> </div> <p>If you want to allow management access through the Ethernet port, select Ethernet Access Enabled. This is the factory default setting for this parameter.</p>
IP Access Control	<p>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, including access and management by Prizm.</p>
Allowed Source IP <i>1 to 3</i>	<p>If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the SM from any IP address. You may populate as many as all three.</p> <p>If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.</p>

Protocol Filtering Tab of the SM

Table 35 Protocol Filtering tab of the SM

The screenshot displays the 'Protocol Filtering' configuration interface for a Subscriber Module (SM). The breadcrumb trail at the top indicates the path: General > IP > Radio > SNMP > Quality of Service (QoS) > Security > VLAN > VLAN Membership > DiffServe > Protocol Filtering > NAT > NAT Port Mapping > Unit Settings.

The main title is 'Configuration => Protocol Filtering' for the device '2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48'. The 'Packet Filter Configuration' section lists several protocols that can be filtered, each with a checkbox: PPPoE, All IPv4, SMB (Network Neighborhood), SNMP, Bootp Client, Bootp Server, IPv4 Multicast, User Defined Port 1 (See Below), User Defined Port 2 (See Below), User Defined Port 3 (See Below), All other IPv4, ARP, and All others.

The 'User Defined Port Filtering Configuration' section contains three identical blocks for Port #1, Port #2, and Port #3. Each block includes a text input field for the port number (set to 0), and radio buttons for 'Enabled' and 'Disabled' for both TCP and UDP protocols. The 'Disabled' option is selected for all.

At the bottom of the configuration area, there are two buttons: 'Save Changes' and 'Reboot'.

In the Protocol Filtering tab of the SM, you may set the following parameters.

Table 36 AP Protocol Filtering attributes

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

Attribute	Meaning
Packet Filter Types	<p>For any box selected, the Protocol and Port Filtering feature blocks the associated protocol type.</p> <p>To filter packets in any of the user-defined ports, you must do all of the following:</p> <p>Check the box for User Defined Port <i>n</i> (See Below) in the Packet Filter Types section of this tab.</p> <p>In the User Defined Port Filtering Configuration section of this tab, both provide a port number at Port #<i>n</i>.</p> <p>check TCP, UDP, or both.</p> <p>If the DHCP state parameter is set to Enabled in the Configuration => IP tab of the SM, <i>do not</i> check the Bootp Client option for Packet Filter Types in its Protocol Filtering tab, because doing so would 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.</p>
User Defined Port Filtering Configuration	<p>You can specify ports for which to block subscriber access, regardless of whether NAT is enabled.</p>

Port configuration tab of the SM

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

Figure 14 Port Configuration tab of the SM

Port Configuration		
FTP Port :	<input type="text" value="21"/>	Default port number is 21
HTTP Port :	<input type="text" value="80"/>	Default port number is 80
SNMP Port :	<input type="text" value="161"/>	Default port number is 161
SNMP Trap Port :	<input type="text" value="162"/>	Default port number is 162

In the Port Configuration tab of the SM, you may set the following parameters.

Table 37 SM Port Configuration attributes

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.
SNMP Port	The listen port on the device used for SNMP communication.
SNMP Trap Port	The destination port used on the device to which SNMP traps are sent.

Task 6: Configuring radio parameters

Radio tab of the AP

Figure 15 Radio tab of the AP

Radio Configuration	
Radio Frequency Carrier :	None
Alternate Frequency Carrier 1 :	None
Alternate Frequency Carrier 2 :	None
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	One Quarter
Color Code :	0 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Sector ID :	0
Signal to Noise Ratio Calculation :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

MAC Control Parameters	
Downlink Dynamic Rate Adapt :	1x2x3x
Uplink Dynamic Rate Adapt :	1x2x3x

Frame Configuration	
Max Range :	2 Miles (Range: 1— 40 miles)
Downlink Data :	75 % (Range: 10 — 90 %)
Control Slots :	0 (Range: 0 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)


Power Control	
Transmitter Output Power :	-30 dBm (Range: -30 — +21 dBm)
External Gain :	0 dB (Range: 0 — 35 dB)
SM Receive Target Level :	-55 dBm (Range : -40—80 dBm)

The Radio tab of the AP contains some of the configurable parameters that define how the AP operates.

Table 38 AP Radio attributes


Attribute	Meaning
Radio 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.


Attribute	Meaning
Alternate Frequency Carrier 1	<p>If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:</p> <ol style="list-style-type: none">1. Click the General tab.2. Set the Region Code parameter from its drop-down list.3. Click the Save Changes button.4. Click the Reboot button.5. Click the Radio tab. <p>From the drop-down list, select the frequency that the AP should switch to if it detects a radar signature on the frequency configured in the Radio Frequency Carrier parameter.</p>
Alternate Frequency Carrier 2	<p>From the drop-down list, select the frequency that the AP should switch to if it detects a radar signature on the frequency configured in the Alternate Frequency Carrier 1 parameter.</p>

Attribute	Meaning
Cyclic Prefix	<p>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 1/4 cyclic prefix means that for every 4 bits of throughput data transmitted, an additional bit is used. A 1/8 cyclic prefix means that for every 8 bits of throughput data transmitted, an additional bit is used, and a 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.</p> <p>PMP 450 radios use a default cyclic prefix of 1/4 that is configurable by the operator to 1/8 or 1/16. The cyclic prefix is set on the Configuration > Radio page of the AP. Changing the default from 1/4 to 1/8 can increase throughput by ~12% (assuming a 75% duty cycle) in installations with low multipath conditions. Moving from a 1/8 cyclic prefix to a 1/16 cyclic prefix can increase throughput by another ~12%. It is recommended to test 1/8 or 1/16 cyclic prefix configurations to determine actual performance based on RF conditions. Deploying networks using 1/8 or 1/16 cyclic prefixes is feasible in all but the worst multi-path environments (urban areas with buildings causing many reflections).</p> <p>During installation use Link Tests to confirm link quality per standard installation and alignment procedures. If a Link Test shows low throughput or low efficiency, consider changing the Cyclic Prefix to 1/4 on <i>both</i> the AP and SM along with other standard installation troubleshooting procedures such as re-aiming, off-axis aiming, changing location, raising or lowering the height of the radio, adjusting the Transmission Power up or down, or identifying and mitigating sources of interference.</p> <div data-bbox="597 1243 1448 1398" style="border: 1px solid black; padding: 5px;"> <p> CAUTION</p> <p>The cyclic prefix must be set the same on both the AP and the SM. If they don't match, the SM will not register to the AP.</p> </div>
Color Code	<p>Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP <i>must</i> match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.</p> <p>Color code allows you to force an SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (<i>not</i> all 255 color codes).</p>

Attribute	Meaning
Subscriber Color Code Rescan (When not on a Primary Color Code)	<p>This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code.</p> <p>The time (in minutes) for a subscriber to rescan (if this AP is not configured with the SM's primary color code). This timer will only fire once – if the Subscriber Color Code Wait Period for Idle timer is configured with a nonzero value and the Subscriber Color Code Rescan expires, the Subscriber Color Code Wait Period for Idle will be started. If the Subscriber Color Code Wait Period for Idle timer is configured with a zero value and the Subscriber Color Code Rescan timer expires, the SM will immediately go into rescan mode</p>
Subscriber Color Code Wait Period for Idle	<p>The time (in minutes) for a subscriber to rescan while idle (if this AP is not configured with the SM's primary color code). This timer will fire periodic events. The fired event determines if any RF unicast traffic (either inbound or outbound) has occurred since the last event. If the results of the event determine that no RF unicast traffic has occurred (SM is idle), then the subscriber will rescan.</p>
Installation Color Code	<p>With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. SMs with Installation Color Code enabled will first try any configured Color Code values first, then will use the Installation Color Code feature as a last result to connect to the AP. The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message “SM is registered via ICC – Bridging Disabled!” is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the Rescan APs functionality on the AP Eval page).</p>
Power Save Mode	<p>Select either</p> <p>Enabled (the default), to reduce module power consumption by approximately 10% without affecting the transmitter output power. This is the recommended setting.</p> <p>Disabled, to continue normal power consumption, but do so only under guidance from technical support.</p>
Sector ID	<p>Specify a number in the range 1 to 6 to associate with this AP. The Sector ID setting does not affect the operation of the AP. On the AP Evaluation tab of the Tools page in the SM, the Sector ID field identifies the AP that the SM sees. The following steps may be useful:</p> <ol style="list-style-type: none"> 1. Assign a unique Sector ID to each sector in an AP cluster. 2. Repeat the assignment pattern throughout the entire system.

Attribute	Meaning												
Signal to Noise Ratio Calculation	<p>Enabling this parameter allows operators to use Signal-to-Noise calculations to monitor link quality.</p> <p>The Signal-to-Noise Ratio may be monitored on the AP's Session Status page, Link Capacity Test page, and Link Status page.</p> <p>See the table below for required Signal-to-Noise Ratios required for each modulation state:</p> <table border="1" data-bbox="587 520 1354 739"> <thead> <tr> <th>Modulation</th> <th>Downlink</th> <th>Uplink</th> </tr> </thead> <tbody> <tr> <td>1X</td> <td>7 dB</td> <td>9 dB</td> </tr> <tr> <td>2X</td> <td>15 dB</td> <td>16 dB</td> </tr> <tr> <td>3X</td> <td>23 dB</td> <td>24 dB</td> </tr> </tbody> </table> <p>Note that locking a radio a lower modulation may result in a lower SNR ratio reading that a higher modulation. For example an AP/SM pair that is getting a SNR of 23/29 dB for downlink/uplink when modulation is set to 1X/2X/3X gets 22/27 dB for a setting of 1X/2X. And when set to 1X (No rate adapt) the SNR reads 12/18 dB. For highest SNR calculation the rate adapt must be set to its highest rate adapt modulation.</p>	Modulation	Downlink	Uplink	1X	7 dB	9 dB	2X	15 dB	16 dB	3X	23 dB	24 dB
Modulation	Downlink	Uplink											
1X	7 dB	9 dB											
2X	15 dB	16 dB											
3X	23 dB	24 dB											
Max Range	<p>Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which an SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance</p> <ul style="list-style-type: none"> • does not increase the power of transmission from the AP. • can reduce aggregate throughput. <p>Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you <i>must</i> set this parameter on all other APs in the cluster exactly the same, except as described in the NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).</p> <p>For the PMP 450 Series AP, the typical maximum range achievable depends on the operation mode as follows:</p> <ul style="list-style-type: none"> • 5 miles (8 km) in 1X operation • 2.5 miles (4 km) in 2X operation • 1.25 miles (2 km) in 3X operation <p>A value of 15 for this parameter decreases the number of available data slots by 1. With a higher value, the number is further decreased as the AP compensates for the expected additional air delay.</p>												

Attribute	Meaning
Downlink Data	<p>Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 6 Mb, then 75% specified for this parameter allocates 4.5 Mb for the downlink and 1.5 Mb for the uplink. The default for this parameter is 75%.</p> <div data-bbox="592 451 1442 548" style="border: 1px solid black; padding: 5px;"><p> NOTE You must set this parameter exactly the same for all APs in a cluster.</p></div>

Attribute	Meaning										
Control Slots	<p>Field results have indicated that, in general, systems perform better with a slightly higher number of control slots than previously recommended. If you are experiencing latency or SM-servicing issues, increasing the number of control slots may increase system performance, depending on traffic mix over time.</p> <p>Use care when changing the control slot configuration of only some APs, because changes affect the uplink/downlink ratio and can cause collocation issues.</p> <div data-bbox="600 594 1450 821" style="border: 1px solid black; padding: 5px;"> <p> NOTE</p> <p>Change control slot configuration in an operating, stable system cautiously and with a back-out plan. After changing a control slot configuration, monitor the system closely for problems as well as improvements in system performance..</p> </div> <p style="text-align: center;">Table 39: Control slot settings for all OFDM APs in cluster</p> <table border="1" data-bbox="727 932 1318 1314" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th data-bbox="734 940 1052 1096">Number of SMs that Register to the AP</th> <th data-bbox="1052 940 1312 1096">Number of Control Slots Recommended</th> </tr> </thead> <tbody> <tr> <td data-bbox="734 1096 1052 1150">1 to 10</td> <td data-bbox="1052 1096 1312 1150">2</td> </tr> <tr> <td data-bbox="734 1150 1052 1205">11 to 50</td> <td data-bbox="1052 1150 1312 1205">4</td> </tr> <tr> <td data-bbox="734 1205 1052 1260">51 to 150</td> <td data-bbox="1052 1205 1312 1260">6</td> </tr> <tr> <td data-bbox="734 1260 1052 1314">151 to 200</td> <td data-bbox="1052 1260 1312 1314">8</td> </tr> </tbody> </table> <p>This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests.</p> <p>If too few reserved control slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced.</p> <p>In a typical cluster, each AP should be set to the same number of control slots to assure proper timing in the send and receive cycles. However, where high incidence of small packets exists, as in a sector that serves several VoIP streams, additional control slots may provide better results. For APs in a cluster of mismatched control slots settings, or where OFDM and FSK APs of the same frequency band are collocated, use the frame calculator.</p>	Number of SMs that Register to the AP	Number of Control Slots Recommended	1 to 10	2	11 to 50	4	51 to 150	6	151 to 200	8
Number of SMs that Register to the AP	Number of Control Slots Recommended										
1 to 10	2										
11 to 50	4										
51 to 150	6										
151 to 200	8										

Attribute	Meaning				
Broadcast Repeat Count	<p>The default is 2 repeats (in addition to the original broadcast packet, for a total of 3 packets sent for every one needed), and is settable to 1 or 0 repeats (2 or 1 packets for every broadcast).</p> <p>ARQ (Automatic Repeat reQuest) is not present in downlink broadcast packets, since it would cause unnecessary uplink traffic from every SM for each broadcast packet. For successful transport without ARQ, the AP repeats downlink broadcast packets. The SMs filter out all repeated broadcast packets and, thus, do not transport further.</p> <p>The default of 2 repeats is optimum for typical uses of the network as an internet access system. In applications with heavy download broadcast such as video distribution, overall throughput is significantly improved by setting the repeat count to 1 or 0. This avoids flooding the downlink with repeat broadcast packets.</p>				
Transmitter Output Power	<p>Nations and regions may regulate transmitter output power. For example</p> <ul style="list-style-type: none"> • 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. <p>The professional installer of the equipment has the responsibility to</p> <ul style="list-style-type: none"> • maintain awareness of applicable regulations. • calculate the permissible transmitter output power for the module. • confirm that the initial power setting is compliant with national or regional regulations. • confirm that the power setting is compliant following any reset of the module to factory defaults. 				
External Gain	<p>This value represents the amount of gain introduced by an external antenna.</p> <p>If your network operates in a region in which DFS shutdown capability is required, and you do not see this parameter, perform the following steps:</p> <ol style="list-style-type: none"> 1. Click the General tab. 2. Set the Region Code parameter from its drop-down list. 3. Click the Save Changes button. 4. Click the Reboot button. 5. Click the Radio tab. <table border="1" data-bbox="683 1640 1352 1816" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th data-bbox="683 1640 1101 1730">Module Type</th> <th data-bbox="1101 1640 1352 1730">Recommended Setting</th> </tr> </thead> <tbody> <tr> <td data-bbox="683 1730 1101 1816">OFDM connectorized with antenna that was purchased with it</td> <td data-bbox="1101 1730 1352 1816">17</td> </tr> </tbody> </table>	Module Type	Recommended Setting	OFDM connectorized with antenna that was purchased with it	17
Module Type	Recommended Setting				
OFDM connectorized with antenna that was purchased with it	17				

Attribute	Meaning
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.

Radio tab of the SM

Table 40 Radio tab of SM

Radio Configuration	
Custom Radio Frequency Scan Selection List :	<input type="checkbox"/> 5735 <input type="checkbox"/> 5740 <input type="checkbox"/> 5745 <input type="checkbox"/> 5750 <input type="checkbox"/> 5755 <input type="checkbox"/> 5760 <input type="checkbox"/> 5765 <input type="checkbox"/> 5770 <input type="checkbox"/> 5775 <input type="checkbox"/> 5780 <input type="checkbox"/> 5785 <input type="checkbox"/> 5790 <input type="checkbox"/> 5795 <input type="checkbox"/> 5800 <input type="checkbox"/> 5805 <input type="checkbox"/> 5810 <input type="checkbox"/> 5815 <input type="checkbox"/> 5820 <input type="checkbox"/> 5825 <input type="checkbox"/> 5830 <input type="checkbox"/> 5835 <input type="checkbox"/> 5840 <input type="checkbox"/> 5845 <input type="checkbox"/> 5850 <input type="checkbox"/> 5855 <input type="checkbox"/> 5860 <input type="checkbox"/> 5865 <input type="button" value="Select All"/> <input type="button" value="Clear All"/> <input type="button" value="Restore"/>
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	One Quarter
Color Code 1 :	0 (0—254) / Priority Primary
Color Code 2 :	0 (0—254) / Priority Disable
Color Code 3 :	0 (0—254) / Priority Disable
Color Code 4 :	0 (0—254) / Priority Disable
Color Code 5 :	0 (0—254) / Priority Disable
Color Code 6 :	0 (0—254) / Priority Disable
Color Code 7 :	0 (0—254) / Priority Disable
Color Code 8 :	0 (0—254) / Priority Disable
Color Code 9 :	0 (0—254) / Priority Disable
Color Code 10 :	0 (0—254) / Priority Disable
Installation Color Code :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Signal to Noise Ratio Calculation :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
MAC Control Parameters	
Downlink Dynamic Rate Adapt :	1x2x3x
Uplink Dynamic Rate Adapt :	1x2x3x
Power Control	
Transmitter Output Power :	-30 dBm (Range: -30 — +21 dBm)
External Gain :	0 dB (Range: 0 — 35 dB)

In the Radio tab of the SM, you may set the following parameters.

Table 41 SM Radio attributes

Attribute	Meaning
Custom Radio Frequency Scan Selection List	<p>Check any frequency that you want the SM to scan for AP transmissions. The frequency <i>band</i> of the SM affects what channels you should select.</p> <p>In a 5.7-GHz SM, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed in this field (default selections), then the SM scans for a signal on any channel. If you select only one, then the SM limits the scan to that channel.</p>
Channel Bandwidth	The channel size used by the radio for RF transmission. This parameter is dictated by the AP's settings.

Attribute	Meaning
Color Code 1 to 10	<p>Color code allows you to force the SM to register to only a specific AP, even where the SM can communicate with multiple APs. For registration to occur, the color code of the SM and the AP <i>must</i> match. Specify a value from 0 to 254.</p> <p>Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. The default setting for the color code value is 0. This value matches only the color code of 0 (<i>not</i> all 255 color codes).</p> <p>SMs may be configured with up to 10 color codes. These color codes can be tagged as Primary, Secondary, or Tertiary, or Disable. When the SM is scanning for APs, it will first attempt to register to an AP that matches one of the SM's primary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM's secondary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM's tertiary color codes. This is all done in the scanning mode of the SM and will repeat until a registration has occurred.</p> <p>Color codes in the same priority group are treated equally. For example, all APs matching one of the SM's primary color codes are analyzed equally. Likewise, this evaluation is done for the secondary and tertiary groups in order. The analysis for selecting an AP within a priority group is based on various inputs, including signal strength and number of SMs already registered to each AP.</p> <p>The first color code in the configuration is the pre-Release 9.5 color code. Thus, it is always a primary color code for legacy reasons.</p> <p>The color codes can be disabled, with the exception of the first color code.</p>
Installation Color Code	<p>With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. 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. SMs with Installation Color Code enabled will first try any configured Color Code values first, then will use the Installation Color Code feature as a last result to connect to the AP. The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message “SM is registered via ICC – Bridging Disabled!” is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the Rescan APs functionality on the AP Eval page).</p>

Attribute	Meaning												
Large VC data Q	<p>Certain applications such as video Surveillance cameras operate by sending bursts of IP traffic upstream. Some systems will send short bursts of packets at over 50 Mbps and then be idle for some period of time and then send another burst of data.</p> <p>In order for the RF interface of a radio to accommodate these bursts of traffic, there is a configurable parameter on SM radios to operate with a large input queue at the radio's data VC. This large queue allows packets which arrive at a rate greater than the radio link capacity to be stored in this deep queue until the radio is ready to transmit them. The queue size has been optimized to allow large packets to be stored just long enough so that there is always data available to be transmitted, but not large enough to cause packets to sit in a queue for a second or more.</p> <p>Configuration of this parameter is shown on the Configuration => Radio web page on the SM..</p> <p>If an operator is experiencing packet loss in the uplink due to bursting IP traffic and the overall traffic rate is less than or equal to the uplink capacity of the radio system, then the large VC data Q should be enabled.</p>												
Signal to Noise Ratio Calculation	<p>Enabling this parameter allows operators to use Signal-to-Noise calculations to monitor link quality.</p> <p>The Signal-to-Noise Ratio may be monitored on the SM's Home page, Link Capacity Test page, and Link Status page.</p> <p>See the table below for required Signal-to-Noise Ratios required for each modulation state:</p> <table border="1" data-bbox="581 1192 1344 1413"> <thead> <tr> <th>Modulation</th> <th>Downlink</th> <th>Uplink</th> </tr> </thead> <tbody> <tr> <td>1X</td> <td>7 dB</td> <td>9 dB</td> </tr> <tr> <td>2X</td> <td>15 dB</td> <td>16 dB</td> </tr> <tr> <td>3X</td> <td>23 dB</td> <td>24 dB</td> </tr> </tbody> </table> <p>Note that locking a radio a lower modulation may result in a lower SNR ratio reading than a higher modulation. For example an AP/SM pair that is getting a SNR of 23/29 dB for downlink/uplink when modulation is set to 1X/2X/3X gets 22/27 dB for a setting of 1X/2X. And when set to 1X (No rate adapt) the SNR reads 12/18 dB. For highest SNR calculation the rate adapt must be set to its highest rate adapt modulation.</p>	Modulation	Downlink	Uplink	1X	7 dB	9 dB	2X	15 dB	16 dB	3X	23 dB	24 dB
Modulation	Downlink	Uplink											
1X	7 dB	9 dB											
2X	15 dB	16 dB											
3X	23 dB	24 dB											

Attribute	Meaning
Transmitter Output Power	<p>The professional installer of the equipment has the responsibility to</p> <ul style="list-style-type: none">• maintain awareness of applicable regulations.• calculate the permissible transmitter output power for the module.• confirm that the initial power setting is compliant with national or regional regulations.• confirm that the power setting is compliant following any reset of the module to factory defaults.

Task 7: Setting up SNMP agent

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

SNMP Tab of the AP

Table 42 SNMP tab of the AP

General
IP
Radio
SNMP
Quality of Service (QoS)
Security
Time
VLAN
VLAN Membership
DiffServ
Unit Settings

- Home
- Configuration
- Statistics
- Tools
- Account
- Quick Start
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

Configuration => SNMP

5.7GHz - Access Point - 0a-00-3e-d5-b9-97

SNMP Community Strings

SNMP Community String 1 :

SNMP Community String 1 Permissions Read Only
 Read / Write

SNMP Community String 2 (Read Only)

SNMP Accessing Addresses

Accessing IP / Subnet Mask 1 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 2 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 3 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 4 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 5 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 6 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 7 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 8 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 9 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 10 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>

Trap Addresses

Trap Address 1 :	<input type="text" value="0.0.0"/>
Trap Address 2 :	<input type="text" value="0.0.0"/>
Trap Address 3 :	<input type="text" value="0.0.0"/>
Trap Address 4 :	<input type="text" value="0.0.0"/>
Trap Address 5 :	<input type="text" value="0.0.0"/>
Trap Address 6 :	<input type="text" value="0.0.0"/>
Trap Address 7 :	<input type="text" value="0.0.0"/>
Trap Address 8 :	<input type="text" value="0.0.0"/>
Trap Address 9 :	<input type="text" value="0.0.0"/>
Trap Address 10 :	<input type="text" value="0.0.0"/>

Trap Enable

Sync Status : Enabled
 Disabled

Session Status : Enabled
 Disabled

Site Information

Site Name :

Site Contact :

Site Location :

You may set the SNMP tab parameters as follows.

Table 43 AP SNMP attributes

Attribute	Meaning
SNMP Community String 1	Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is Canopy .
SNMP Community String 1 Permissions	You can designate the SNMP Community String 1 to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.
SNMP Community String 2 (Read Only)	Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is Canopyro . This password will never authenticate a user or an NMS to read/write access. The Community String value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the Accessing Subnet , Trap Address , and Permission parameters.
Accessing IP / Subnet Mask 1 to 10	Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both <ul style="list-style-type: none"> • The network IP address in the form xxx.xxx.xxx.xxx • The CIDR (Classless Interdomain Routing) prefix length in the form /xx For example the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet). 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct Community String value. The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.
SNMP Trap Server DNS Usage	The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.

Attribute	Meaning
Trap Address 1 to 10	<p>Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) or DNS names to which SNMP traps should be sent. Traps inform Prizm or an NMS that something has occurred. For example, trap information is sent</p> <ul style="list-style-type: none"> • after a reboot of the module. • when an NMS attempts to access agent information but either • supplied an inappropriate community string or SNMP version number. • is associated with a subnet to which access is disallowed.
Trap Enable, Sync Status	<p>If you want sync status traps (sync lost and sync regained) sent to Prizm or an NMS, select Enabled. If you want these traps suppressed, select Disabled.</p>
Trap Enable, Session Status	<p>If you want session status traps sent to Prizm or an NMS, select Enabled.</p>
Site Information Viewable to Guest Users	<p>Operators can enable or disable site information from appearing when a user is in GUEST account mode.</p>
Site Name	<p>Specify a string to associate with the physical module. This parameter is written into the <i>sysName</i> SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.</p>
Site Contact	<p>Enter contact information for the module administrator. This parameter is written into the <i>sysContact</i> SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.</p>
Site Location	<p>Enter information about the physical location of the module. This parameter is written into the <i>sysLocation</i> SNMP MIB-II object and can be polled by PrizmEMS or an NMS. The buffer size for this field is 128 characters.</p>

SNMP Tab of the SM

Table 44 SNMP tab of SM

General | IP | Radio | **SNMP** | Quality of Service (QoS) | Security | VLAN | VLAN Membership | DiffServ
Protocol Filtering | NAT | PPPoE | NAT Port Mapping | Unit Settings

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
- Logoff
- Account: admin
- Level: ADMINISTRATOR

Configuration => SNMP

2.4GHz - Subscriber Module - 0a-00-3e-23-20-67

SNMP Community Strings [-]

SNMP Community String 1 :

SNMP Community String 1 Permissions : Read Only Read / Write

SNMP Community String 2 (Read Only) :

SNMP Accessing Addresses [-]

Accessing IP / Subnet Mask 1 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 2 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 3 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 4 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 5 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 6 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 7 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 8 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 9 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>
Accessing IP / Subnet Mask 10 :	<input type="text" value="0.0.0"/>	<input type="text" value="/ 0"/>

Trap Addresses [-]

Trap Address 1 :	<input type="text" value="0.0.0"/>
Trap Address 2 :	<input type="text" value="0.0.0"/>
Trap Address 3 :	<input type="text" value="0.0.0"/>
Trap Address 4 :	<input type="text" value="0.0.0"/>
Trap Address 5 :	<input type="text" value="0.0.0"/>
Trap Address 6 :	<input type="text" value="0.0.0"/>
Trap Address 7 :	<input type="text" value="0.0.0"/>
Trap Address 8 :	<input type="text" value="0.0.0"/>
Trap Address 9 :	<input type="text" value="0.0.0"/>
Trap Address 10 :	<input type="text" value="0.0.0"/>

Site Information [-]

Site Name :


Site Contact :

Site Location :

In the SNMP tab of the SM, you may set the following parameters.

Table 45 SM SNMP attributes

Attribute	Meaning
SNMP Community String 1	Specify a control string that can allow an Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is Canopy .
SNMP Community String 1 Permissions	You can designate the SNMP Community String 1 to be the password for Prizm, for example, to have read/write access to the module via SNMP, or for all SNMP access to the module to be read only.
SNMP Community String 2 (Read Only)	Specify an additional control string that can allow an Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is Canopy2 . This password will never authenticate a user or an NMS to read/write access. The Community String value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the Accessing Subnet , Trap Address , and Permission parameters.

Attribute	Meaning
Accessing IP / Subnet Mask <i>1 to 10</i>	<p>Specify the addresses that are allowed to send SNMP requests to this SM. Prizm or the NMS has an address that is among these addresses (this subnet). You must enter both</p> <p>The network IP address in the form xxx.xxx.xxx.xxx</p> <p>The CIDR (Classless Interdomain Routing) prefix length in the form /xx</p> <p>For example</p> <p>the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).</p> <p>192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the SM, presuming that the device supplies the correct Community String value.</p> <p>The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.</p> <div data-bbox="683 961 1453 1255" style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <p style="text-align: center;">RECOMMENDATION:</p> <div style="display: flex; align-items: center;">  <p>The subscriber can access the SM by changing the subscriber device to the accessing subnet. This hazard exists because the Community String and Accessing Subnet are both visible parameters. To avoid this hazard, configure the SM to filter (block) SNMP requests.</p> </div> </div>
SNMP Trap Server DNS Usage	<p>The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.</p>
Trap Address <i>1 to 10</i>	<p>Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent after a reboot of the module.</p> <p>when Prizm or an NMS attempts to access agent information but either supplied an inappropriate community string or SNMP version number. is associated with a subnet to which access is disallowed.</p>
Read Permissions	<p>Select Read Only if you wish to disallow Prizm or NMS SNMP access to configurable parameters and read-only fields of the SM.</p>

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

Task 8: Configuring syslog

This task is only performed when system logging is required. Both the AP and the SM may be configured to send system messages to a syslog server. An example of a syslog message that would be sent from a radio is as follows:

```
<6>1 2011-05-13T12:28:31Z 169.245.1.1 - - - BOM*****System Startup*****
```

By default syslog is disabled on all devices.

Configuring AP system logging (syslog)

To configure system logging, select menu option **Configuration, Syslog**. The Syslog Configuration page is displayed (Figure 16).

Figure 16 AP Syslog Configuration page

Configuration → Syslog

5.7GHz OFDM - Access Point - 0a-00-3e-3f-ff-53

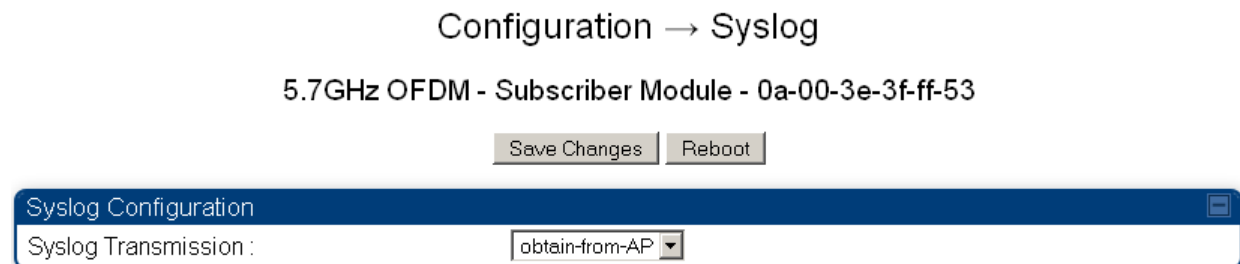
Syslog Configuration	
Syslog DNS Server Usage :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name
Syslog Server :	<input type="text" value="0.0.0.0"/>
Syslog Server Port :	<input type="text" value="514"/> <i>Default port number is 514</i>
AP Syslog Transmit :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SM Syslog Transmit :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Table 46 Syslog Configuration attributes

Attribute	Meaning
Syslog DNS Server Usage	To configure the AP to append or not append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
AP Syslog Transmit	When enabled, syslog messages will be sent from the AP.
SM Syslog Transmit	When enabled, allows all SMs in a sector to learn the enabling or disabling syslog messages transmission setting at registration. In order for the SM to use this information from the AP, the SM must be configured to learn syslog settings from the AP.

Configuring SM system logging (syslog)

To configure system logging, select menu option **Configuration, Syslog**. The Syslog Configuration page is displayed (Figure 16).

Figure 17 SM Syslog Configuration page**Table 47** Syslog Configuration attributes

Attribute	Meaning
Syslog Transmission	The SM can choose to either learn its syslog configuration from the AP or to override the AP's sector settings with its own settings. The ability to override the AP settings lets an operator enable or disable syslog settings for individual SMs in a sector.

Task 9: Configuring remote access

Configuring SM IP over-the-air access

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

Figure 18 SM IP Configuration page

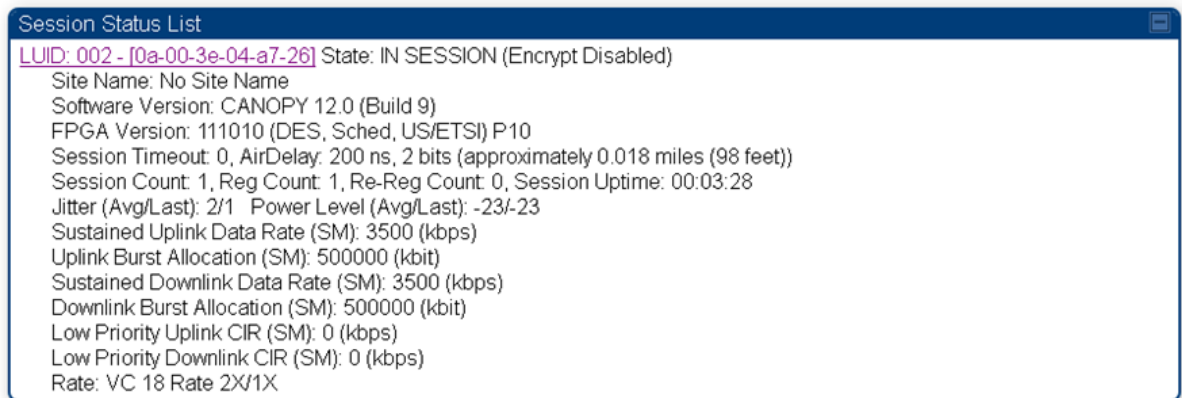
Configuration → IP

5.7GHz OFDM - Subscriber Module - 0a-00-3e-3f-ff-53

LAN1 Network Interface Configuration	
IP Address :	<input type="text" value="192.168.2.57"/>
Network Accessibility :	<input checked="" type="radio"/> Public <input type="radio"/> Local
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway IP Address :	<input type="text" value="192.168.2.1"/>
DHCP state :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DNS IP Address :	<input checked="" type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	<input type="text" value="0.0.0.0"/>
Alternate DNS Server :	<input type="text" value="0.0.0.0"/>
Domain Name :	<input type="text" value="example.com"/>

Accessing SM over-the-air by LUID

The SM may be accessed via the AP management GUI by navigating to either **Home, Session Status** or **Home, Remote Subscribers** and clicking on the SM's hyperlink.

Figure 19 AP Session Status page**Figure 20** AP Remote Subscribers page

Denying All Remote Access

Wherever the No Remote Access feature is enabled by the following procedure, physical access to the module is required for

- any change in the configuration of the module.
- any software upgrade in the module.

Where additional security is more important than ease of network administration, you can disable all remote access to a module as follows. After this procedure, no access to the module is possible through HTTP, SNMP, FTP, or telnet over an RF link.

To deny remote access to the module, perform the following steps:

- 1** Insert the override plug into the RJ-11 GPS utility port of the module
- 2** Power up or power cycle the module
- 3** Access the web page <http://169.254.1.1/lockconfig.html>
- 4** Click the checkbox
- 5** Save the changes
- 6** Remove the override plug
- 7** Reboot the module

Reinstating Remote Access Capability

Where ease of network administration is more important than the additional security that the No Remote Access feature provides, this feature can be disabled as follows. After this procedure, access to the module is possible through HTTP, SNMP, FTP, or telnet over an RF link.

To reinstate all remote access to the module, perform the following steps:

- 1** Insert the override plug into the RJ-11 GPS utility port of the module
- 2** Power up or power cycle the module
- 3** Access the web page <http://169.254.1.1/lockconfig.html>
- 4** Click the check box to uncheck the field
- 5** Save the changes
- 6** Remove the override plug
- 7** Reboot the module

Task 10: Monitoring the AP-SM Link

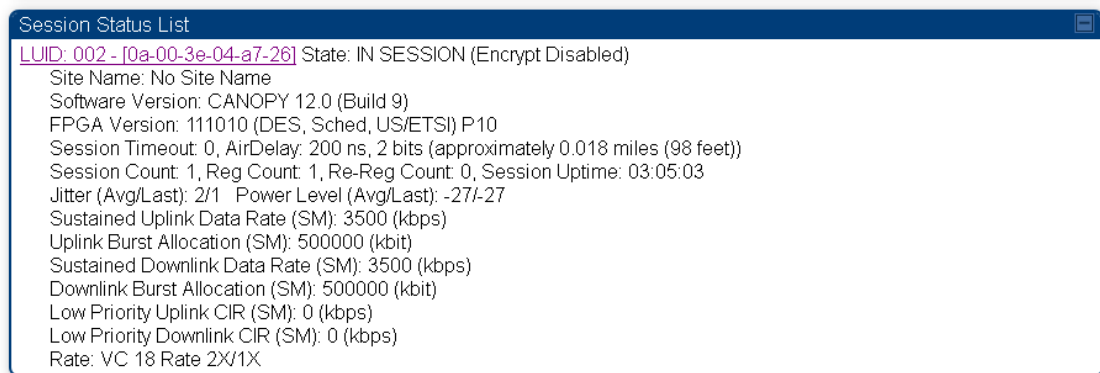
Monitoring the AP-SM Link

After the SM installer has configured the link, either an operator in the network office or the SM installer in the field (if read access to the AP is available to the installer) should perform the following procedure. Who is authorized and able to do this may depend on local operator password policy, management VLAN setup, and operational practices.

To monitor the AP-SM link for performance, proceed as follows:

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

Figure 21 AP Session Status page



- 4** Find the **Session Count** line under the MAC address of the SM.
- 5** Check and note the values for **Session Count**, **Reg Count**, and **Re-Reg Count**.
- 6** Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.
- 7** If these values are low (for example, 1, 1, and 0, respectively, meaning that the SM registered and started a stable session once) and are not changing
 - consider the installation successful.
 - monitor these values from the network office over the next several hours and days.

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

Task 11: Configuring quality of service

Maximum Information Rate (MIR) Parameters

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

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

You can independently set each of these parameters per AP or per SM.

Token Bucket Algorithm

The software uses a *token bucket* algorithm that

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

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

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

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

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

Which set of these MIR parameters are applicable depends on the interactions of other parameter values. Also, where the **Configuration Source** parameter setting in the AP specifies that BAM values should be used, they are used only if Prizm is configured to send the values that it stores for the MIR parameters.

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in [Figure 22](#).

NOTE

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

Figure 22 Uplink and downlink rate caps adjusted to apply aggregate cap

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

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

For example, in the SM, if you set the **Sustained Uplink Data Rate** parameter to 2,000 kbps and the **Sustained Downlink Data Rate** parameter to 10,000 kbps, then the uplink and downlink MIR that will be enforced for the SM can be calculated as shown in [Figure 23](#).

Figure 23 Uplink and downlink rate cap adjustment example

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

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

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

Committed Information Rate

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum, unless CIR is oversubscribed. Bandwidth can be, and typically will be, higher than the minimum, but this guarantee helps the WISP to attract and retain subscribers.

In BAM Release 2.1 and in Prizm Release 2.0, CIR configuration is supported as follows:

- The GUI allows you to view and change CIR configuration parameters per SM.

- When an SM successfully registers and authenticates, if BAM or Prizm has CIR configuration data for the SM, then messages make the CIR configuration available to the SM, depending on the Configuration Source setting.
- The operator can disable the CIR feature in the SM without deleting the CIR configuration data.

Bandwidth from the SM Perspective

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

Interaction of Burst Allocation and Sustained Data Rate Settings

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

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

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

High-priority Bandwidth

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

NOTE

The number of channels available to the AP is reduced by the number of SMs configured for the high-priority channel. With this feature enabled on all SMs, an AP can support 100 SMs (instead of 200).

A module prioritizes traffic by

- reading the Low Latency bit (Bit 3) in the IPv4 Type of Service (ToS) byte in a received packet. Bit 3 is set by a device outside the system.
- reading the 802.1p field of the 802.1Q header in a received packet, where VLAN is enabled on the module.

- comparing the 6-bit Differentiated Services Code Point (DSCP) field in the ToS byte of a received packet to a corresponding value in the Diffserv tab of the Configuration page of the module. A packet contains no flag that indicates whether the encoding is for the Low Latency bit or the DSCP field. For this reason, you must ensure that all elements in your trusted domain, including routers and endpoints, set and read the ToS byte with the same scheme.

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

- The 6-bit length of the field allows it to specify one of 64 service differentiations.
- These correlate to 64 individual (**CodePoint**) parameters in the Diffserv tab of the Configuration page.
- Per RFC 2474, 3 of these 64 are preset and cannot be changed. (See <http://www.faqs.org/rfcs/rfc1902.html>.)
- For any or all of the remaining 61 CodePoint parameters, you can specify a value of
 - 0 through 3 for low-priority handling.
 - 4 through 7 for high-priority handling.



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

An example of the Diffserv tab in the Configuration page and parameter descriptions are provided under [DiffServ Tab of the AP on Page 2-116](#). This tab and its rules are identical from module type to module type. However, any of the 61 configurable Code Points can be set to a different value from module to module, thus defining unique per-hop behavior for some traffic.

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

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

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

Traffic Scheduling

The characteristics of traffic scheduling in a sector are summarized in [Table 48](#).

Table 48 Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	14 Mbps

Category	Factor	Treatment
Latency	Number of frames required for the scheduling process	1
	Round-trip latency	≈ 6 ms
	AP broadcast the download schedule	No
High-priority Channel	Allocation for <i>uplink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for <i>downlink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	CIR high-priority CIR low-priority Other high-priority Other low-priority
Transmit Frame Spreading	Support for Transmit Frame Spreading feature	In Release 7.0 and later
CIR	Capability	In all releases

CAUTION

Power requirements affect the recommended maximums for power cord length feeding the CMMmicro or CMM4. See the dedicated user guide that supports the CMM that you are deploying. However, the requirements *do not* affect the maximums for the CMM2.

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

Setting the Configuration Source

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

- all MIR settings:
 - Sustained Uplink Data Rate

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

Table 49 Recommended combined settings for typical operations

Most operators who use...	should set this parameter...	in this web page/tab...	in the AP to...
no authentication server	Authentication Mode	Configuration/ Security	Authentication Disabled
	Configuration Source	Configuration/ General	SM
Prizm with authentication server	Authentication Mode	Configuration/ Security	Authentication Required
	Configuration Source	Configuration/ General	Authentication Server

Table 50 Where feature values are obtained for an SM with authentication required

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

NOTES:

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

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

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

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

The high-priority channel is unavailable to Series P7 and P8 SMs.

For any SM whose **Authentication Mode** parameter *is not* set to **Authentication Required**, the listed settings are derived as shown:

Table 51 Where feature values are obtained for an SM with authentication disabled

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

For the case where the **Configuration Source** parameter in the AP is set to **Authentication Server**, the SM stores a value for the **Dynamic Learning VLAN** parameter that differs from its factory default. When Prizm does not send VLAN values (because **VLAN Enable** is set to **No** in Prizm), the SM

- uses this stored **Disable** value for **Dynamic Learning**.
- shows the following in the VLAN Configuration web page:
 - *either Enable or Disable* as the value of the **Dynamic Learning** parameter.
 - **Allow Learning : No** under **Active Configuration**.

For the case where the **Configuration Source** parameter in the AP is set to **Authentication Server+SM**, and Prizm does not send VLAN values, the SM

- uses the configured value in the SM for **Dynamic Learning**. If the SM is set to factory defaults, then this value is **Enable**.
- shows under **Active Configuration** the result of the configured value in the SM. For example, if the SM is set to factory defaults, then the VLAN Configuration page shows **Allow Learning : Yes**.

This selection (**Authentication Server+SM**) is *not* recommended where Prizm manages the VLAN feature in SMs.

Quality of Service (QoS) Tab of the AP

Figure 24 Quality of Service (QoS) tab of the AP

Configuration => Quality of Service (QoS)

2.4GHz - Access Point - 0a-00-3e-23-20-66

Save Changes

AP Bandwidth Settings

(Uplink + Downlink) Sustained Data Rate <= 40000 kbps	
Sustained Uplink Data Rate :	20000 (kbps) (Range: 0— 40000 kbps)
Uplink Burst Allocation :	500000 (kbits) (Range: 0— 500000 kbits)
Sustained Downlink Data Rate :	20000 (kbps) (Range: 0— 40000 kbps)
Downlink Burst Allocation :	500000 (kbits) (Range: 0— 500000 kbits)
Broadcast Downlink CIR :	200 (kbps) (Range: 0— 2333 kbps)

Save Changes

Reboot

In the Quality of Service (QoS) tab, you may set AP bandwidth parameters as follows.

Table 52 AP QoS attributes

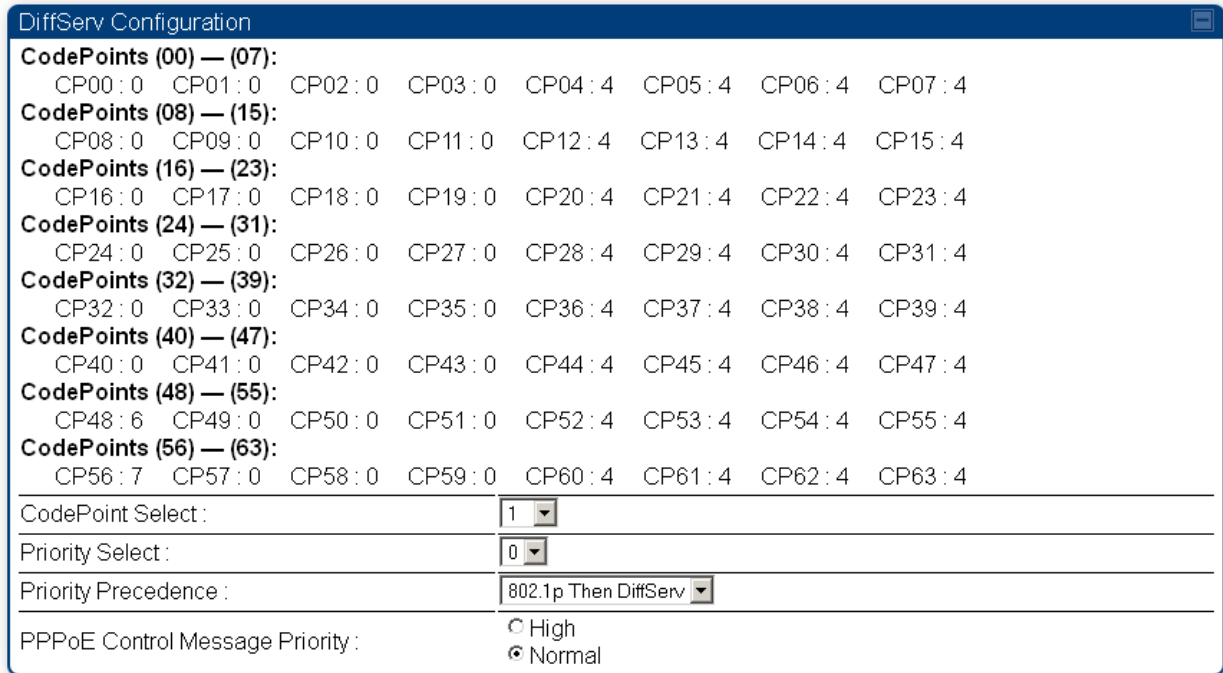
Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that each SM registered to this AP is replenished with credits for transmission. This default imposes no restriction on the uplink. See <ul style="list-style-type: none"> • Maximum Information Rate (MIR) Parameters on page 2-106 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108 • Configuration Source on page 2-42

Attribute	Meaning
Uplink Burst Allocation	<p>Specify the maximum amount of data to allow each SM to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. See</p> <ul style="list-style-type: none">• Maximum Information Rate (MIR) Parameters on page 2-106• Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108• Configuration Source on page 2-42
Sustained Downlink Data Rate	<p>Specify the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. This default imposes no restriction on the uplink. See</p> <ul style="list-style-type: none">• Maximum Information Rate (MIR) Parameters on page 2-106• Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108• Configuration Source on page 2-42
Downlink Burst Allocation	<p>Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the Sustained Downlink Data Rate. See</p> <ul style="list-style-type: none">• Maximum Information Rate (MIR) Parameters on page 2-106• Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108• Configuration Source on page 2-42

Attribute	Meaning												
Broadcast Downlink CIR	<p>Broadcast Downlink CIR (Committed Information Rate, a minimum) supports some system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default.</p> <p>Broadcast Downlink CIR is closely related to the Broadcast Repeat Count parameter, which is settable in the Radio tab of the Configuration page in the AP: when the Broadcast Repeat Count is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the Broadcast Repeat Count parameter. (See Broadcast Repeat Count on Page 2-86.)</p> <p>Table 53 Broadcast Downlink CIR achievable per Broadcast Repeat Count</p> <table border="1" data-bbox="591 789 1274 1148"> <thead> <tr> <th data-bbox="591 789 769 993">Broadcast Repeat Count</th> <th data-bbox="769 789 1019 993">Number of times each packet is sent</th> <th data-bbox="1019 789 1274 993">Highest Achievable Value for Broadcast Downlink CIR</th> </tr> </thead> <tbody> <tr> <td data-bbox="591 993 769 1045">0</td> <td data-bbox="769 993 1019 1045">1</td> <td data-bbox="1019 993 1274 1045">7000 kbps</td> </tr> <tr> <td data-bbox="591 1045 769 1098">1</td> <td data-bbox="769 1045 1019 1098">2</td> <td data-bbox="1019 1045 1274 1098">3500 kbps</td> </tr> <tr> <td data-bbox="591 1098 769 1148">2</td> <td data-bbox="769 1098 1019 1148">3</td> <td data-bbox="1019 1098 1274 1148">2333 kbps</td> </tr> </tbody> </table>	Broadcast Repeat Count	Number of times each packet is sent	Highest Achievable Value for Broadcast Downlink CIR	0	1	7000 kbps	1	2	3500 kbps	2	3	2333 kbps
Broadcast Repeat Count	Number of times each packet is sent	Highest Achievable Value for Broadcast Downlink CIR											
0	1	7000 kbps											
1	2	3500 kbps											
2	3	2333 kbps											

DiffServ Tab of the AP

Figure 25 Diffserv tab of the AP



You may set the following Diffserv tab parameters.

Table 54 AP Diffserv attributes

Attribute	Meaning
CodePoint 1 through CodePoint 47	Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. Consistent with RFC 2474
CodePoint 49 through CodePoint 55	CodePoint 0 is predefined to a fixed priority value of 0 (low-priority channel). CodePoint 48 is predefined to a fixed priority value of 6 (high-priority channel). CodePoint 56 is predefined to a fixed priority value of 7 (high-priority channel).
CodePoint 57 through CodePoint 63	You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See Error! Reference source not found. on Page Error! Bookmark not defined.
CodePoint Select	This represents the CodePoint Selection to be modified via Priority Select

Attribute	Meaning
Priority Select	The priority setting input for the CodePoint selected in CodePoint Select
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits should be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the SM to utilize the high priority channel for PPPoE control messages. Configuring the SM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the SM.

Quality of Service (QoS) Tab of the SM

Figure 26 Quality of Service (QoS) tab of the SM

Configuration => Quality of Service (QoS)

2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

MIR Bandwidth Settings
(Uplink + Downlink) Sustained Data Rate <= 40000 kbps

Sustained Uplink Data Rate : (kbps) (Range: 0-- 40000 kbps)

Sustained Downlink Data Rate : (kbps) (Range: 0-- 40000 kbps)

Uplink Burst Allocation : (kbits) (Range: 0 -- 500000 kbits)

Downlink Burst Allocation : (kbits) (Range: 0 -- 500000 kbits)

CIR Bandwidth Settings

Low Priority Uplink CIR : (kbps) (Range: 0 -- 20000 kbps)

Low Priority Downlink CIR : (kbps) (Range: 0 -- 20000 kbps)

Hi Priority Channel : Enabled Disabled

Hi Priority Uplink CIR : (kbps) (Range: 0 -- 20000 kbps)

Hi Priority Downlink CIR : (kbps) (Range: 0 -- 20000 kbps)

In the Quality of Service (QoS) tab of the SM, you may set the following parameters.

Table 55 AP Quality of Service attributes

Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See <ul style="list-style-type: none"> • Maximum Information Rate (MIR) Parameters on page 2-106 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108 • Configuration Source on page 2-42

Attribute	Meaning
Sustained Downlink Data Rate	<p>Specify the rate at which the AP should be replenished with credits (tokens) for transmission to this SM. This default imposes no restriction on the uplink. See</p> <ul style="list-style-type: none"> • Maximum Information Rate (MIR) Parameters on Page 2-106 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108 • Configuration Source on page 2-42
Uplink Burst Allocation	<p>Specify the maximum amount of data to allow this SM to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. See</p> <ul style="list-style-type: none"> • Maximum Information Rate (MIR) Parameters on page 2-106 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108 • Configuration Source on page 2-42
Downlink Burst Allocation	<p>Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the Sustained Downlink Data Rate with transmission credits. See</p> <ul style="list-style-type: none"> • Maximum Information Rate (MIR) Parameters on page 2-106 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-108 • Configuration Source on page 2-42
Low Priority Uplink CIR	<p>See</p> <ul style="list-style-type: none"> • Committed Information Rate on page 2-107 • Configuration Source on page 2-42
Low Priority Downlink CIR	<p>See</p> <ul style="list-style-type: none"> • Committed Information Rate on page 2-107 • Configuration Source on page 2-42
Hi Priority Channel	<p>See</p> <ul style="list-style-type: none"> • High-priority Bandwidth on page 2-108 • Configuration Source on page 2-42

Attribute	Meaning
Hi Priority Uplink CIR	See <ul style="list-style-type: none"> • High-priority Bandwidth on page 2-108 • Committed Information Rate on page 2-107 • Configuration Source on page 2-42.
Hi Priority Downlink CIR	See <ul style="list-style-type: none"> • High-priority Bandwidth on page 2-108 • Committed Information Rate on Page 2-107 • Configuration Source on page 2-42.

DiffServ Tab of the SM

Figure 27 Diffserv tab of the SM

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | VLAN | VLAN Membership | **DiffServe** | Protocol
 Filtering | NAT | NAT Port Mapping | Unit Settings

Configuration => DiffServe

2.4GHz - Subscriber Module - 0a-00-3e-20-a5-48

DiffServe Configuration

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

CodePoint Select :

Priority Select :

Save Changes

Reboot

In the Diffserv tab of the SM, you may set the following parameters.

Table 56 SM Diffserv attributes

Attribute	Meaning
CodePoint 1 through CodePoint 47	<p>Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. Consistent with RFC 2474</p> <p>CodePoint 0 is predefined to a fixed priority value of 0 (low-priority channel).</p>
CodePoint 49 through CodePoint 55	<p>CodePoint 48 is predefined to a fixed priority value of 6 (high-priority channel).</p> <p>CodePoint 56 is predefined to a fixed priority value of 7 (high-priority channel).</p>
CodePoint 57 through CodePoint 63	<p>You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See Error! Reference source not found. on Page Error! Bookmark not defined.</p>

Task 12: Configuring a RADIUS server

Configuring a RADIUS AAA (Authentication, Authorization, and Accounting) server in a PMP 450 network is optional, but can provide added security, increase ease of network management and provide usage-based billing data.

Understanding RADIUS for PMP 450

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

RADIUS Functions

RADIUS protocol support provides the following functions:

- **SM Authentication** allows only known SMs onto the network (blocking “rogue” SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to “rogue” APs). RADIUS authentication is used for SMs, but is not used for APs.
- **SM Authorization** configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when an SM registers to an AP.
- **SM Accounting** provides support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP.
- **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed IP** allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).

Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

- FreeRADIUS, Version 2.1.8
- Aradial RADIUS, Version 5.1.12



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

Choosing Authentication Mode and Configuring for Authentication Servers - AP

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

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

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

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

Figure 28 Security tab of the AP

Configuration → Security

5.7GHz - Access Point - 0a-00-3e-fc-56-40

Save Changes

Authentication Server Settings			
Authentication Mode :	<input checked="" type="checkbox"/> Disabled <input type="checkbox"/> Authentication Server <input type="checkbox"/> AP Pre-Shared Key <input type="checkbox"/> RADIUS AAA		
Authentication Server 1 :		Shared Secret
Authentication Server 2 :		Shared Secret	
Authentication Server 3 :	0.0.0.0	Shared Secret	
Authentication Server 4 (BAM ONLY) :	0.0.0.0		
Authentication Server 5 (BAM ONLY) :	0.0.0.0		
Authentication Key :		(Using All 0xFF's Key)	
Select Key :	<input type="radio"/> Use Key above <input checked="" type="radio"/> Use Default Key		

SM Authentication Mode – Require RADIUS or Follow AP

If it is desired that an SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set **Enforce Authentication** to AAA. With this enabled, an SM will not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected.

If it is desired that an SM use the authentication method configured on the AP it is registering to, set **Enforce Authentication** to **Disabled**. With **Enforce Authentication** disabled, an SM will attempt to register using whichever **Authentication Mode** is configured on the AP it is attempting to register to.

Note, requiring SMs to use RADIUS by enabling **Enforce Authentication** avoids the security issue of SMs possibly registering to “rogue” APs which have authentication disabled.

Figure 29 Security tab of the SM

Configuration → Security

5.7GHz - Subscriber Module - 0a-00-3e-fe-ed-df

Save Changes

Authentication Key Settings

Authentication Key : (Using All 0xFF's Key)

Select Key : Use Key above
 Use Default Key

AAA Authentication Settings

Lock AAA : Enabled
 Disabled

Phase 1 :

Phase 2 :

Identity/Realm : Enable Realm
 Disable Realm

Identity @ Realm

Username :

Password :

Confirm Password :

SM - Phase 1 (Outside Identity) parameters and settings

The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are

eapttls (Extensible Authentication Protocol Tunneled Transport Layer Security) and **eapMSChapV2** (Extensible Authentication Protocol – Microsoft Challenge-Handshake Authentication Protocol).

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. If Realms are being used in the RADIUS system (**eapttls** only), 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.

SM - Phase 2 (Inside Identity) parameters and settings

If using **capttls** for Phase 1 authentication, 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 **MSCHAPv2** (Microsoft's version of CHAP). The protocol must be consistent with the authentication protocol configured on the RADIUS server. 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. 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.

Handling Certificates

Managing SM Certificates via the SM GUI

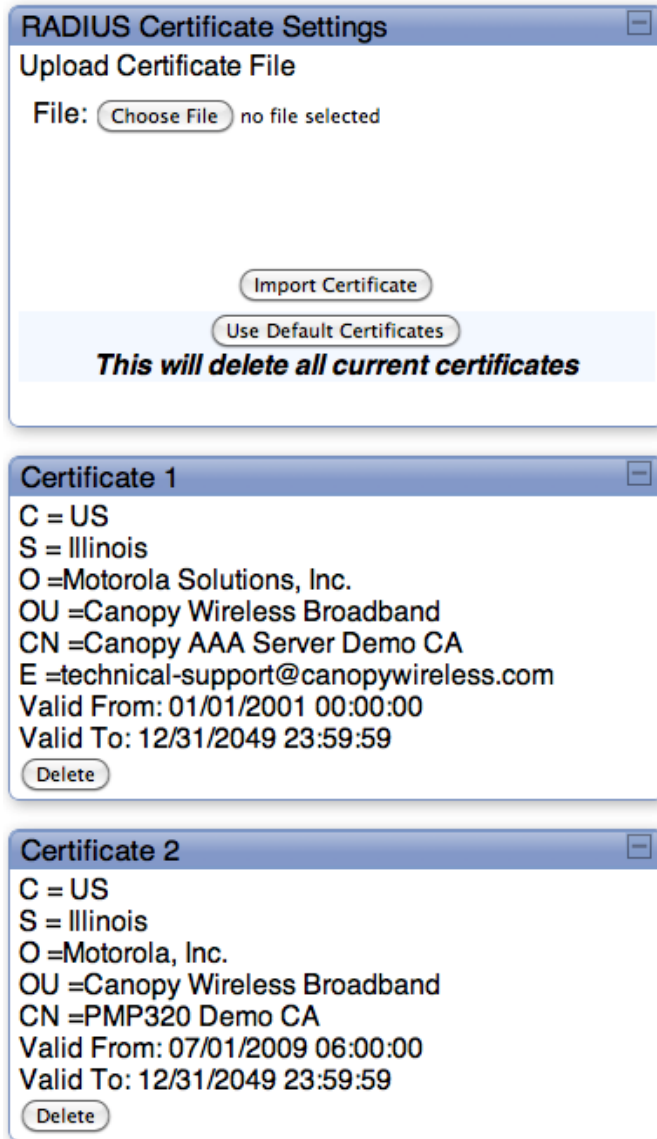
The default public Canopy certificates are loaded into SMs upon factory software installation. The default certificates are not secure and are intended for use during lab and field trials as part of gaining experience with the RADIUS functionalities or as an option during debug. For secure operation, an operator will want to create or procure their own certificates.

Up to 2 certificates can be resident on an 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.

To upload a certificate manually to an 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.

Figure 30 SM Certificate Management

Using CNUT to distribute certificates to SMs

CNUT Release 4.0 supports distribution of certificates to SMs. Please see the CNUT documentation for additional information (the CNUT documentation may be found on the Cambium support website <http://www.cambiumnetworks.com/support>).

Configuring your RADIUS servers for SM authentication

Your RADIUS server will need to be configured to use the following:

- EAPTTLS or MSCHAPv2 as the Phase 1/Outer Identity protocol.

- If **Enable Realm** is selected on the SM's **Configuration > Security** tab, then the same Realm as appears there (or access to it).
- The same Phase 2 (Inner Identity) protocol as configured on the SM's **Configuration > Security** tab under Phase 2 options.
- The username and password for each SM configured on each SM's **Configuration > Security** tab.
- An IP address and NAS shared secret that is the same as the IP address and **Shared Secret** configured on the AP's **Configuration > Security** tab for that RADIUS server.
- A server private certificate, server key, and CA certificate that complement the public certificates distributed to the SMs, as well as the Canopy dictionary file that defines Vendor Specific Attributes (VSAa). Default certificate files and the dictionary file are available from the software site: www.cambiumnetworks.com/support/pmp/software/ after entering your name, email address, and either Customer Contract Number or the MAC address of a module covered under the 12 month warranty.

Optionally, operators may configure the RADIUS server response messages (Accept or Reject) so that the user has information as to why they have been rejected. The AP displays the RADIUS Authentication Reply message strings in the Session Status list as part of each SM's information. The SM will show this string (listed as Authentication Response on the SM GUI) on the main Status page in the Subscriber Module Stats section.

(Note: Aradial AAA servers only support operator-configurable Authentication Accept responses, not Authentication Reject responses).

Figure 31 AP display of RADIUS accept for SM

```
Session Status List
LUID: 002 - [0a-00-3e-23-f9-b0] State: IN SESSION (Encrypt Disabled)
Site Name: Firmware Public SM#125(.125 Advantage)
Software Version: CANOPY 11.1 (Build 5)
FPGA Version: 030411 (DES, Sched, US/ETSI) P10
Session Timeout: 0, AirDelay: 300 ns, 3 bits (approximately 0.027 miles (147 feet))
Session Count: 4, Reg Count: 2, Re-Reg Count: 0, Session Uptime: 10:34:35
Sequence Number Mismatch: 0
RSSI (Last): 2306 Jitter (Last): 6 Power Level (Last): -48
Sustained Uplink Data Rate (SM): 3500 (kbps)
Uplink Burst Allocation (SM): 500000 (kbit)
Sustained Downlink Data Rate (SM): 3500 (kbps)
Downlink Burst Allocation (SM): 500000 (kbit)
Low Priority Uplink CIR (SM): 0 (kbps)
Low Priority Downlink CIR (SM): 0 (kbps)
Rate: VC 18 Rate 2X/2X
RADIUS Authentication Reply: Welcome to Canopy!
```


Figure 32 AP display of RADIUS rejected SM

```

LUID: 004 - [0a-00-3e-20-97-e7] State: IDLE
Site Name: Firmware Public SM 122( 122 P9 Lite)
Session Timeout: 0, AirDelay: 200 ns, 2 bits (approximately 0.018 miles (98 feet))
Session Count: 5, Reg Count: 3, Re-Reg Count: 0
RSSI (Avg/Last): 2307/2308 Jitter (Avg/Last): 1/1 Power Level (Avg/Last): -48/-48
Sustained Uplink Data Rate (AP): 20000 (kbps)
Uplink Burst Allocation (AP): 500000 (kbit)
Sustained Downlink Data Rate (AP): 20000 (kbps)
Downlink Burst Allocation (AP): 500000 (kbit)
Low Priority Uplink CIR (D): 0 (kbps)
Low Priority Downlink CIR (D): 0 (kbps)
RADIUS Authentication Reply: AAA Authorization Rejected

```

Figure 33 SM display of RADIUS accpet

Subscriber Module Stats	
Session Status :	REGISTERED VC 18 Rate 2X/2X
Registered AP :	0a-00-3e-23-f9-9f No Site Name
Color Code :	240 (Primary)
Channel Frequency :	2415.0 MHz
Power Level :	Actual: -47 dBm Min: -48 dBm Max: -47 dBm
Transmit Power Level :	-3 dBm
Jitter (Interference Level) :	Actual: 2 Min: 0 Max: 3
Air Delay :	3 approximately 0.027 miles (147 feet)
Authentication Message :	Welcome to Canopy!

Configuring your RADIUS server for SM configuration

Table 57 lists Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details. The associated SM GUI page, tab, and parameter is listed to aid cross-referencing and understanding of the VSAs.

A RADIUS dictionary file is available from the software site:

www.cambiumnetworks.com/support/pmp/software/

The RADIUS dictionary file defines the VSAs and their values and is usually imported into the RADIUS server as part of server and database setup.

Assigning SM management IP addressing via RADIUS

Operators may use a RADIUS AAA server to assign management IP addressing to SM modules (framed IP address). SMs now interpret attributes Framed-IP-Address, Framed-IP-Netmask, and Motorola-Canopy-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Motorola-Canopy-Gateway attribute and is available on the Motorola Software Support website.

In order for these attributes to be assigned and used by the SM, the following must be true:

- The Canopy system is configured for AAA authentication

- The SM is *not* configured for DHCP on its management interface. If DHCP is enabled and these attributes are configured in the RADIUS server, the attributes will be ignored by the SM.
- The SM management interface must be configured to be publically accessible. If the SM is configured to have local accessibility, the management interface will still be assigned the framed addressing, and the SM will become publically accessible via the assigned framed IP addressing.
- When using these attributes, for the addressing to be implemented by the SM operators must configure Framed-IP-Address in RADIUS. If Framed-IP-Address is not configured but Framed-IP-Netmask and/or Motorola-Canopy-Gateway is configured, the attributes will be ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) / 255.255.255.0 (NAT enabled) and Motorola-Canopy-Gateway defaults to 0.0.0.0.

Table 57 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Req'd	Value	Size
SM GUI Page > Tab > Parameter				Default	Size
MS-MPPE-Send-Key	26.311.16	-	Y	-	-
MS-MPPE-Recv-Key	26.311.17	-	Y	-	-
Motorola-Canopy-LPULCIR	26.161.1	integer	N	0-20000 kbps	
Configuration > Quality of Service > Low Priority Uplink CIR				0 kbps	32 bits
Motorola-Canopy-LPDL CIR	26.161.2	integer	N	0-20000 kbps	
Configuration > Quality of Service > Low Priority Downlink CIR				0 kbps	32 bits
Motorola-Canopy-HPULCIR	26.161.3	integer	N	0-20000 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Motorola-Canopy-HPDL CIR	26.161.4	integer	N	0-20000 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Motorola-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable	
Configuration > Quality of Service > Hi Priority Channel				0	32 bits
Motorola-Canopy-ULBR	26.161.6	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Sustained Uplink Data Rate				dependent on radio feature set	32 bits
Motorola-Canopy-ULBL	26.161.7	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Motorola-Canopy-DLBR	26.161.8	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Motorola-Canopy-DLBL	26.161.9	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits

Motorola-Canopy-	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Motorola-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Motorola-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Motorola-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Motorola-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Motorola-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits
Motorola-Canopy-VLSMMGPASS	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Motorola-Canopy-BCASTMIR	26.161.24	integer	N	0-50000+ kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data				dependent on radio feature set	32 bits
Motorola-Canopy-Gateway	26.161.25	ipaddr	N	-	
Configuration > IP > Gateway IP Address				0.0.0.0	-
Motorola-Canopy-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Note about VSA numbering: 26 connotes Vendor Specific Attribute, per RFC 2865 26.311 is Microsoft Vendor Code, per IANA					

Using RADIUS for centralized AP and SM user name and password management

AP – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the AP from a centralized RADIUS server:

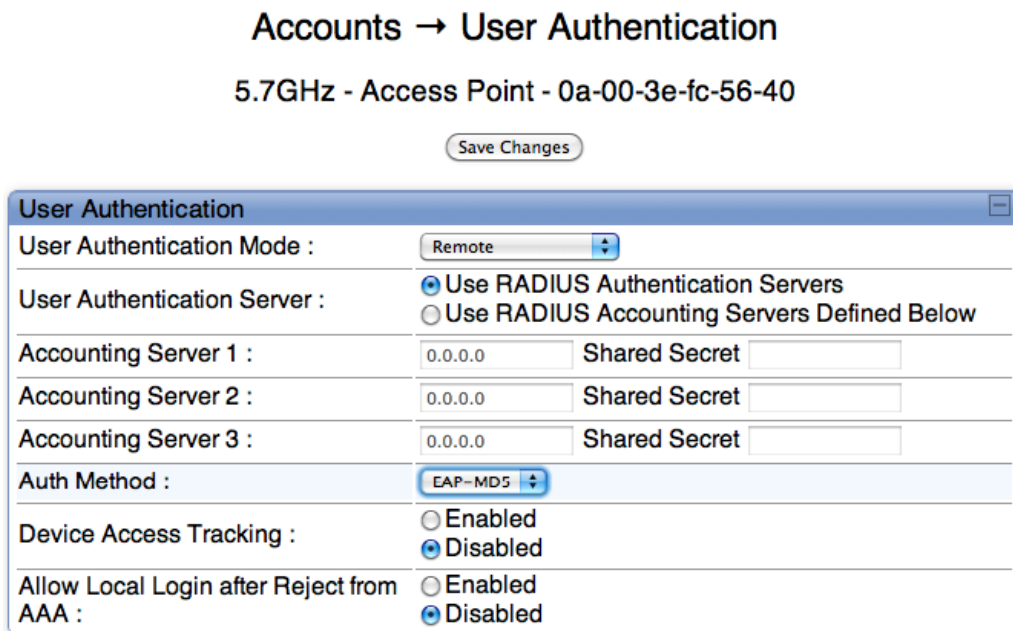
- 1 Set **Authentication Mode** on the AP's Configuration > Security tab to **RADIUS AAA**

- 2** Set **User Authentication Mode** on the AP's Account > User Authentication tab (the tab only appears after the AP is set to RADIUS authentication) to **Remote** or **Remote then Local**.
- **Local:** The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.
 - **Remote:** Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out.
 - **Remote then Local:** Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

Either the same RADIUS server used for SM authentication and authorization can be used for user authentication and accounting (access control), or a separate RADIUS accounting server can be used. Indicate your network design under **User Authentication Server**.

If separate accounting server(s) are used, configure the IP address(es) and **Shared Secret(s)** in the **Accounting Server** fields. The default **Shared Secret** is "CanopyAcctSecret". Up to 3 servers can be used for redundancy. Servers 2 and 3 are meant for backup and reliability, not splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, Server 2 is not tried.

Figure 34 User Authentication tab of the AP



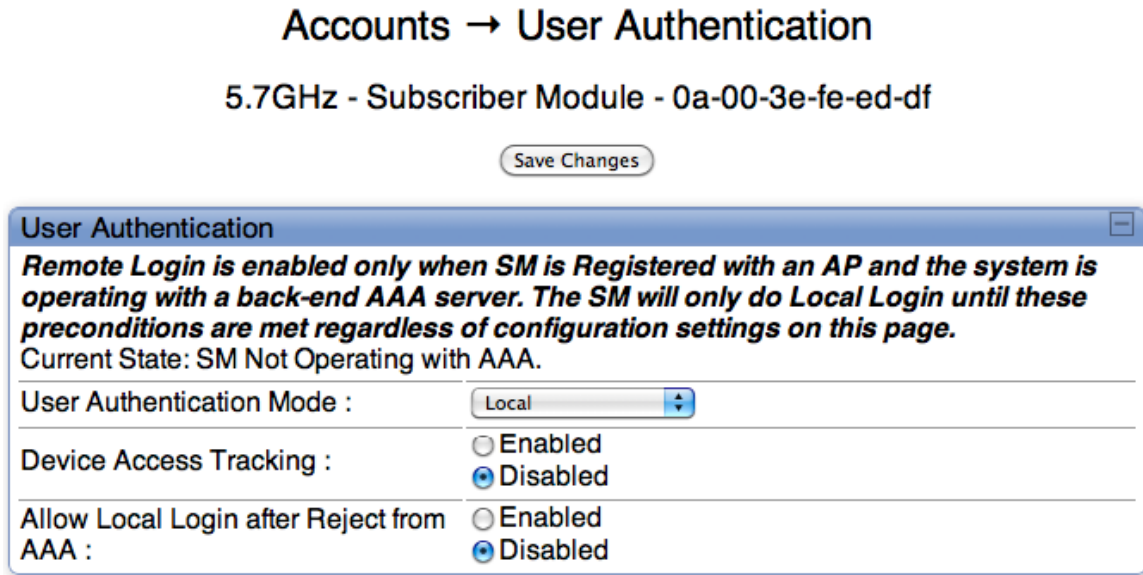
SM – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the SM from a centralized RADIUS server:

- 1** Set **Authentication Mode** on the AP's Configuration > Security tab to **AAA** (RADIUS)
- 2** Set **User Authentication Mode** on the AP's Account > User Authentication and Accounting tab (the tab only appears after the AP is set to AAA authentication) to **Remote** or **Remote then Local**.
- 3** Set **User Authentication Mode** on the SM's Account > User Authentication and Accounting tab to **Remote** or **Remote then Local**.
 - **Local:** The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.
 - **Remote:** Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern will be displayed until the server responds or times out.
 - **Remote then Local:** Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

Note, remote access control is enabled only after the SM registers to an AP that has **Authentication Mode** set to **RADIUS AAA**. Local access control will always be used before registration and will be used after registration if the AP is not configured for RADIUS.

Figure 35 User Authentication tab of the SM



Access Tracking

To track logon and logoff times on individual radios by technicians, installers, and administrators, on the AP or SM's **Account > User Authentication and Accounting** tab under **Accounting** (Access Tracking) choose **Enabled**.

Device Access Tracking is enabled separately from **User Authentication Mode**. A given AP or SM can be configured for both, either, or neither.

RADIUS Device Data Accounting

PMP 450 systems include support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP. The attributes included in the RADIUS accounting messages are shown in the table below.

Table 58 Device data accounting RADIUS attributes

Sender	Message	Attribute	Value	Description
AP	Accounting-	Acct-Status-Type	1 - Start	This message is sent

Sender	Message	Attribute	Value	Description
	Request	Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	every time an SM registers with an AP, and after the SM stats are cleared.
		Event-Timestamp	UTC time the event occurred on the AP	
AP	Accounting-Request	Acct-Status-Type	2 - Stop	This message is sent every time an SM becomes unregistered with an AP, and when the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets received at the SM over regular data VC and the high priority data VC (if enabled). Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets sent from the SM over regular data VC and the high priority data VC (if enabled).	
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^{32} over the course of the session	
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	

Sender	Message	Attribute	Value	Description
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the regular data VC and the high priority data VC (if enabled).	
		Acct-Session-Time	Uptime of the SM session.	
		Acct-Terminate-Cause	Reason code for session termination	
AP	Accounting-Request	Acct-Status-Type	3 - Interim-Update	<p>This message is sent periodically per the operator configuration on the AP in seconds.</p> <p>Interim update counts are cumulative over the course of the session</p>
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets sent to the SM over regular data VC and the high priority data VC (if enabled). Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets set from the SM over regular data VC and the high priority data VC (if enabled).	
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2 ³² over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2 ³² over the course of the session	
		Acct-Session-Time	Uptime of the SM session.	

Sender	Message	Attribute	Value	Description
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the regular data VC and the high priority data VC (if enabled).	

The data accounting configuration is located on the AP's **Accounts > User Authentication and Access Tracking** GUI menu, and the AP's **Authentication Mode** must be set to **Radius AAA** for the menu to appear. The accounting may be configured via the AP GUI as shown in the figures below. By default accounting messages are not sent and the operator has the choice of configuring to send only Device Access accounting messages (when a user logs in or out of the radio), only Data Usage messages, or both. When Data Accounting is enabled, the operator must specify the interval of when the data accounting messages are sent (0 – disabled, or in the range of 30-10080 minutes). The default interval is 30 minutes.

Table 59 RADIUS accounting messages configuration

The screenshot shows the 'Access Tracking Configuration' window. It contains three rows of configuration options:

- Accounting Messages :** A dropdown menu with 'Disable' selected.
- Accounting Data Usage Interval :** A text input field with '0' and a unit label 'minutes(0=Disabled,min-30,max-10080)'.
- SM Re-authentication Interval :** A text input field with '0' and a unit label 'minutes(0=Disabled,min-30,max-10080)'. A dropdown menu is open below this field, showing options: 'Disable', 'Device Access', 'Data Usage' (highlighted), and 'All'.

Table 60 RADIUS data accounting message interval

The screenshot shows the 'Access Tracking Configuration' window with the following configuration:

- Accounting Messages :** A dropdown menu with 'Data Usage' selected.
- Accounting Data Usage Interval :** A text input field with '30' and a unit label 'minutes(0=Disabled,min-30,max-10080)'.
- SM Re-authentication Interval :** A text input field with '0' and a unit label 'minutes(0=Disabled,min-30,max-10080)'.

The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify the AAA of the change.

If an operator clears the VC statistics on the device through the management GUI, a RADIUS stop message and data start message will be issued for each device affected. The start and stop messages will only be sent once every 5 minutes, so if an operator clears these statistics multiple times within 5 minutes, only one set of data stop/start messages will be sent. This may result in inaccurate data accumulation results.

RADIUS Device Re-Authentication

PMP 450 systems include support for periodic SM re-authentication in a network without requiring the SM to re-register (and drop the session). The re-authentication may be configured to occur in the range of every 30 minutes to weekly.

Table 61 Device re-authentication configuration

Access Tracking Configuration		
Accounting Messages :	Disable	
Accounting Data Usage Interval :	0	minutes(0=Disabled,min-30,max-10080)
SM Re-authentication Interval :	30	minutes(0=Disabled,min-30,max-10080)

The re-authentication interval is only configurable on the AP. When this feature is enabled, each SM that enters the network will re-authenticate each the interval time has expired without dropping the session. The response that the SM receives from the AAA server upon re-authentication is one of the following:

- **Success:** The SM will continue normal operation
- **Reject:** The SM will de-register and will attempt network entry again after 1 minute and then if rejected will attempt re-entry every 15 minutes
- **Timeout or other error:** The SM will remain in session and attempt 5 times to re-authenticate with the RADIUS-REQUEST message. If these attempts fail, then the SM will go out of session and proceed to re-authenticate after 5 minutes, then every 15 minutes.

Although re-authentication is an independent feature, it was designed to work alongside with the RADIUS data usage accounting messages. If a user is over their data usage limit the network operator can reject the user from staying in the network. Operators may configure the RADIUS ‘Reply-Message’ attribute with an applicable message (i.e. “Data Usage Limit Reached”) that will be sent to the subscriber module and displayed on the general page.

RADIUS Attribute Framed-IP-Address

Operators may now use a RADIUS AAA server to assign management IP addressing to SM modules (framed IP address). SMs now interpret attributes Framed-IP-Address, Framed-IP-Netmask, and Motorola-Canopy-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Motorola-Canopy-Gateway attribute and is available on the Motorola Software Support website.

In order for these attributes to be assigned and used by the SM, the following must be true:

- The Canopy system is configured for AAA authentication
- The SM is *not* configured for DHCP on its management interface. If DHCP is enabled and these attributes are configured in the RADIUS server, the attributes will be ignored by the SM.
- The SM management interface must be configured to be publically accessible. If the SM is configured to have local accessibility, the management interface will still be assigned the framed addressing, and the SM will become publicly accessible via the assigned framed IP addressing.

- When using these attributes, for the addressing to be implemented by the SM operators must configure Framed-IP-Address in RADIUS. If Framed-IP-Address is not configured but Framed-IP-Netmask and/or Motorola-Canopy-Gateway is configured, the attributes will be ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) / 255.255.255.0 (NAT enabled) and Motorola-Canopy-Gateway defaults to 0.0.0.0.

Chapter 3: Reference information

FCC and ICC Information

Table 62 US FCC IDs and Industry Canada Certification Numbers and Covered Configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna (OFDM)	Maximum Tx Output Power
ABZ89FT7634	109W-5780	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5780APC	17 dBi Connectorized	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			
ABZ89FT7635	109W-5790	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			

ABZ89FT7635	109W-5790	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated with 18 dBi Reflector Dish	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			
		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			
ABZ89FT7635	109W-5790	5 MHz channels, centered on 5727.5-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated with 9 dBi Cassegrain LENS	19 dBm
		10 MHz channels, centered on 5730-5845 in 5 MHz increments (within the 5725-5850 MHz ISM band)			

		20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)			
--	--	--	--	--	--

Transmitter Output Power

Table 63 PMP 450 AP transmitter output power

Radio/ Frequency	Channel Size	Region(s)	Transmit Output Power Range	TX Default Setting	Antenna Gain (18 dBi – 1dB cable loss)	Max EIRP (Tx + Antenna Gain)
PMP 450 AP 5.8 GHz OFDM/FSK	5 MHz	United States and Canada	-30 to +19 dBm	19 dBm	17 dBi	36 dBm
		Europe and India	-30 to +13 dBm	13 dBm	17 dBi	30 dBm
	10 MHz	United States and Canada	-30 to +19 dBm	19 dBm	17 dBi	36 dBm
		Europe and India	-30 to +16 dBm	16 dBm	17 dBi	33 dBm
	20 MHz	United States, Canada, Europe and India	-30 to +19 dBm	19 dBm	17 dBi	36 dBm

Exposure Separation Distances

To protect from overexposure to RF energy, install PMP 450 radios so as to provide and maintain the minimum separation distances from all persons shown in [Table 64](#).

Table 64 Exposure Separation Distances

Module Type	Separation Distance from Persons
PMP 450 AP or SM	At least 20 cm (approx 8 in)

Details of Exposure Separation Distances Calculations and Power Compliance Margins

Limits and guidelines for RF exposure come from:

- US FCC limits for the general population. See the FCC web site at <http://www.fcc.gov>, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See Safety Code 6 on the Health Canada web site at <http://www.hc-sc.gc.ca/>.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at <http://www.icnirp.de/> and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

The applicable power density exposure limits from the documents referenced above are

- 10 W/m² for RF energy in the 5.7-GHz frequency band.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P \cdot G}{4 \pi d^2}$$

where
 S = power density in W/m²
 P = RMS transmit power capability of the radio, in W
 G = total Tx gain as a factor, converted from dB
 d = distance from point source, in m

Rearranging terms to solve for distance yields

$$d = \sqrt{\frac{P \cdot G}{4 \pi S}}$$

[Table 65](#) shows calculated minimum separation distances d , recommended distances and resulting power compliance margins for each frequency band and antenna combination.

Table 65 Calculated Exposure Distances and Power Compliance Margins

Freq. Band	Antenna	Variable			d (calculated)	Recommended Separation Distance	Power Compliance Margin
		P	G	S			
5.4 / 5.8 GHz OFDM	Integrated, 9 dBi patch	0.079 W (19 dBm)	.08 W (9 dBi)	10 W/m ² or 1 mW/cm ²	8 cm	20 cm (8 in)	8
	Integrated, 9 dBi patch with 9 dBi Cassegrain LENS	0.079 W (19 dBm)	.05 W (18 dBi)	10 W/m ² or 1 mW/cm ²	18 cm	50 cm (20 in)	8
	Integrated, 9 dBi patch with 18 dBi Reflector Dish	0.079 W (19 dBm)	.5 W (27 dBi)	10 W/m ² or 1 mW/cm ²	56 cm	150 cm (60 in)	7

The “Recommended Distances” are chosen to give significant compliance margin in all cases. They are also chosen so that an OFDM module has the same exposure distance as a Canopy module, to simplify communicating and heeding exposure distances in the field.

These are conservative distances:

- They are along the beam direction (the direction of greatest energy). Exposure to the sides and back of the module will be significantly less.
- They meet sustained exposure limits for the general population (not just short term occupational exposure limits), with considerable margin.
- The calculated compliance distance d is overestimated because the far-field equation models the antenna as a point source and neglects the physical dimension of the antenna.

Appendix A: Glossary

Term	Definition
~.	The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.
10Base-T	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.
100Base-TX	Technology in Ethernet communications that can deliver 100 Mb of data across 328 feet (100 meters) of CAT 5 cable.
169.254.0.0	Gateway IP address default in Motorola fixed wireless broadband IP network modules.
169.254.1.1	IP address default in Motorola fixed wireless broadband IP network modules.
169.254.x.x	IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.
255.255.0.0	Subnet mask default in Motorola fixed wireless broadband IP network modules and in Microsoft and Apple operating systems.
802.3	An IEEE standard that defines the contents of frames that are transferred through Ethernet connections. Each of these frames contains a preamble, the address to which the frame is sent, the address that sends the frame, the length of the data to expect, the data, and a checksum to validate that no contents were lost.
802.11	The IEEE standard for wireless local area networks.
802.15	The IEEE standard for wireless personal area networks.
Access Point Cluster	Two to six Access Point Modules that together distribute network or Internet services to a community of 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.
Access Point Module	Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
ACT/4	Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Activate	To provide feature capability to a module, but not to enable (turn on) the feature in the module. See also Enable.

Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html .
Advanced Encryption Standard (AES)	Over-the-air link option that provides extremely secure wireless connections. Advanced Encryption Standard (AES) uses 128-bit secret keys as directed by the government of the U.S.A. AES is not exportable and requires a special AP to process the large keys.
AES	See Advanced Encryption Standard.
Aggregate Throughput	The sum of the throughputs in the uplink and the downlink.
AP	Access Point Module. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
APA	Access Point module address.
Apache	A trademark of Apache Software Foundation, used with permission.
APAS	Access Point Authentication Server. Licensed to authenticate SMs that attempt to register to it. The AP licensed as APAS may or may not have authentication enabled (turned on). See also Activate and Enable.
API	Application programming interface for web services that supports Prizm integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system.
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html .
ASN.1	Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.
Attenuation	Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.
Authentication Key	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f, padded with leading zeroes in Release 4.2.3 and later. This key must be unique to the individual SM.
Backhaul Module	Also known as BH. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module. See also Backhaul Timing Master and Backhaul Timing Slave.

Backhaul Timing Master	Backhaul Module that sends network timing (synchronization) to another Backhaul Module, which serves as the Backhaul timing slave.
Backhaul Timing Slave	Backhaul Module that receives network timing (synchronization) from another Backhaul Module, which serves as the Backhaul timing master.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
BH	Backhaul Module. A module that provides point-to-point connectivity as either a standalone link or a link to an Access Point cluster through a selected Access Point Module.
Bit Error Rate	Ratio of incorrect data received to correct data received.
Box MIB	Management Information Base file that defines module-level objects. See also Management Information Base.
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
Bridge Entry Timeout Field	Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.
Buckets	Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.
Burst	Preset amount limit of data that may be continuously transferred.
C/I Ratio	Ratio of intended signal (carrier) to unintended signal (interference) received.
Canopy	A trademark of Motorola, Inc.
Carrier-to-interference Ratio	Ratio of intended reception to unintended reception.
CarSenseLost Field	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
CAT 5 Cable	Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
chkconfig	A command that the Linux® operating system accepts to enable MySQL® and Apache™ Server software for various run levels of the mysqld and httpd utilities.
CIR	See Committed Information Rate.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.

CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster. If this CMM is connected to a Backhaul Module (BH), then this CMM is the central point of connectivity for the entire site.
CodePoint	See DiffServ.
Color Code Field	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Committed Information Rate (CIR)	For an SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum. In the Motorola implementation, this is controlled by the Low Priority Uplink CIR, Low Priority Downlink CIR, High Priority Uplink CIR, and High Priority Downlink CIR parameters.
Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCErrors Field	This field displays how many CRC errors occurred on the Ethernet controller.
CRM	Customer relationship management system.
Data Encryption Standard	Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Date of Last Transaction	A field in the data that the cmd show esn command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.
Dell	A trademark of Dell, Inc.
Demilitarized Zone	Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html .
DES	Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Desensed	Received an undesired signal that was strong enough to make the module insensitive to the desired signal.
DFS	See Dynamic Frequency Selection.
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that 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 system. See http://www.faqs.org/rfcs/rfc2131.html . See also Static IP Address Assignment.

Diffraction	Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.
DiffServ	Differentiated Services, consistent with RFC 2474. A byte in the type of service (TOS) field of packets whose values correlates to the channel on which the packet should be sent. The value is a numeric code point. Motorola modules map each of 64 code points to values of 0 through 7. Three of these code points have fixed values, and the remaining 61 are settable. Values of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. (However, configuring DiffServ does not automatically enable the VLAN feature.) Among the settable parameters, the values are set in the AP for all downlinks within the sector and in the SM for each uplink.
Disable	To turn off a feature in the module after both the feature activation file has activated the module to use the feature and the operator has enabled the feature in the module. See also Activate and Enable.
DLT	Date of last transaction. A field in the data that the cmd show esn command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM.
DMZ	Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html .
Dynamic Frequency Selection (DFS)	A requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems, and to avoid co-channel operation with these systems. See also Region Code.
Dynamic Host Configuration Protocol	See DHCP.
Electronic Serial Number	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
Element Pack	A license for Prizm management of a multi-point sector and covers the AP and up to 200 SMs or a backhaul link.
Enable	To turn on a feature in the module after the feature activation file has activated the module to use the feature. See also Activate.
Engine	Bandwidth and Authentication Manager (BAM) interface to the AP and SMs. Unique sets of commands are available on this interface to manage parameters and user access. Distinguished from SSE. See also SSE.
ESN	Electronic Serial Number. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.

ESN Data Table	Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.
/etc/services	File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.
EthBusErr Field	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
Fade Margin	The difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link. Standard operating margin.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target module. When installed on the module, this file activates the module to have the feature enabled or disabled in a separate operator action.
Field-programmable Gate Array	Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html .
FPGA	Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
Frame Spreading	Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.
Frame Timing Pulse Gated Field	Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.
Free Space Path Loss	Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.
Fresnel Zone	Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.
FSK	Frequency Shift Keying, a variation of frequency modulation to transmit data, in which two or more frequencies are used.

FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html .
Global Positioning System	Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS/3	Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
GUI	Graphical user interface.
High-priority Channel	Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service DiffServ Control Point (DSCP) bits. Enabling the high-priority channel reduces the maximum number of SMs that can be served in the sector.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html .
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html .
indiscards count Field	How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors count Field	How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
innucastpkts count Field	How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
inoctets count Field	How many octets were received on the interface, including those that deliver framing information.
Intel	A registered trademark of Intel Corporation.
inucastpkts count Field	How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

inunknownprotos count Field	How many inbound packets were discarded because of an unknown or unsupported protocol.
IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html .
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
Jitter	Timing-based measure of the reception quality of a link. An acceptable link displays a jitter value between 0 and 4 for a 10-Mbps Backhaul timing slave in Release 4.0 and later, between 0 and 9 for a 20-Mbps Backhaul timing slave, or between 5 and 9 for any Subscriber Module or for a Backhaul timing slave in any earlier release. OFDM modules do not have this parameter.
L2TP over IPsec	Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.
Late Collision Field	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Latency Tolerance	Acceptable tolerance for delay in the transfer of data to and from a module.
Line of Sight	Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
Linux	A registered trademark of Linus Torvalds.
LNK/5	Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Logical Unit ID	Final octet of the 4-octet IP address of the module.
LOS	Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.

MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Management Information Base	Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
Master	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul module that provides synchronization over the air to another Backhaul module (a Backhaul timing slave) and applies to a Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically copied onto a redundant BAM server (BAM slave). In each case, the master is not a product. Rather, the master is the role that results from deliberate configuration steps.
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Motorola implementation, this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
Media Access Control Address	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MIR	See Maximum Information Rate.
MySQL	A registered trademark of MySQL AB Company in the United States, the European Union, and other countries.
mysqladmin	A command to set the administrator and associated password on the Bandwidth and Authentication Manager (BAM) server.
mysql-server	Package group that enables the SQL Database Server application in the Red Hat® Linux® 9 operating system to provide SQL data for Bandwidth and Authentication Manager (BAM) operations.
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html .
NBI	See Northbound Interface.
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.
NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html .

Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html .
Network Management Station	See NMS.
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects). See also Simple Network Management Protocol.
Northbound Interface (NBI)	The interface within Prizm to higher-level systems. This interface consists of a Simple Network Management Protocol (SNMP) agent for integration with a network management system (NMS); a Simple Object Access Protocol (SOAP) XML-based application programming interface (API) for web services that supports integration with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system; and console automation that allows such higher-level systems to launch and appropriately display the PrizmEMS management console in a custom-developed GUI.
Object	Network variable that is defined in the Management Information Base.
OptiPlex	A trademark of Dell, Inc.
OSS	Operations support system, such as a customer relationship management (CRM), billing, or provisioning system. The application programming interface (API) for Prizm supports integrating Prizm with an OSS.
outdiscards count Field	How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrors count Field	How many outbound packets contained errors that prevented their transmission.
outnucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outoctets count Field	How many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Override Plug	Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.
Pentium	A registered trademark of Intel Corporation.

php-mysql	Package group that enables the Web Server application in the Red Hat® Linux® 9 operating system to provide data from the SQL Database Server application as PHP in the Bandwidth and Authentication Manager (BAM) GUI.
PMP	See Point-to-Multipoint Protocol.
Point-to-Multipoint Protocol	Defined in RFC 2178, which specifies that data that originates from a central network element can be received by all other network elements, but data that originates from a non-central network element can be received by only the central network element. See http://www.faqs.org/rfcs/rfc2178.html . Also referenced as PMP.
Point-to-Point Protocol	Standards that RFC 1661 defines for data transmittal on the Internet. Also known as PPP or PTP. See http://www.faqs.org/rfcs/rfc1661.html .
Power Control	Feature in Release 4.1 and later that allows the module to operate at less than 18 dB less than full power to reduce self-interference.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
PPTP	Point to Point Tunneling Protocol. One of several virtual private network implementations. Regardless of whether the Network Address Translation (NAT) feature enabled, Subscriber Modules support VPNs that are based on this protocol.
Prizm	The software product that allows users to partition their entire networks into criteria-based subsets and independently monitor and manage those subsets. Prizm Release 1.0 and later includes a Northbound Interface to higher-level systems. Prizm integrates Bandwidth and Authentication Manager (BAM) functionality.
Protective Earth	Connection to earth (which has a charge of 0 volts). Also known as ground.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.
PTMP	See Point-to-Multipoint Protocol.
PTP	See Point-to-Point Protocol.
QoS	Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM about the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.
Quality of Service	A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.
Quick Start	Interface page that requires minimal configuration for initial module operation.

Radio Signal Strength Indicator	Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.
Random Number	Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.
Reader	A registered trademark of Adobe Systems, Incorporated.
Recharging	Resumed accumulation of data in available data space (buckets). See Buckets.
Red Hat	A registered trademark of Red Hat, Inc.
Reflection	Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.
Region Code	A parameter that offers multiple fixed selections, each of which automatically implements either the Dynamic Frequency Selection (DFS) standard that is required by law or regulatory to apply or no DFS, based on the frequency band range and the selected region.
Registrations MIB	Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.
repl-m	A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) master server, uses SFTP to copy both the database and the repl-s script to a BAM slave server, and remotely executes the repl-s script on the BAM slave server. See Master, Slave, repl-s, Secure Shell, and SFTP.
repl-s	A command that sets up the database replication process on a Bandwidth and Authentication Manager (BAM) slave server. See Master, Slave, and repl-m.
RES	Result. A field in the data that the cmd show esn command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server.
RetransLimitExp Field	This field displays how many times the retransmit limit has expired.
RF	Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.
RJ-11	Standard cable that is typically used for telephone line or modem connection.
RJ-45	Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later modules auto-sense whether the cable is straight-through or crossover.

Router	Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.
RPM	Red Hat® Package Manager.
rpm	A command that the Linux® operating system accepts to identify the version of Linux® software that operates on the Bandwidth and Authentication Manager (BAM) server.
RSSI	Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.
RxBabErr Field	This field displays how many receiver babble errors occurred.
RxOverrun Field	This field displays how many receiver overrun errors occurred on the Ethernet controller.
SDK	PrizmEMS™ Software Development Kit (SDK)—the document that provides server administrator tasks, GUI developer information for console automation that allows higher-level systems to launch and appropriately display the Prizm management console. The SDK also describes the how to define new element types and customize the Details views.
Secure Shell	A trademark of SSH Communications Security.
Self-interference	Interference with a module from another module in the same network.
SES/2	Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Session Key	Software key that the SM and Bandwidth and Authentication Manager (BAM) separately calculate based on that both the authentication key (or the factory-set default key) and the random number. BAM sends the session key to the AP. Neither the subscriber nor the network operator can view this key. See also Random Number.
SFTP	Secure File Transfer Protocol.
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.faqs.org/rfcs/rfc1157.html .
skey	Software key that correlates to the random number that the Bandwidth and Authentication Manager (BAM) server generates and sends in a challenge through the AP to the SM. The network operator can create and, at some security risk, send this key over the air to the SM. The SQL database in the BAM server correlates this key to QoS information about the SM. The format of this key is 32 hexadecimal characters of 0 to 9 and a to f. This key must be unique to the individual SM. Also known as authentication key.

Slave	Designation that defines the role of a component relative to the role of another. This designation both applies to a Backhaul slave that receives synchronization over the air from another Backhaul module (a Backhaul timing master) and applies to a redundant Bandwidth and Authentication Manager (BAM) server whose SQL database is automatically overwritten by a copy from the primary BAM server (BAM master). In each case, the slave is not a product. Rather, the slave is the role that results from deliberate configuration steps.
SM	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
SM MIB	Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.
SNMP	See Simple Network Management Protocol, defined in RFC 1157.
SNMP Trap	Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.
SOAP	Simple Object Access Protocol (SOAP). The protocol that the Northbound Interface in Prizm uses to support integration of Prizm with an operations support systems (OSS) such as a customer relationship management (CRM), billing, or provisioning system
SSE	Bandwidth and Authentication Manager (BAM) interface to the SQL server. Unique sets of commands are available on this interface to manage the BAM SQL database and user access. Distinguished from Engine. See also Engine.
Standard Operating Margin	See Fade Margin.
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html . See also DHCP.
su -	A command that opens a Linux® operating system session for the user root.
Subnet Mask	32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.
Subscriber Module	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
Sustained Data Rate	Preset rate limit of data transfer.
Switch	Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.

SYN/I	Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Sync	GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.
TCP	Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html .
tcp	Transport Control type of port. The system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE telnet communications, and Port 9090:tcp for Engine telnet communications.
TDD	Time Division Duplexing. Synchronized data transmission with some time slots allocated to devices transmitting on the uplink and some to the device transmitting on the downlink.
telnet	Utility that allows a client computer to update a server. A firewall can prevent the use of the telnet utility to breach the security of the server. See http://www.faqs.org/rfcs/rfc818.html , http://www.faqs.org/rfcs/rfc854.html and http://www.faqs.org/rfcs/rfc855.html .
Textual Conventions MIB	Management Information Base file that defines system-specific textual conventions. See also Management Information Base.
Time of Last Transaction	A field in the data that the cmd show esn command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM. Expressed in the database output as TLT.
TLT	Time of last transaction. A field in the data that the cmd show esn command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the time of day of the most recent authentication attempt by the SM.
TNAF	Total number of authentication requests failed. A field in the data that the cmd show esn command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate but was denied by BAM.

TNAR	Total number of authentication requests. A field in the data that the cmd show esn command generates from the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field indicates how many times the SM (identified by ESN in the related data) attempted to authenticate, regardless of whether the attempt succeeded.
Tokens	Theoretical amounts of data. See also Buckets.
TOS	8-bit field in that prioritizes data in a IP transmission. See http://www.faqs.org/rfcs/rfc1349.html .
TxUnderrun Field	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
UDP	User Datagram Protocol. A set of Network, Transport, and Session Layer protocols that RFC 768 defines. These protocols include checksum and address information but does not retransmit data or process any errors. See http://www.faqs.org/rfcs/rfc768.html .
UDP	User-defined type of port.
U-NII	Unlicensed National Information Infrastructure radio frequency band, in the 5.1-GHz through 5.8-GHz ranges.
VID	VLAN identifier. See also VLAN.
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	Virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. SMs support L2TP over IPsec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.