Cambium PMP 450 Operations Guide

System Release 12.0

Cambium Networks

PMP 450 module essential information

Table 1 PMP 450 module essential information

Default IP Address for Management GUI Access	169.254.1.1
Default Administrator Username	admin
Default Administrator Password	(no password)
Software Upgrade Procedure	See "Updating the software version and using CNUT" in the *PMP 450 Configuration and User Guide*
Resetting the Module to Factory Defaults (2 options)	1. On the radio GUI, navigate to **Configuration**, **Unit Settings** and select **Set to Factory Defaults** ***OR*** 2. On the radio GUI, navigate to **Configuration**, **Unit Settings** and enable and save option **Set to Factory Defaults Upon Default Plug Detection**. When the unit is powered on with a default/override plug (see section "Acquiring the Override Plug" in the *PMP 450 Configuration and User Guide*) the radio will be returned to its factory default settings.

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.

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 AP or SM unit's 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

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 AP/SM so as to provide and maintain the minimum separation distances from all persons.

The minimum separation distances for each frequency variant are specified in Calculated distances and power compliance margins on page 8-11.

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.

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 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 radar systems that operate in the 5250-5350 and 5470-5725 MHz bands. These features must be implemented in all products able to operate outdoors in the UNII band. The use of the 5600 – 5650 MHz band is prohibited, even with detect-and-avoid functionality implemented.

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 rule.

Contents

List of Figures

List of Tables

About This Operations Guide

This guide discusses the techniques to maintain and grow a PMP 450 network.

Users of this guide should have knowledge of the following areas:

- Radio network design
- Outdoor radio equipment installation
- System installation, configuration, monitoring and fault finding

This guide contains the following chapters:

General information

Version information

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

Issue	Date of issue	Remarks
001v000	September 2012	System Release 12.0

Contacting Cambium Networks

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

Cambium main website: http://www.cambiumnetworks.com/

Sales enquiries: solutions@cambiumnetworks.com

Email support: support@cambiumnetworks.com

Telephone numbers:

For full list of Cambium support telephone numbers, see:

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

Address:

Cambium Networks
3800 Golf Road, Suite 360
Rolling Meadows, IL 60008

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. http://www.cambiumenetworks.com/support/pmp/software/index.php
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.
    - CNUT Support Capture Tool information
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.

Extended warranties are available for PMP 450 products. 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
>
> **Warning text and consequence for not following the instructions in the warning.**

Cautions

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

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

Notes

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

> NOTE
>
> Note text.

Chapter 1: Growing Your Network

Keys to successfully growing your network include

- monitoring the RF environment.
- considering software release compatibility.
- redeploying modules appropriately and quickly.

Monitoring the RF environment

Regardless of whether you are maintaining or growing your network, you may encounter new RF traffic that can interfere with your current or planned equipment. Regularly measuring *over a period of time* and logging the RF environment, as you did before you installed your first equipment in an area, enables you to recognize and react to changes. See section Using the Spectrum Analyzer Tool on page 5-1 for details.

Considering Software Release Compatibility

Within the same network, modules can operate on multiple software releases. However, the features that can be enabled are limited to those that the earliest software supports.

MIB File Set Compatibility

Although MIB files are text files (not software), they define objects associated with configurable parameters and indicators for the module and its links. In each release, some of these parameters and indicators are not carried forward from the previous release, and some parameters and indicators are introduced or changed.

For this reason, use the MIB files from your download to replace previous MIB files in conjunction with your software upgrades, even if the file names are identical to those of your previous files. Date stamps on the MIB files distinguish the later set.

MIB files may be downloaded from:
http://www.cambiumnetworks.com/support/pmp/software/index.php

Redeploying Modules

Successfully redeploying a module may involve

- maintaining full and accurate records of modules being redeployed from warehouse stock.
- exercising caution about

  - software compatibility. For example, whether desired features can be enabled with the redeployed module in the network.
  - hardware compatibility; for example, where a CMMmicro is deployed.
  - the value of each configurable parameter. Whether all are compatible in the new destination.
- remembering to use auto discovery to add the redeployed SM to the network in Wireless Manager

Wiring to Extend Network Sync

The following procedure can be used to extend network sync by one additional hop. Where a collocated module receives sync over the air, the collocated modules can be wired to pass the sync as follows:

Procedure 1 Wiring to extend network synchronization

1 Connect the GPS Utility ports of the collocated modules using a sync cable with RJ-11 connectors.

2 Set the **Sync Input** parameter on the Configuration page of the collocated AP timing master to **Sync to Received Signal (Timing Port)**.

3 Set the **Frame Timing Pulse Gated** parameter on the Configuration page of the collocated SM timing slave to **Enable.**
NOTE: This setting prevents interference in the event that the SM timing slave loses sync.

Chapter 2: Managing Bandwidth and Authentication

This section provides a high-level description of bandwidth and authentication management in a network, and includes the following sections:

- Configuring quality of service on page 2-2 describes the Quality of Service (QoS) mechanisms implemented in the PMP 450 system.
- Configuring a RADIUS server on page 2-15 describes how to integrate a RADIUS server into a PMP 450 management network.

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.

Maximum Information Rate Data Entry Checking

Uplink and downlink MIR is enforced as shown in Figure 1.

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

Figure 1 Uplink and downlink rate caps adjusted to apply aggregate cap

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

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

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 high priority channel enabled on all SMs, the total sector capacity is reduced by 50%.

A module prioritizes traffic by

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

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

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

NOTE

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

An example of the Diffserv tab in the Configuration page and parameter descriptions are provided under DiffServ Tab of the AP on Page 2-10. 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 2.

Table 2 Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	90 Mbps
Latency	Number of frames required for the scheduling process	1
	Round-trip latency	≈ 6 ms
	AP broadcast the download schedule	No
High-priority Channel	Allocation for *uplink* high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for *downlink* high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	Other high-priority Other low-priority

⚠ 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, and the high-priority channel as follows. The **Configuration Source** parameter affects the source of:

- all MIR settings:
    - Sustained Uplink Data Rate
    - Uplink Burst Allocation
    - 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

Table 3 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	**Disabled**
	Configuration Source	Configuration/ General	**SM**
Wireless Manager (Authentication Server)	**Authentication Mode**	Configuration/ Security	**Authentication Server**
	Configuration Source	Configuration/ General	**Authentication Server**
RADIUS AAA server	**Authentication Mode**	Configuration/ Security	**RADIUS AAA**
	Configuration Source	Configuration/ General	**Authentication Server**

Table 4 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
Authentication Server	Authentication Server	Authentication Server	Authentication Server
SM	SM	SM	SM
Authentication Server+SM	Authentication Server	Authentication Server, then SM	Authentication Server, then SM

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.

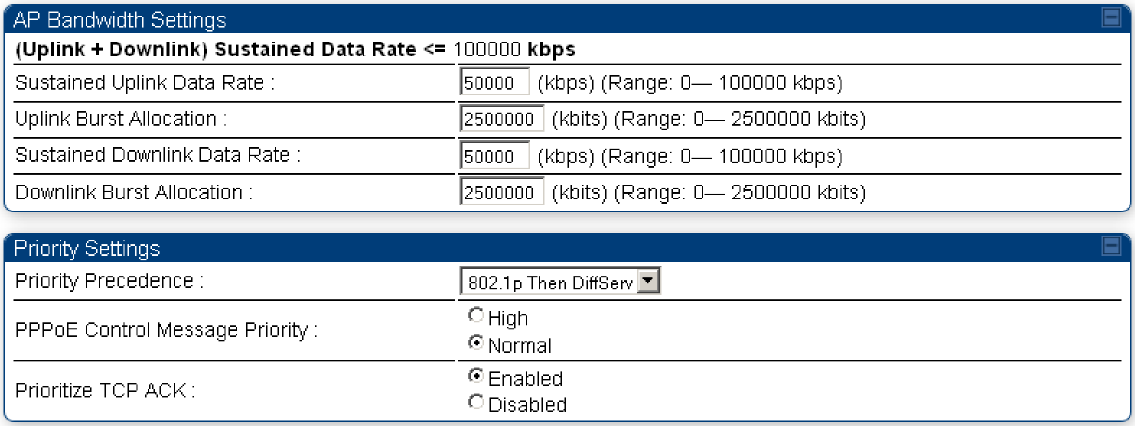
For any SM whose **Authentication Mode** parameter *is not* set to **Authentication Required**, the listed settings are derived as shown:

Table 5 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
Authentication Server	AP	AP	AP
SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM

Quality of Service (QoS) Tab of the AP

Figure 2 Quality of Service (QoS) tab of the AP



AP Bandwidth Settings

(Uplink + Downlink) Sustained Data Rate <= 100000 **kbps**

Sustained Uplink Data Rate :	50000 (kbps) (Range: 0— 100000 kbps)
Uplink Burst Allocation :	2500000 (kbits) (Range: 0— 2500000 kbits)
Sustained Downlink Data Rate :	50000 (kbps) (Range: 0— 100000 kbps)
Downlink Burst Allocation :	2500000 (kbits) (Range: 0— 2500000 kbits)

Priority Settings

Priority Precedence :	802.1p Then DiffServ
PPPoE Control Message Priority :	○ High ● Normal
Prioritize TCP ACK :	● Enabled ○ Disabled

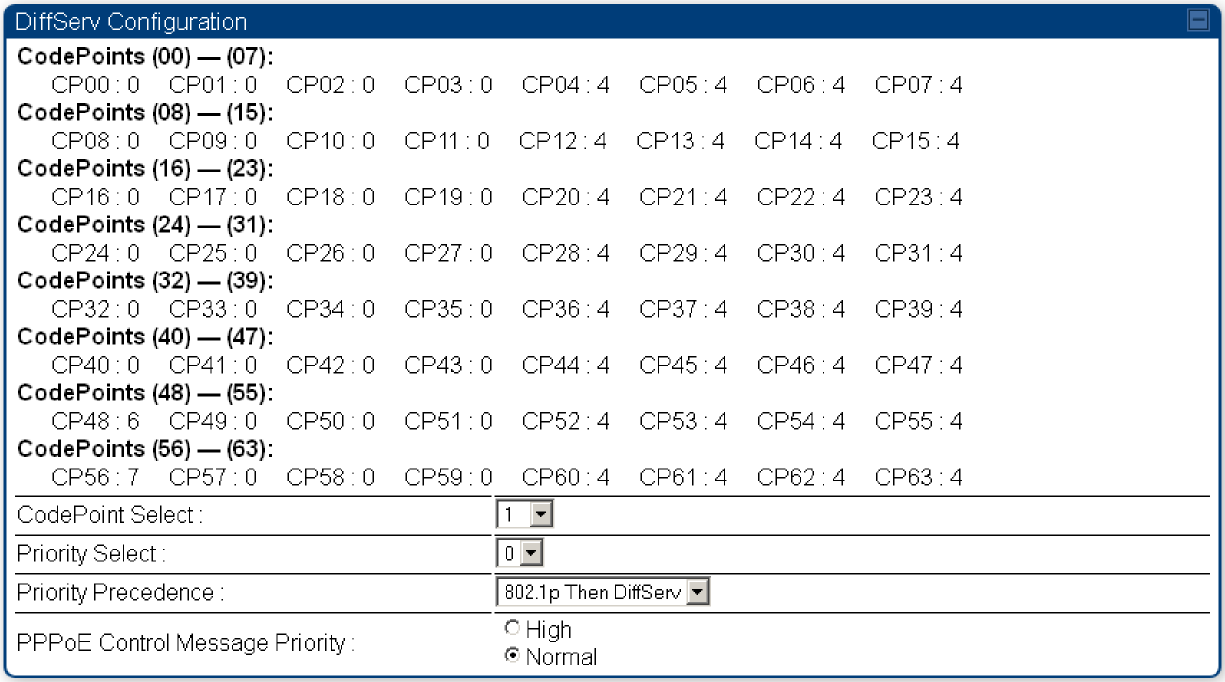
In the Quality of Service (QoS) tab, you may set AP bandwidth parameters as follows.

Table 6 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 • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6
Uplink Burst Allocation	Specify the maximum amount of data to allow each SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6
Sustained Downlink Data Rate	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 • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6

Attribute	Meaning
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. See • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6
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 AP to utilize the high priority channel for PPPoE control messages. Configuring the AP in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the AP.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements.

DiffServ Tab of the AP



DiffServ Configuration

CodePoints (00) — (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4
CodePoints (08) — (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4
CodePoints (16) — (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4
CodePoints (24) — (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4
CodePoints (32) — (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4
CodePoints (40) — (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 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 :	1
Priority Select :	0
Priority Precedence :	802.1p Then DiffServ
PPPoE Control Message Priority :	○ High ● Normal

Figure 3 Diffserv tab of the AP

You may set the following Diffserv tab parameters.

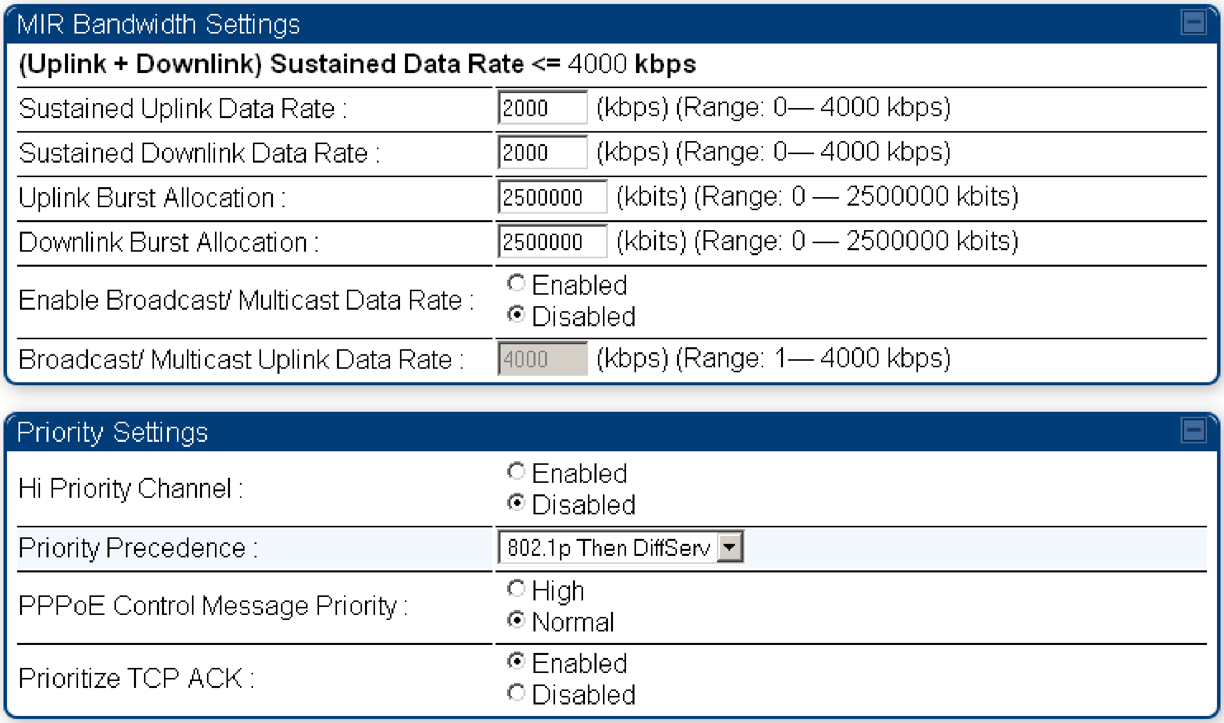
Table 7 AP Diffserv attributes

Attribute	Meaning
CodePoint 1 through CodePoint 47 CodePoint 49 through CodePoint 55 CodePoint 57 through CodePoint 63	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 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). 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.
CodePoint Select	This represents the CodePoint Selection to be modified via Priority Select
Priority Select	The priority setting input for the CodePoint selected in CodePoint Select
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits should be used first when making priority decisions.

Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the AP to utilize the high priority channel for PPPoE control messages. Configuring the AP in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the AP.

Quality of Service (QoS) Tab of the SM

Figure 4 Quality of Service (QoS) tab of the SM



MIR Bandwidth Settings

(Uplink + Downlink) Sustained Data Rate <= 4000 **kbps**

Sustained Uplink Data Rate :	2000 (kbps) (Range: 0— 4000 kbps)
Sustained Downlink Data Rate :	2000 (kbps) (Range: 0— 4000 kbps)
Uplink Burst Allocation :	2500000 (kbits) (Range: 0 — 2500000 kbits)
Downlink Burst Allocation :	2500000 (kbits) (Range: 0 — 2500000 kbits)
Enable Broadcast/ Multicast Data Rate :	○ Enabled ● Disabled
Broadcast/ Multicast Uplink Data Rate :	4000 (kbps) (Range: 1— 4000 kbps)

Priority Settings

Hi Priority Channel :	○ Enabled ● Disabled
Priority Precedence :	802.1p Then DiffServ
PPPoE Control Message Priority :	○ High ● Normal
Prioritize TCP ACK :	● Enabled ○ Disabled

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

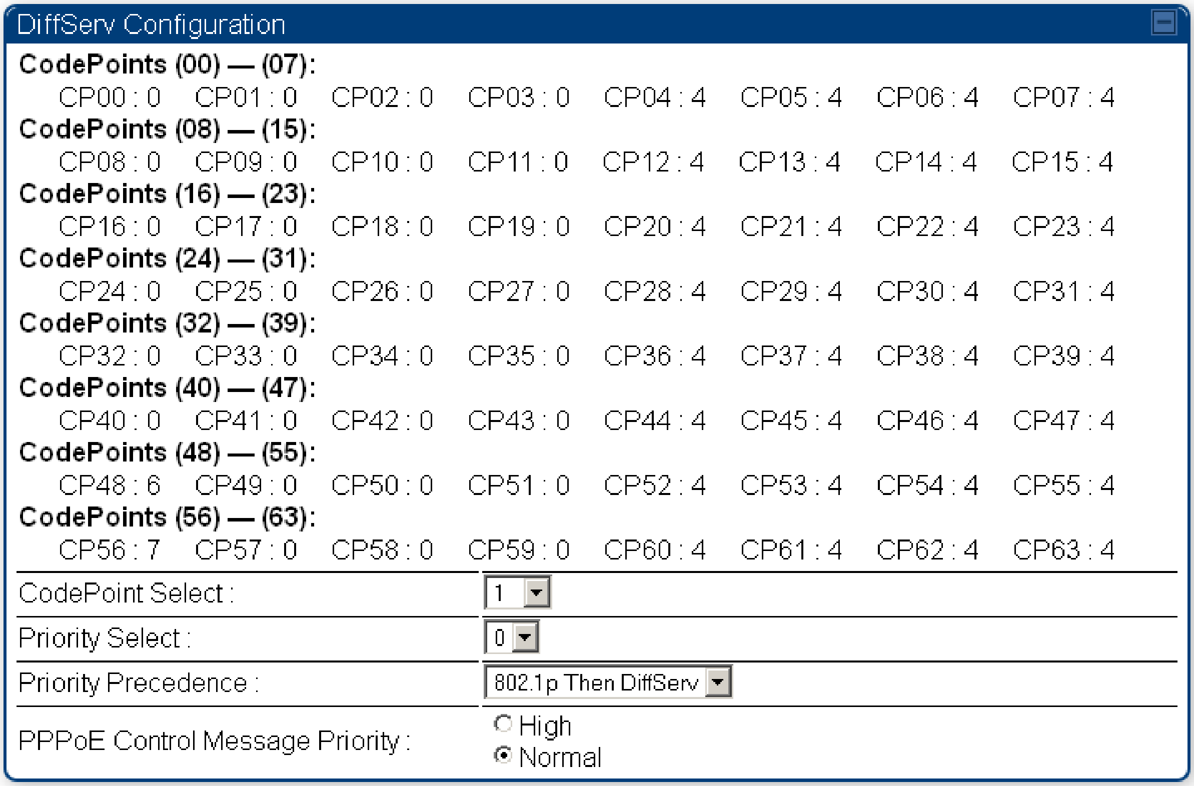
Table 8 AP Quality of Service attributes

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 • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6

Attribute	Meaning
Sustained Downlink Data Rate	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 • Maximum Information Rate (MIR) Parameters on Page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6
Uplink Burst Allocation	Specify the maximum amount of data to allow this SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the **Sustained Downlink Data Rate** with transmission credits. See • Maximum Information Rate (MIR) Parameters on page 2-2 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-3 • Setting the Configuration Source on page 2-6
Hi Priority Channel	See • High-priority Bandwidth on page 2-4 • Setting the Configuration Source on page 2-6
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.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements.

DiffServ Tab of the SM

Figure 5 Diffserv tab of the SM



DiffServ Configuration

CodePoints (00) — (07):

CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4

CodePoints (08) — (15):

CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4

CodePoints (16) — (23):

CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4

CodePoints (24) — (31):

CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4

CodePoints (32) — (39):

CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4

CodePoints (40) — (47):

CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 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 :	1
Priority Select :	0
Priority Precedence :	802.1p Then DiffServ
PPPoE Control Message Priority :	○ High ● Normal

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

Table 9 SM Diffserv attributes

Attribute	Meaning
CodePoint 1 through CodePoint 47 CodePoint 49 through CodePoint 55 CodePoint 57 through CodePoint 63	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 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). 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.
CodePoint Select	This represents the CodePoint Selection to be modified via Priority Select
Priority Select	The priority setting input for the CodePoint selected in CodePoint Select
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits 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.

Configuring a RADIUS server

Configuring a RADIUS 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

RADIUS Functions

RADIUS protocol support provides the following functions:

- **SM Authentication** allows only known SMs onto the network (blocking "rogue" SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to "rogue" APs). RADIUS authentication is used for SMs, but is not used for APs.
- **SM Configuration:** Configures authenticated SMs with MIR (Maximum Information Rate), 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

Note, Aradial 5.3 has a bug that prevents "remote device login", preventing usage of the user name and password management features.

Choosing Authentication Mode and Configuring for Authentication Servers - AP

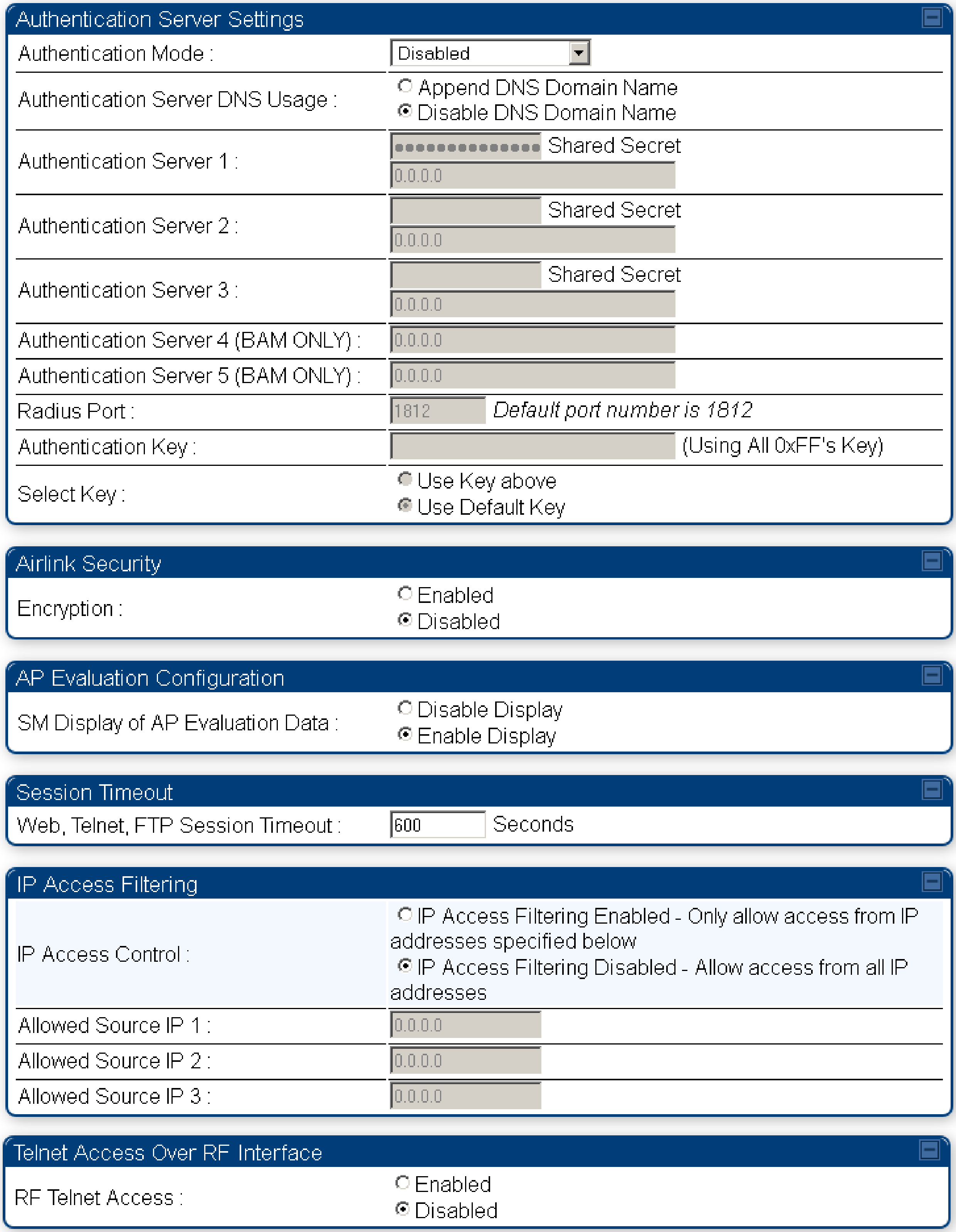
On the AP's Configuration > Security tab, select the **RADIUS AAA Authentication Mode**. The following describes the other **Authentication Mode** options for reference, and then the **RADIUS AAA** option.

- **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 Wireless Manager in BAM-only mode. Authentication will be required for an SM to register to the AP. Only SMs listed by MAC address in the Wireless Manager 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 6 Security tab of the AP



Authentication Server Settings

Authentication Mode :	Disabled
Authentication Server DNS Usage :	○ Append DNS Domain Name ● Disable DNS Domain Name
Authentication Server 1 :	●●●●●●●●●●●●●● Shared Secret 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 *Default port number is 1812*
Authentication Key :	(Using All 0xFF's Key)
Select Key :	○ Use Key above ● Use Default Key

Airlink Security

Encryption :	○ Enabled ● Disabled

AP Evaluation Configuration

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

Session Timeout

Web, Telnet, FTP Session Timeout :	600 Seconds

IP Access Filtering

IP Access Control :	○ IP Access Filtering Enabled - Only allow access from IP addresses specified below ● IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0
Allowed Source IP 2 :	0.0.0.0
Allowed Source IP 3 :	0.0.0.0

Telnet Access Over RF Interface

RF Telnet Access :	○ Enabled ● Disabled

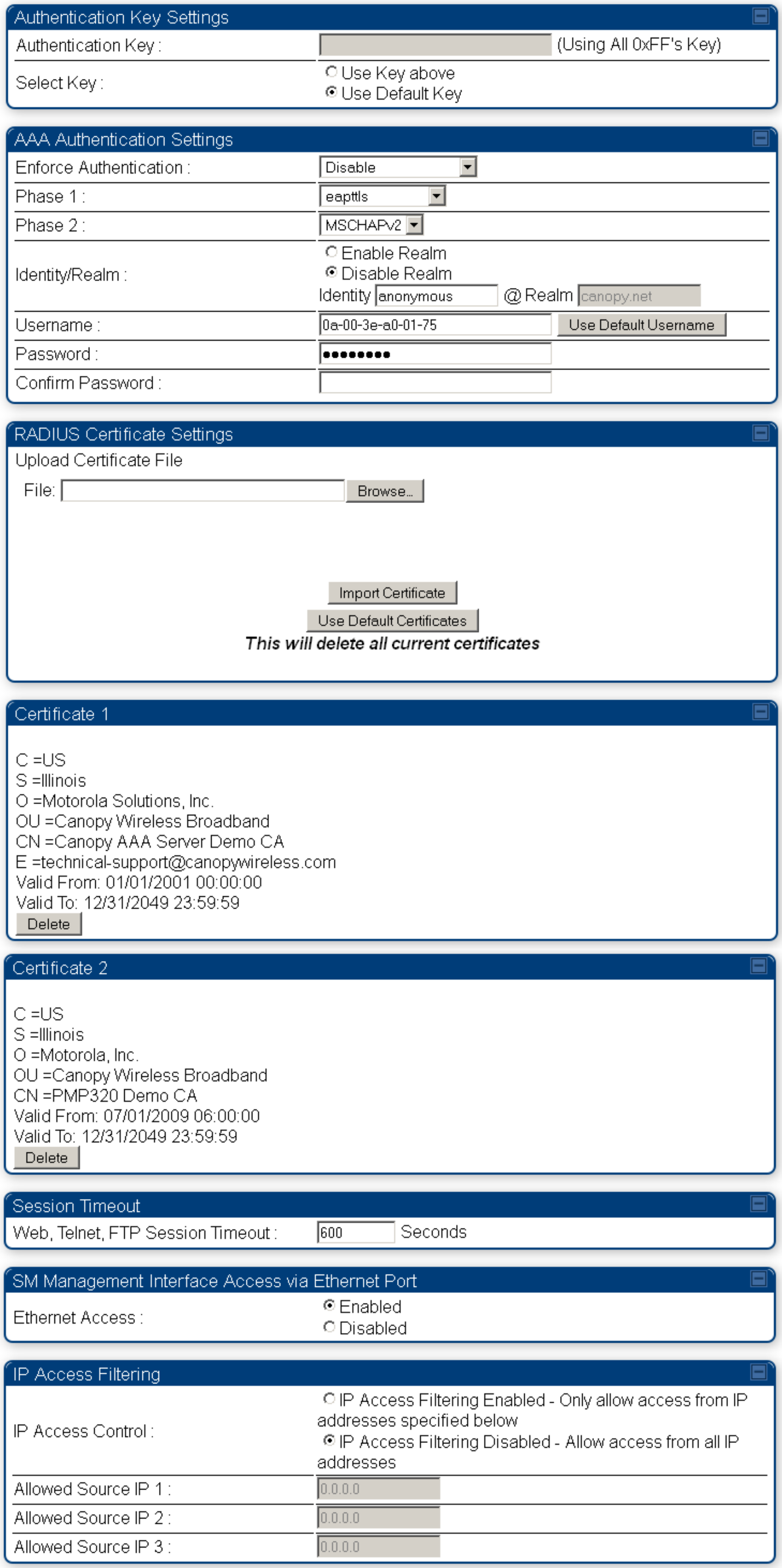
SM Authentication Mode – Require RADIUS or Follow AP

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 7 Security tab of the SM



Authentication Key Settings

Authentication Key :	(Using All 0xFF's Key)
Select Key :	○ Use Key above ● Use Default Key

AAA Authentication Settings

Enforce Authentication :	Disable
Phase 1 :	eapttls
Phase 2 :	MSCHAPv2
Identity/Realm :	○ Enable Realm ● Disable Realm Identity anonymous @ Realm canopy.net
Username :	0a-00-3e-a0-01-75 Use Default Username
Password :	••••••••
Confirm Password :	

RADIUS Certificate Settings

Upload Certificate File

File: Browse...

Import Certificate

Use Default Certificates

This will delete all current certificates

Certificate 1

C =US
S =Illinois
O =Motorola Solutions, Inc.
OU =Canopy Wireless Broadband
CN =Canopy AAA Server Demo CA
E =technical-support@canopywireless.com
Valid From: 01/01/2001 00:00:00
Valid To: 12/31/2049 23:59:59
Delete

Certificate 2

C =US
S =Illinois
O =Motorola, Inc.
OU =Canopy Wireless Broadband
CN =PMP320 Demo CA
Valid From: 07/01/2009 06:00:00
Valid To: 12/31/2049 23:59:59
Delete

Session Timeout

Web, Telnet, FTP Session Timeout :	600 Seconds

SM Management Interface Access via Ethernet Port

Ethernet Access :	● Enabled ○ Disabled

IP Access Filtering

IP Access Control :	○ IP Access Filtering Enabled - Only allow access from IP addresses specified below ● IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0
Allowed Source IP 2 :	0.0.0.0
Allowed Source IP 3 :	0.0.0.0

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 **eapttls** 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.

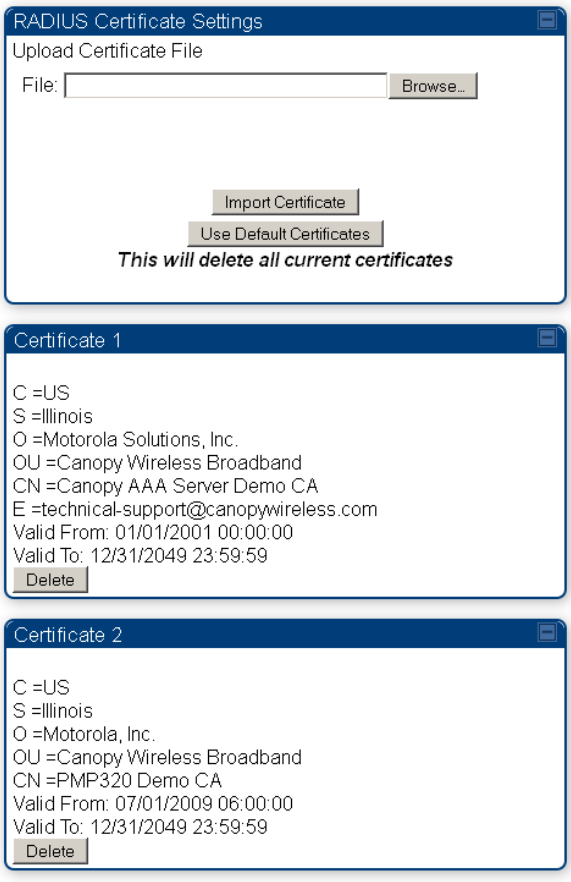
Up to 2 certificates can be resident on an SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore fhe 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate 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 8 SM Certificate Management



This will delete all current certificates

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

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

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).

Configuring your RADIUS server for SM configuration

Table 10 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 Cambium-Canopy-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Cambium-Canopy-Gateway attribute and is available on the Cambium 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 Cambium-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 Cambium-Canopy-Gateway defaults to 0.0.0.0.

Table 10 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Req’d	Value	
SM GUI Page > Tab > Parameter				**Default**	**Size**
MS-MPPE-Send-Key	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key	26.311.17	-	Y	-	
-				-	-
Cambium-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable	
Configuration > Quality of Service > Hi Priority Channel				0	32 bits
Cambium-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
Cambium-Canopy-ULBL	26.161.7	integer	N	0-50000+ kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Cambium-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
Cambium-Canopy-DLBL	26.161.9	integer	N	0-50000+ kbps	

Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Cambium-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Cambium-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Cambium-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Cambium-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Cambium-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits
Cambium-Canopy-	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Cambium-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
Cambium-Canopy-Gateway	26.161.25	ipaddr	N	-	
Configuration > IP > Gateway IP Address				0.0.0.0	-
Cambium-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.

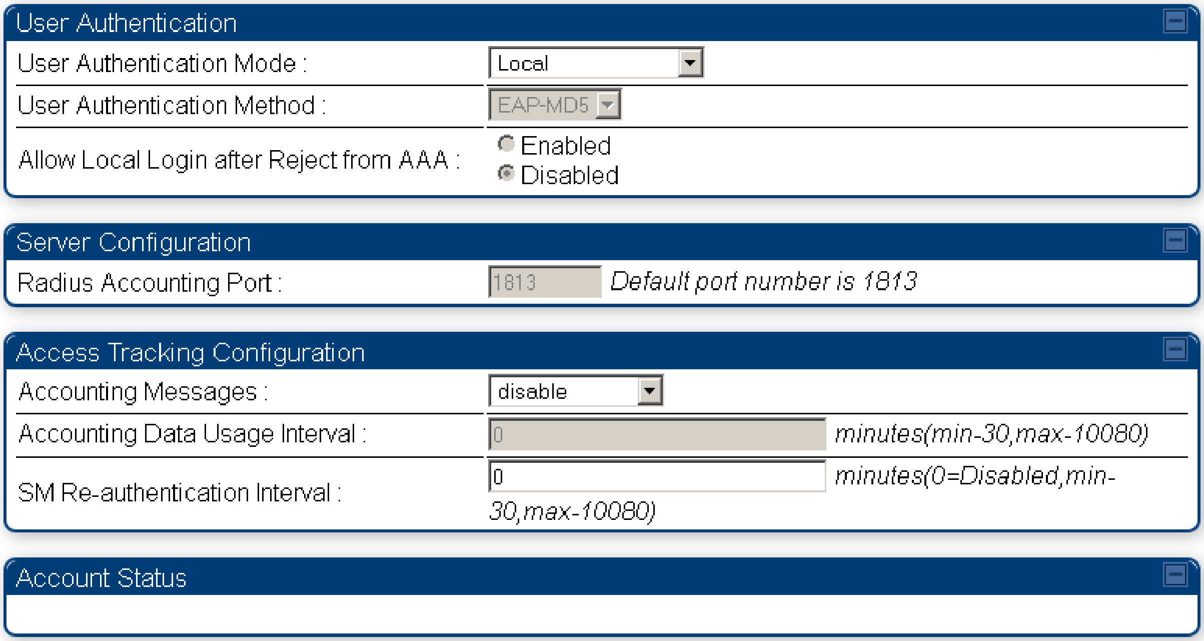
- **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, 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 can be used for user authentication and accounting (access control), or a separate RADIUS accounting server can be used. Indicate your network design under **Authentication Server Settings** in the AP's **Security** tab.

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 9 User Authentication tab of the AP



User Authentication

User Authentication Mode :	Local
User Authentication Method :	EAP-MD5
Allow Local Login after Reject from AAA :	○ Enabled ● Disabled

Server Configuration

Radius Accounting Port :	1813 *Default port number is 1813*

Access Tracking Configuration

Accounting Messages :	disable
Accounting Data Usage Interval :	0 *minutes(min-30,max-10080)*
SM Re-authentication Interval :	0 *minutes(0=Disabled,min-30,max-10080)*

Account Status

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 **RADIUS AAA** (RADIUS)

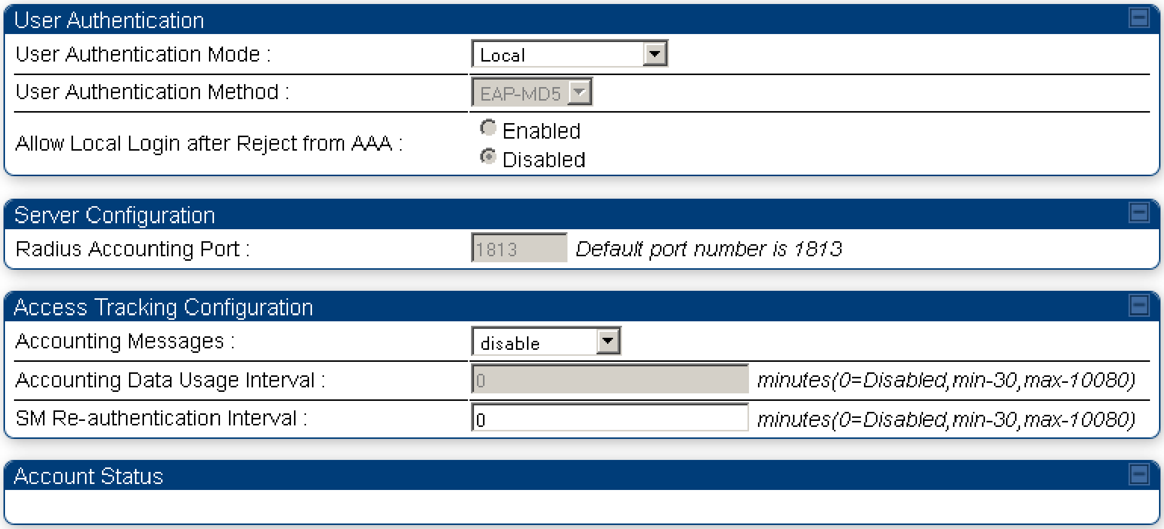
2 Set **User Authentication Mode** on the AP's Account > User Authentication and Access Tracking tab (the tab only appears after the AP is set to AAA authentication) to **Remote** or **Remote then Local**.

3 Set **User Authentication Mode** on the SM's Account > User Authentication and Access Tracking 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.

igure 10 User Authentication and Access Tracking tab of the AP



User Authentication

User Authentication Mode : Local

User Authentication Method : EAP-MD5

Allow Local Login after Reject from AAA : ○ Enabled ● Disabled

Server Configuration

Radius Accounting Port : 1813 *Default port number is 1813*

Access Tracking Configuration

Accounting Messages : disable

Accounting Data Usage Interval : 0 *minutes(0=Disabled,min-30,max-10080)*

SM Re-authentication Interval : 0 *minutes(0=Disabled,min-30,max-10080)*

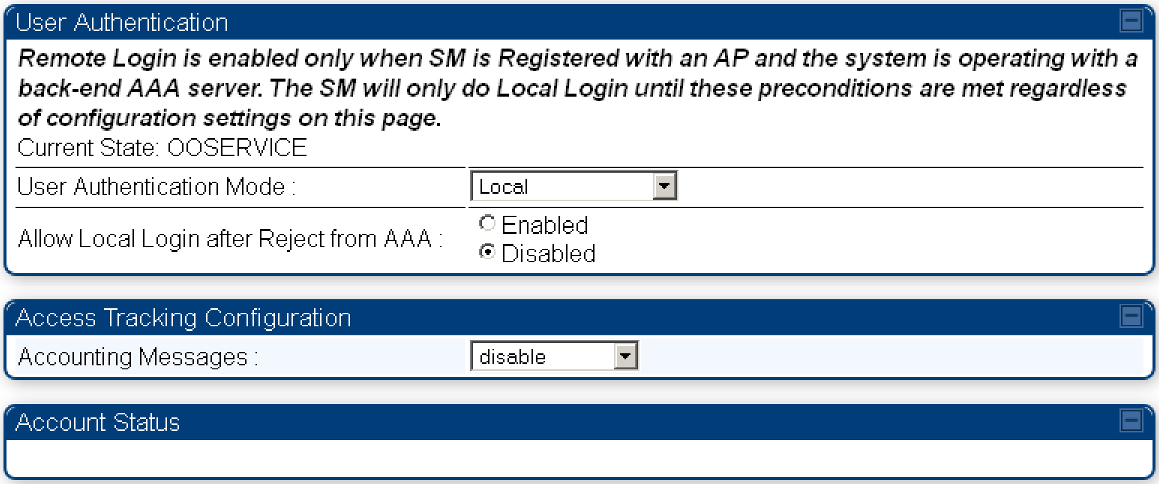
Account Status

Table 11 AP User Authentication and Access Tracking attributes

Attribute	Meaning
User Authentication Mode	• **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 AP. 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 AP.
User Authentication Method	The user authentication method employed by the radios is EAP-MD5.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user will be allowed to login locally to the radio's management interface.

Attribute	Meaning
Radius Accounting Port	The destination port on the AAA server used for Radius accounting communication.
Accounting Messages	• disable – no accounting messages are sent to the RADIUS server • deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 13). • dataUsage – accounting messages are sent to the RADIUS server regarding data usage (see Table 13).
Accounting Data Usage Interval	The interval for which accounting data messages are sent from the radio to the RADIUS server. If 0 is configured for this parameter, no data usage messages are sent.
SM Re-authentication Interval	The interval for which the SM will re-authenticate to the RADIUS server.

Figure 11 User Authentication tab of the SM



User Authentication

Remote Login is enabled only when SM is Registered with an AP and the system is operating with a back-end AAA server. The SM will only do Local Login until these preconditions are met regardless of configuration settings on this page.

Current State: OOSERVICE

User Authentication Mode :	Local
Allow Local Login after Reject from AAA :	○ Enabled ● Disabled

Access Tracking Configuration

Accounting Messages :	disable

Account Status

Table 12 SM User Authentication and Access Tracking attributes

Attribute	Meaning
User Authentication Mode	• **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.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user will be allowed to login locally to the radio's management interface.
Accounting Messages	• disable – no accounting messages are sent to the RADIUS server • deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 13).

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 Access Tracking** tab under **Accounting** (Access Tracking) set **Accounting Messages** to "deviceAccess".

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 13 Device data accounting RADIUS attributes

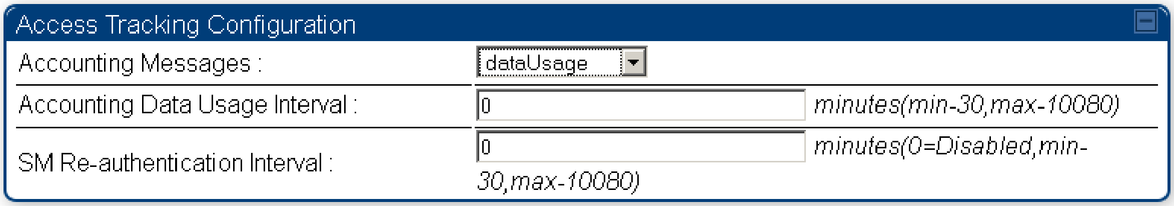
Sender	Message	Attribute	Value	Description
AP	Accounting-Request	Acct-Status-Type	1 - Start	This message is sent every time an SM registers with an AP, and after the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		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	

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).	
		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	This message is sent periodically per the operator configuration on the AP in seconds. Interim update counts are cumulative over the course of the session
		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	

Sender	Message	Attribute	Value	Description
		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.	
		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 14 RADIUS accounting messages configuration



Access Tracking Configuration

Accounting Messages : dataUsage

Accounting Data Usage Interval : 0 minutes(min-30,max-10080)

SM Re-authentication Interval : 0 minutes(0=Disabled,min-30,max-10080)

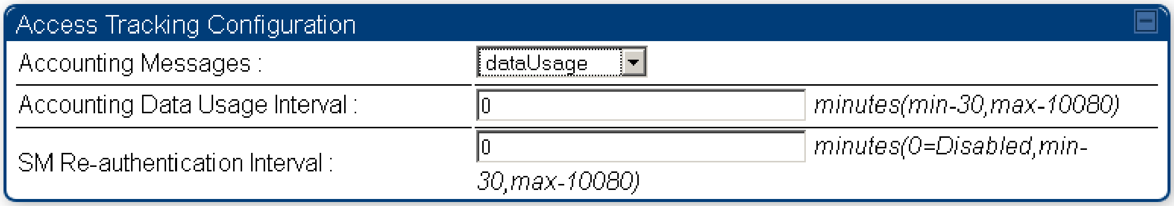
The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify 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 15 Device re-authentication configuration



Access Tracking Configuration

Accounting Messages :	dataUsage ▾	
Accounting Data Usage Interval :	0	*minutes(min-30,max-10080)*
SM Re-authentication Interval :	0	*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 Cambium-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Cambium-Gateway attribute and is available on the Cambium 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 Cambium-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 Cambium-Gateway defaults to 0.0.0.0

Chapter 3: Managing the network from a Network Management Station (NMS)

SNMPv2 (Simple Network Management Protocol Version 2) can be used to manage and monitor the modules under SMI (Structure of Management Information) specifications. SMI specifies management information definitions in ASN.1 (Abstract Syntax Notation One) language. SNMPv2 supports both 32-bit and 64-bit counters. The SMI for SNMPv2 is defined in RFC 1902 at http://www.faqs.org/rfcs/rfc1902.html.

Roles of Hardware and Software Elements

Role of the Agent

In SNMP, software on each managed device acts as the *agent*. The agent collects and stores management information in ASN.1 format, in a structure that a MIB (management information base) defines. The agent responds to commands to

- send information about the managed device.
- modify specific data on the managed device.

Role of the Managed Device

In SNMP, the managed device is the network element that operates on the agent software. In the fixed wireless broadband IP network, this managed device is the module (AP, SM, or BH). With the agent software, the managed device has the role of server in the context of network management.

Role of the NMS

In SNMP, the NMS (network management station) has the role of client. An application (manager software) operates on the NMS to manage and monitor the modules in the network through interface with the agents.

Dual Roles for the NMS

The NMS can simultaneously act as an agent. In such an implementation, the NMS acts as

- client to the agents in the modules, when polling for the agents for information and sending modification data to the agents.
- server to another NMS, when being polled for information gathered from the agents and receiving modification data to send to the agents.

Simple Network Management Protocol (SNMP) Commands

To manage a module, SNMPv2 supports the `set` command, which instructs the agent to change the data that manages the module.

To monitor a network element, SNMPv2 supports

- the `get` command, which instructs the agent to send information about the module to the manager in the NMS.

- traversal operations, which the manager uses to identify supported objects and to format information about those objects into relational tables.

In a typical network, the manager issues these commands to the agents of more than one module (to all SMs in the operator network, for example).

Traps from the Agent

When a specified event occurs in the module, the agent initiates a trap, for which the agent sends an unsolicited asynchronous message to the manager.

AP SNMP Proxy to SMs

When the AP receives from an NMS an SNMP request for an SM, it is capable of sending that request via proxy to the SM. In this case, the SM responds directly to the NMS. (The AP performs no processing on the response.)

Management Information Base (MIB)

The MIB, the SNMP-defined data structure, is a tree of standard branches that lead to optional, non-standard positions in the data hierarchy. The MIB contains both

- objects that SNMP is allowed to control (bandwidth allocation or access, for example)
- objects that SNMP is allowed to monitor (packet transfer, bit rate, and error data, for example).

The path to each object in the MIB is unique to the object. The endpoint of the path is the object identifier.

Cascading Path to the MIB

The standard MIB hierarchy includes the following cascading branch structures:

- the top (standard body) level:
  - ccitt (0)
  - **iso (1)**
  - iso-ccitt (2)
- under iso (1) above:
  - standard (0)
  - registration-authority (1)
  - member-body (2)
  - **identified-organization (3)**
- under identified-organization (3) above:
  - dod (6)
  - other branches
- under dod (6) above:
  - internet (1)
  - other branches
- under internet (1) above:
  - mgmt (2)
  - private (4)
  - other branches
- under mgmt (2) above: mib-2 (1) and other branches. (See MIB-II below.)
- under private (4) above: enterprise (1) and other branches. (See Canopy Enterprise MIB below.)
- Beneath this level are non-standard branches that the enterprise may define.

Thus, the path to an object that is managed under MIB-II begins with the decimal string **1.3.6.1.2.1** and ends with the object identifier and instance(s), and the path to an object that is managed under the Cambium Enterprise MIB begins with **1.3.6.1.4.1**, and ends with the object identifier and instance(s).

Object Instances

An object in the MIB can have either only a single instance or multiple instances, as follows:

- a scalar object has only a single instance. A reference to this instance is designated by `.0`, following the object identifier.
- a tabular object has multiple instances that are related to each other. Tables in the MIB associate these instances. References to these instances typically are designated by `.1`, `.2`, and so forth, following the object identifier.

Management Information Base Systems and Interface (MIB-II)

The standard MIB-II (Management Information Base systems and interface) objects are programmed into the modules. To read this MIB, see *Management Information Base for Network Management of TCP/IP-based Internets: MIB II*, RFC 1213 at http://www.faqs.org/rfcs/rfc1213.html.

The MIB-II standard categorizes each object as one of the types defined in Table 16.

Table 16 Categories of MIB-II objects

Objects in category…	Control or identify the status of…
system	system operations in the module.
interfaces	the network interfaces for which the module is configured.
ip	Internet Protocol information in the module.
icmp	Internet Control Message Protocol information in the module. (These messages flag IP problems and allow IP links to be tested.)
tcp	Transport Control Protocol information in the module (to control and ensure the flow of data on the Internet).
udp	User Datagram Protocol information in the module (for checksum and address).

Canopy Enterprise MIB

The Cambium Enterprise MIB provides additional reporting and control, extending the objects for any NMS that uses SNMP interaction. This MIB comprises five text files that are formatted in standard ASN.1 (Abstract Syntax Notation One) language.

To use this MIB with an NMS, perform the following steps.

Procedure 2 Using the MIB with an NMS

1 On the NMS, immediately beneath the `root` directory, create directory *`mibviewer`*.

2 Immediately beneath the *`mibviewer`* directory, create directory *`cambiummibs`*.

3 Download the following three standard MIB files from the Internet Engineering Task Force at http://www.simpleweb.org/ietf/mibs into the *`mibviewer/cambiummibs`* directory on the NMS:

- SNMPv2-SMI.txt, which defines the Structure of Management Information specifications.
- SNMPv2-CONF.txt, which allows macros to be defined for object group, notification group, module compliance, and agent capabilities.
- SNMPv2-TC.txt, which defines general textual conventions.

4 Move the following files or the subset of these files from your software release package directory into the *`mibviewer/cambiummibs`* directory on the NMS. If necessary, first download the “PMP Enterprise MIBs” from http://www.cambiumnetworks.com/support/pmp/software/index.php.

> ⚠ **CAUTION**
>
> Do not edit these MIB files in ASN.1. These files are intended for manipulation by only the NMS. However, you can view these files through a commercially available MIB viewer. Such viewers are listed under MIB Viewers on Page 3-55.

5 Download a selected MIB viewer into directory *`mibviewer`*.

6 As instructed by the user documentation that supports your NMS, import the eight MIB files that are listed above.

SM MIB Objects

The objects that the Canopy Enterprise MIB defines for SMs are listed below:

Table 17 SM MIB Objects

Object Name	OID	Type
rfScanList.0	.1.3.6.1.4.1.161.19.3.2.1.1.0	OctetString
lanIpSm.0	.1.3.6.1.4.1.161.19.3.2.1.3.0	IpAddress
lanMaskSm.0	.1.3.6.1.4.1.161.19.3.2.1.4.0	IpAddress
defaultGwSm.0	.1.3.6.1.4.1.161.19.3.2.1.5.0	IpAddress
networkAccess.0	.1.3.6.1.4.1.161.19.3.2.1.6.0	Integer

authKeySm.0	.1.3.6.1.4.1.161.19.3.2.1.7.0	OctetString
enable8023link.0	.1.3.6.1.4.1.161.19.3.2.1.8.0	Integer
authKeyOption.0	.1.3.6.1.4.1.161.19.3.2.1.9.0	Integer
timingPulseGated.0	.1.3.6.1.4.1.161.19.3.2.1.10.0	Integer
naptPrivateIP.0	.1.3.6.1.4.1.161.19.3.2.1.11.0	IpAddress
naptPrivateSubnetMask.0	.1.3.6.1.4.1.161.19.3.2.1.12.0	IpAddress
naptPublicIP.0	.1.3.6.1.4.1.161.19.3.2.1.13.0	IpAddress
naptPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.2.1.14.0	IpAddress
naptPublicGatewayIP.0	.1.3.6.1.4.1.161.19.3.2.1.15.0	IpAddress
naptRFPublicIP.0	.1.3.6.1.4.1.161.19.3.2.1.16.0	IpAddress
naptRFPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.2.1.17.0	IpAddress
naptRFPublicGateway.0	.1.3.6.1.4.1.161.19.3.2.1.18.0	IpAddress
naptEnable.0	.1.3.6.1.4.1.161.19.3.2.1.19.0	Integer
arpCacheTimeout.0	.1.3.6.1.4.1.161.19.3.2.1.20.0	Integer
tcpGarbageCollectTmout.0	.1.3.6.1.4.1.161.19.3.2.1.21.0	Integer
udpGarbageCollectTmout.0	.1.3.6.1.4.1.161.19.3.2.1.22.0	Integer
dhcpServerEnable.0	.1.3.6.1.4.1.161.19.3.2.1.24.0	Integer
dhcpServerLeaseTime.0	.1.3.6.1.4.1.161.19.3.2.1.25.0	Integer
dhcpIPStart.0	.1.3.6.1.4.1.161.19.3.2.1.26.0	IpAddress
dnsAutomatic.0	.1.3.6.1.4.1.161.19.3.2.1.27.0	Integer
prefferedDNSIP.0	.1.3.6.1.4.1.161.19.3.2.1.28.0	IpAddress
alternateDNSIP.0	.1.3.6.1.4.1.161.19.3.2.1.29.0	IpAddress
dmzIP.0	.1.3.6.1.4.1.161.19.3.2.1.30.0	IpAddress
dmzEnable.0	.1.3.6.1.4.1.161.19.3.2.1.31.0	Integer
dhcpNumIPsToLease.0	.1.3.6.1.4.1.161.19.3.2.1.32.0	Integer
ingressVID.0	.1.3.6.1.4.1.161.19.3.2.1.55.0	Integer
hiPriorityChannel.0	.1.3.6.1.4.1.161.19.3.2.1.58.0	Integer
upLnkDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.62.0	Integer
upLnkLimit.0	.1.3.6.1.4.1.161.19.3.2.1.63.0	Integer
dwnLnkDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.64.0	Integer

dwnLnkLimit.0	.1.3.6.1.4.1.161.19.3.2.1.65.0	Integer
ipAccessFilterEnable.0	.1.3.6.1.4.1.161.19.3.2.1.68.0	Integer
allowedIPAccess1.0	.1.3.6.1.4.1.161.19.3.2.1.69.0	IpAddress
allowedIPAccess2.0	.1.3.6.1.4.1.161.19.3.2.1.70.0	IpAddress
allowedIPAccess3.0	.1.3.6.1.4.1.161.19.3.2.1.71.0	IpAddress
rfDhcpState.0	.1.3.6.1.4.1.161.19.3.2.1.72.0	Integer
bCastMIR.0	.1.3.6.1.4.1.161.19.3.2.1.73.0	Integer
smLEDModeFlag.0	.1.3.6.1.4.1.161.19.3.2.1.75.0	Integer
ethAccessEnable.0	.1.3.6.1.4.1.161.19.3.2.1.76.0	Integer
pppoeEnable.0	.1.3.6.1.4.1.161.19.3.2.1.77.0	Integer
pppoeAuthenticationType.0	.1.3.6.1.4.1.161.19.3.2.1.78.0	Integer
pppoeAccessConcentrator.0	.1.3.6.1.4.1.161.19.3.2.1.79.0	OctetString
pppoeServiceName.0	.1.3.6.1.4.1.161.19.3.2.1.80.0	OctetString
pppoeUserName.0	.1.3.6.1.4.1.161.19.3.2.1.81.0	OctetString
pppoePassword.0	.1.3.6.1.4.1.161.19.3.2.1.82.0	OctetString
pppoeTCPMSSClampEnable.0	.1.3.6.1.4.1.161.19.3.2.1.83.0	Integer
pppoeMTUOverrideEnable.0	.1.3.6.1.4.1.161.19.3.2.1.84.0	Integer
pppoeMTUOverrideValue.0	.1.3.6.1.4.1.161.19.3.2.1.85.0	Integer
pppoeTimerType.0	.1.3.6.1.4.1.161.19.3.2.1.86.0	Integer
pppoeTimeoutPeriod.0	.1.3.6.1.4.1.161.19.3.2.1.87.0	Integer
timedSpectrumAnalysisDuration.0	.1.3.6.1.4.1.161.19.3.2.1.88.0	Integer
spectrumAnalysisOnBoot.0	.1.3.6.1.4.1.161.19.3.2.1.89.0	Integer
spectrumAnalysisAction.0	.1.3.6.1.4.1.161.19.3.2.1.90.0	Integer
pppoeConnectOD.0	.1.3.6.1.4.1.161.19.3.2.1.91.0	Integer
pppoeDisconnectOD.0	.1.3.6.1.4.1.161.19.3.2.1.92.0	Integer
natConnectionType.0	.1.3.6.1.4.1.161.19.3.2.1.94.0	Integer
wanPingReplyEnable.0	.1.3.6.1.4.1.161.19.3.2.1.95.0	Integer
colorCode2.0	.1.3.6.1.4.1.161.19.3.2.1.97.0	Integer
colorCodepriority2.0	.1.3.6.1.4.1.161.19.3.2.1.98.0	Integer

colorCode3.0	.1.3.6.1.4.1.161.19.3.2.1.99.0	Integer
colorCodepriority3.0	.1.3.6.1.4.1.161.19.3.2.1.100.0	Integer
colorCode4.0	.1.3.6.1.4.1.161.19.3.2.1.101.0	Integer
colorCodepriority4.0	.1.3.6.1.4.1.161.19.3.2.1.102.0	Integer
colorCode5.0	.1.3.6.1.4.1.161.19.3.2.1.103.0	Integer
colorCodepriority5.0	.1.3.6.1.4.1.161.19.3.2.1.104.0	Integer
colorCode6.0	.1.3.6.1.4.1.161.19.3.2.1.105.0	Integer
colorCodepriority6.0	.1.3.6.1.4.1.161.19.3.2.1.106.0	Integer
colorCode7.0	.1.3.6.1.4.1.161.19.3.2.1.107.0	Integer
colorCodepriority7.0	.1.3.6.1.4.1.161.19.3.2.1.108.0	Integer
colorCode8.0	.1.3.6.1.4.1.161.19.3.2.1.109.0	Integer
colorCodepriority8.0	.1.3.6.1.4.1.161.19.3.2.1.110.0	Integer
colorCode9.0	.1.3.6.1.4.1.161.19.3.2.1.111.0	Integer
colorCodepriority9.0	.1.3.6.1.4.1.161.19.3.2.1.112.0	Integer
colorCode10.0	.1.3.6.1.4.1.161.19.3.2.1.113.0	Integer
colorCodepriority10.0	.1.3.6.1.4.1.161.19.3.2.1.114.0	Integer
natDNSProxyEnable.0	.1.3.6.1.4.1.161.19.3.2.1.115.0	Integer
spectrumAnalysisDisplay.0	.1.3.6.1.4.1.161.19.3.2.1.117.0	Integer
syslogSMXmitSetting.0	.1.3.6.1.4.1.161.19.3.2.1.118.0	Integer
eapPeerAAAServerCommonName.0	.1.3.6.1.4.1.161.19.3.2.1.126.0	OctetString
sessionStatus.0	.1.3.6.1.4.1.161.19.3.2.2.1.0	OctetString
airDelay.0	.1.3.6.1.4.1.161.19.3.2.2.4.0	Gauge
radioDbm.0	.1.3.6.1.4.1.161.19.3.2.2.8.0	OctetString
registeredToAp.0	.1.3.6.1.4.1.161.19.3.2.2.9.0	OctetString
dhcpCip.0	.1.3.6.1.4.1.161.19.3.2.2.10.0	IpAddress
dhcpSip.0	.1.3.6.1.4.1.161.19.3.2.2.11.0	IpAddress
dhcpClientLease.0	.1.3.6.1.4.1.161.19.3.2.2.12.0	TimeTicks
dhcpCSMask.0	.1.3.6.1.4.1.161.19.3.2.2.13.0	IpAddress
dhcpDfltRterIP.0	.1.3.6.1.4.1.161.19.3.2.2.14.0	IpAddress
dhcpcdns1.0	.1.3.6.1.4.1.161.19.3.2.2.15.0	IpAddress

dhcpcdns2.0	.1.3.6.1.4.1.161.19.3.2.2.16.0	IpAddress
dhcpcdns3.0	.1.3.6.1.4.1.161.19.3.2.2.17.0	IpAddress
dhcpDomName.0	.1.3.6.1.4.1.161.19.3.2.2.18.0	OctetString
adaptRate.0	.1.3.6.1.4.1.161.19.3.2.2.20.0	OctetString
radioDbmInt.0	.1.3.6.1.4.1.161.19.3.2.2.21.0	Integer
radioTxPwr.0	.1.3.6.1.4.1.161.19.3.2.2.23.0	OctetString
activeRegion.0	.1.3.6.1.4.1.161.19.3.2.2.24.0	OctetString
snmpBerLevel.0	.1.3.6.1.4.1.161.19.3.2.2.25.0	Integer
smSessionTimer.0	.1.3.6.1.4.1.161.19.3.2.2.36.0	TimeTicks
pppoeSessionStatus.0	.1.3.6.1.4.1.161.19.3.2.2.37.0	OctetString
pppoeSessionID.0	.1.3.6.1.4.1.161.19.3.2.2.38.0	Integer
pppoeIPCPAddress.0	.1.3.6.1.4.1.161.19.3.2.2.39.0	IpAddress
pppoeMTUOverrideEn.0	.1.3.6.1.4.1.161.19.3.2.2.40.0	Integer
pppoeMTUValue.0	.1.3.6.1.4.1.161.19.3.2.2.41.0	Integer
pppoeTimerTypeValue.0	.1.3.6.1.4.1.161.19.3.2.2.42.0	Integer
pppoeTimeoutValue.0	.1.3.6.1.4.1.161.19.3.2.2.43.0	Integer
pppoeDNSServer1.0	.1.3.6.1.4.1.161.19.3.2.2.44.0	IpAddress
pppoeDNSServer2.0	.1.3.6.1.4.1.161.19.3.2.2.45.0	IpAddress
pppoeControlBytesSent.0	.1.3.6.1.4.1.161.19.3.2.2.46.0	Counter32
pppoeControlBytesReceived.0	.1.3.6.1.4.1.161.19.3.2.2.47.0	Counter32
pppoeDataBytesSent.0	.1.3.6.1.4.1.161.19.3.2.2.48.0	Counter32
pppoeDataBytesReceived.0	.1.3.6.1.4.1.161.19.3.2.2.49.0	Counter32
pppoeEnabledStatus.0	.1.3.6.1.4.1.161.19.3.2.2.50.0	Integer
pppoeTCPMSSClampEnableStatus.0	.1.3.6.1.4.1.161.19.3.2.2.51.0	Integer
pppoeACNameStatus.0	.1.3.6.1.4.1.161.19.3.2.2.52.0	OctetString
pppoeSvcNameStatus.0	.1.3.6.1.4.1.161.19.3.2.2.53.0	OctetString
pppoeSessUptime.0	.1.3.6.1.4.1.161.19.3.2.2.54.0	TimeTicks
minRadioDbm.0	.1.3.6.1.4.1.161.19.3.2.2.58.0	Integer
maxRadioDbm.0	.1.3.6.1.4.1.161.19.3.2.2.59.0	Integer

pppoeSessIdleTime.0	.1.3.6.1.4.1.161.19.3.2.2.60.0	TimeTicks
radioDbmAvg.0	.1.3.6.1.4.1.161.19.3.2.2.61.0	Integer
zoltarFPGAFreqOffset.0	.1.3.6.1.4.1.161.19.3.2.2.62.0	Integer
zoltarSWFreqOffset.0	.1.3.6.1.4.1.161.19.3.2.2.63.0	Integer
airDelayns.0	.1.3.6.1.4.1.161.19.3.2.2.64.0	Gauge
currentColorCode.0	.1.3.6.1.4.1.161.19.3.2.2.65.0	Integer
currentColorCodePri.0	.1.3.6.1.4.1.161.19.3.2.2.66.0	Integer
currentChanFreq.0	.1.3.6.1.4.1.161.19.3.2.2.67.0	Gauge
dhcpServerPktXmt.0	.1.3.6.1.4.1.161.19.3.2.2.72.0	Counter32
dhcpServerPktRcv.0	.1.3.6.1.4.1.161.19.3.2.2.73.0	Counter32
dhcpServerPktToss.0	.1.3.6.1.4.1.161.19.3.2.2.74.0	Counter32
receiveFragmentsModulationPercentage.0	.1.3.6.1.4.1.161.19.3.2.2.86.0	OctetString
signalToNoiseRatioSM.0	.1.3.6.1.4.1.161.19.3.2.2.95.0	Integer
bridgecbUplinkCreditRate.0	.1.3.6.1.4.1.161.19.3.2.2.97.0	Gauge
bridgecbUplinkCreditLimit.0	.1.3.6.1.4.1.161.19.3.2.2.98.0	Gauge
bridgecbDownlinkCreditRate.0	.1.3.6.1.4.1.161.19.3.2.2.99.0	Gauge
bridgecbDownlinkCreditLimit.0	.1.3.6.1.4.1.161.19.3.2.2.100.0	Gauge
mimoQpskBerDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.101.0	OctetString
mimo16QamBerDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.102.0	OctetString
mimo64QamBerDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.103.0	OctetString
mimo256QamBerDisplay.0	.1.3.6.1.4.1.161.19.3.2.2.104.0	OctetString
mimoBerRcvModulationType.0	.1.3.6.1.4.1.161.19.3.2.2.105.0	OctetString
protocol.1	.1.3.6.1.4.1.161.19.3.2.5.1.2.1	Integer
protocol.2	.1.3.6.1.4.1.161.19.3.2.5.1.2.2	Integer
protocol.3	.1.3.6.1.4.1.161.19.3.2.5.1.2.3	Integer
protocol.4	.1.3.6.1.4.1.161.19.3.2.5.1.2.4	Integer
protocol.5	.1.3.6.1.4.1.161.19.3.2.5.1.2.5	Integer
protocol.6	.1.3.6.1.4.1.161.19.3.2.5.1.2.6	Integer
protocol.7	.1.3.6.1.4.1.161.19.3.2.5.1.2.7	Integer

protocol.8	.1.3.6.1.4.1.161.19.3.2.5.1.2.8	Integer
protocol.9	.1.3.6.1.4.1.161.19.3.2.5.1.2.9	Integer
protocol.10	.1.3.6.1.4.1.161.19.3.2.5.1.2.10	Integer
port.1	.1.3.6.1.4.1.161.19.3.2.5.1.3.1	Integer
port.2	.1.3.6.1.4.1.161.19.3.2.5.1.3.2	Integer
port.3	.1.3.6.1.4.1.161.19.3.2.5.1.3.3	Integer
port.4	.1.3.6.1.4.1.161.19.3.2.5.1.3.4	Integer
port.5	.1.3.6.1.4.1.161.19.3.2.5.1.3.5	Integer
port.6	.1.3.6.1.4.1.161.19.3.2.5.1.3.6	Integer
port.7	.1.3.6.1.4.1.161.19.3.2.5.1.3.7	Integer
port.8	.1.3.6.1.4.1.161.19.3.2.5.1.3.8	Integer
port.9	.1.3.6.1.4.1.161.19.3.2.5.1.3.9	Integer
port.10	.1.3.6.1.4.1.161.19.3.2.5.1.3.10	Integer
localIp.1	.1.3.6.1.4.1.161.19.3.2.5.1.4.1	IpAddress
localIp.2	.1.3.6.1.4.1.161.19.3.2.5.1.4.2	IpAddress
localIp.3	.1.3.6.1.4.1.161.19.3.2.5.1.4.3	IpAddress
localIp.4	.1.3.6.1.4.1.161.19.3.2.5.1.4.4	IpAddress
localIp.5	.1.3.6.1.4.1.161.19.3.2.5.1.4.5	IpAddress
localIp.6	.1.3.6.1.4.1.161.19.3.2.5.1.4.6	IpAddress
localIp.7	.1.3.6.1.4.1.161.19.3.2.5.1.4.7	IpAddress
localIp.8	.1.3.6.1.4.1.161.19.3.2.5.1.4.8	IpAddress
localIp.9	.1.3.6.1.4.1.161.19.3.2.5.1.4.9	IpAddress
localIp.10	.1.3.6.1.4.1.161.19.3.2.5.1.4.10	IpAddress
certIndex.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.1.1	Integer
certIndex.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.1.2	Integer
cert.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.2.1	Integer
cert.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.2.2	Integer
action.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.3.1	Integer
action.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.3.2	Integer

certificateDN.1	.1.3.6.1.4.1.161.19.3.2.7.1.1.4.1	OctetString
certificateDN.2	.1.3.6.1.4.1.161.19.3.2.7.1.1.4.2	OctetString
numAuthCerts.0	.1.3.6.1.4.1.161.19.3.2.7.2.0	Integer
authenticationEnforce.0	.1.3.6.1.4.1.161.19.3.2.7.3.0	Integer
phase1.0	.1.3.6.1.4.1.161.19.3.2.7.4.0	Integer
phase2.0	.1.3.6.1.4.1.161.19.3.2.7.5.0	Integer
authOuterId.0	.1.3.6.1.4.1.161.19.3.2.7.6.0	OctetString
authPassword.0	.1.3.6.1.4.1.161.19.3.2.7.7.0	OctetString
authUsername.0	.1.3.6.1.4.1.161.19.3.2.7.8.0	OctetString
useRealm.0	.1.3.6.1.4.1.161.19.3.2.7.9.0	Integer
realm.0	.1.3.6.1.4.1.161.19.3.2.7.10.0	OctetString
whispBoxSoftwareVer.0	.1.3.6.1.4.1.161.19.3.3.1.1.0	OctetString
whispBoxFPGAVer.0	.1.3.6.1.4.1.161.19.3.3.1.2.0	OctetString
whispBoxEsn.0	.1.3.6.1.4.1.161.19.3.3.1.3.0	OctetString
whispBoxBoot.0	.1.3.6.1.4.1.161.19.3.3.1.4.0	OctetString
boxDeviceType.0	.1.3.6.1.4.1.161.19.3.3.1.6.0	OctetString
boxDeviceTypeID.0	.1.3.6.1.4.1.161.19.3.3.1.7.0	OctetString
boxEncryption.0	.1.3.6.1.4.1.161.19.3.3.1.8.0	OctetString
etherLinkStatus.0	.1.3.6.1.4.1.161.19.3.3.1.9.0	OctetString
boxFrequency.0	.1.3.6.1.4.1.161.19.3.3.1.10.0	OctetString
platformVer.0	.1.3.6.1.4.1.161.19.3.3.1.11.0	Integer
platformType.0	.1.3.6.1.4.1.161.19.3.3.1.12.0	OctetString
dhcpLanIp.0	.1.3.6.1.4.1.161.19.3.3.1.13.0	IpAddress
dhcpLanSubnetMask.0	.1.3.6.1.4.1.161.19.3.3.1.14.0	IpAddress
dhcpLanGateway.0	.1.3.6.1.4.1.161.19.3.3.1.15.0	IpAddress
dhcpRfPublicIp.0	.1.3.6.1.4.1.161.19.3.3.1.16.0	IpAddress
dhcpRfPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.3.1.17.0	IpAddress
dhcpRfPublicGateway.0	.1.3.6.1.4.1.161.19.3.3.1.18.0	IpAddress
lanDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.19.0	OctetString
rfPublicDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.20.0	OctetString

inSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.21.0	Integer
outSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.22.0	Integer
pllOutLockCount.0	.1.3.6.1.4.1.161.19.3.3.1.23.0	Integer
txCalFailure.0	.1.3.6.1.4.1.161.19.3.3.1.24.0	Integer
swVersion.0	.1.3.6.1.4.1.161.19.3.3.1.25.0	OctetString
pldVersion.0	.1.3.6.1.4.1.161.19.3.3.1.26.0	OctetString
platformInfo.0	.1.3.6.1.4.1.161.19.3.3.1.27.0	OctetString
packetOverloadCounter.0	.1.3.6.1.4.1.161.19.3.3.1.29.0	Counter32
whispBoxP11Personality.0	.1.3.6.1.4.1.161.19.3.3.1.30.0	OctetString
whispBoxP11FPGAType.0	.1.3.6.1.4.1.161.19.3.3.1.31.0	OctetString
whispBoxP11BstrapFPGAVer.0	.1.3.6.1.4.1.161.19.3.3.1.32.0	OctetString
rxOverrunPkts.0	.1.3.6.1.4.1.161.19.3.3.1.34.0	Counter32
boxTemperatureC.0	.1.3.6.1.4.1.161.19.3.3.1.35.0	Integer
boxTemperatureF.0	.1.3.6.1.4.1.161.19.3.3.1.36.0	Integer
bridgeCbFecStatbin.0	.1.3.6.1.4.1.161.19.3.3.1.37.0	Counter32
bridgeCbFecStatbout.0	.1.3.6.1.4.1.161.19.3.3.1.38.0	Counter32
bridgeCbFecStatbtoss.0	.1.3.6.1.4.1.161.19.3.3.1.39.0	Counter32
bridgeCbFecStatbtosscap.0	.1.3.6.1.4.1.161.19.3.3.1.40.0	Counter32
bridgeCbFecStatuin.0	.1.3.6.1.4.1.161.19.3.3.1.41.0	Counter32
bridgeCbFecStatuout.0	.1.3.6.1.4.1.161.19.3.3.1.42.0	Counter32
bridgeCbFecStatutoss.0	.1.3.6.1.4.1.161.19.3.3.1.43.0	Counter32
bridgeCbFecStatutosscap.0	.1.3.6.1.4.1.161.19.3.3.1.44.0	Counter32
bridgeCbRFStatbin.0	.1.3.6.1.4.1.161.19.3.3.1.45.0	Counter32
bridgeCbRFStatbout.0	.1.3.6.1.4.1.161.19.3.3.1.46.0	Counter32
bridgeCbRFStatbtoss.0	.1.3.6.1.4.1.161.19.3.3.1.47.0	Counter32
bridgeCbRFStatbtosscap.0	.1.3.6.1.4.1.161.19.3.3.1.48.0	Counter32
bridgeCbRFStatuin.0	.1.3.6.1.4.1.161.19.3.3.1.49.0	Counter32
bridgeCbRFStatuout.0	.1.3.6.1.4.1.161.19.3.3.1.50.0	Counter32
bridgeCbRFStatutoss.0	.1.3.6.1.4.1.161.19.3.3.1.51.0	Counter32

bridgeCbRFStatutosscap.0	.1.3.6.1.4.1.161.19.3.3.1.52.0	Counter32
bridgeCbErrStatNI1QSend.0	.1.3.6.1.4.1.161.19.3.3.1.53.0	Counter32
bridgeCbErrStatNI2QSend.0	.1.3.6.1.4.1.161.19.3.3.1.54.0	Counter32
bridgeCbErrStatBridgeFull.0	.1.3.6.1.4.1.161.19.3.3.1.55.0	Counter32
bridgeCbErrStatSendMsg.0	.1.3.6.1.4.1.161.19.3.3.1.56.0	Counter32
bridgeCbErrStatAPFecQSend.0	.1.3.6.1.4.1.161.19.3.3.1.57.0	Counter32
bridgeCbErrStatApRfQSend.0	.1.3.6.1.4.1.161.19.3.3.1.58.0	Counter32
rfStatXmtUDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.59.0	Counter32
rfStatXmtBDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.60.0	Counter32
rfStatRcvUDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.61.0	Counter32
rfStatRcvBDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.62.0	Counter32
rfStatXmtCntlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.63.0	Counter32
rfStatRcvCntlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.64.0	Counter32
rfStatInSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.65.0	Counter32
rfStatOutSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.66.0	Counter32
rfStatOverrunCount.0	.1.3.6.1.4.1.161.19.3.3.1.67.0	Counter32
rfStatUnderrunCount.0	.1.3.6.1.4.1.161.19.3.3.1.68.0	Counter32
rfStatRcvCorruptDataCount.0	.1.3.6.1.4.1.161.19.3.3.1.69.0	Counter32
rfStatBadBcastCtlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.70.0	Counter32
rfStatPLLOutOfLockCnt.0	.1.3.6.1.4.1.161.19.3.3.1.71.0	Counter32
rfStatBeaconVerMismatchCnt.0	.1.3.6.1.4.1.161.19.3.3.1.72.0	Counter32
rfStatBadFreqBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.73.0	Counter32
rfStatnonLiteBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.74.0	Counter32
rfStatUnsupFeatBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.75.0	Counter32
rfStatUnkwnFeatBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.76.0	Counter32
rfStatTxCalFailCnt.0	.1.3.6.1.4.1.161.19.3.3.1.77.0	Counter32
rfStatBadInSyncIDRcv.0	.1.3.6.1.4.1.161.19.3.3.1.78.0	Counter32
rfStatTempOutOfRange.0	.1.3.6.1.4.1.161.19.3.3.1.79.0	Counter32
rfStatRSSIOutOfRange.0	.1.3.6.1.4.1.161.19.3.3.1.80.0	Counter32
rfStatRangeCapEnf.0	.1.3.6.1.4.1.161.19.3.3.1.81.0	Counter32

rfStatRcvLTStart.0	.1.3.6.1.4.1.161.19.3.3.1.82.0	Counter32
rfStatRcvLTStartHS.0	.1.3.6.1.4.1.161.19.3.3.1.83.0	Counter32
rfStatRcvLTResult.0	.1.3.6.1.4.1.161.19.3.3.1.84.0	Counter32
rfStatXmtLTResult.0	.1.3.6.1.4.1.161.19.3.3.1.85.0	Counter32
whispFeatureKeyOrigin.0	.1.3.6.1.4.1.161.19.3.3.1.86.0	OctetString
radioMSN.0	.1.3.6.1.4.1.161.19.3.3.1.87.0	OctetString
updateStatus.0	.1.3.6.1.4.1.161.19.3.3.1.88.0	Integer
syslogStatTxSuccesses.0	.1.3.6.1.4.1.161.19.3.3.1.89.0	Integer
syslogStatDropped.0	.1.3.6.1.4.1.161.19.3.3.1.90.0	Integer
fecStatLinkLost.0	.1.3.6.1.4.1.161.19.3.3.1.91.0	Counter32
fecStatLinkDetected.0	.1.3.6.1.4.1.161.19.3.3.1.92.0	Counter32
natDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.93.0	OctetString
fecInDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.94.0	Gauge
fecInErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.95.0	Gauge
fecOutDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.96.0	Gauge
fecOutErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.97.0	Gauge
rfInDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.98.0	Gauge
rfInErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.99.0	Gauge
rfOutDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.100.0	Gauge
rfOutErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.101.0	Gauge
fecInDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.102.0	Counter32
fecOutDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.103.0	Counter32
rfInDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.104.0	Counter32
rfOutDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.105.0	Counter32
aggregateBandwidthCap.0	.1.3.6.1.4.1.161.19.3.3.1.108.0	Integer
colorCode.0	.1.3.6.1.4.1.161.19.3.3.2.2.0	Integer
fullAccess.0	.1.3.6.1.4.1.161.19.3.3.2.4.0	OctetString
webAutoUpdate.0	.1.3.6.1.4.1.161.19.3.3.2.5.0	Integer
pass1Status.0	.1.3.6.1.4.1.161.19.3.3.2.6.0	OctetString

pass2Status.0	.1.3.6.1.4.1.161.19.3.3.2.7.0	OctetString
bridgeEntryTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.8.0	Integer
snmpMibPerm.0	.1.3.6.1.4.1.161.19.3.3.2.9.0	Integer
antennaGain.0	.1.3.6.1.4.1.161.19.3.3.2.14.0	Integer
dynamicLearning.0	.1.3.6.1.4.1.161.19.3.3.2.16.0	Integer
managementVID.0	.1.3.6.1.4.1.161.19.3.3.2.17.0	Integer
agingTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.18.0	Integer
frameType.0	.1.3.6.1.4.1.161.19.3.3.2.19.0	Integer
addVlanMember.0	.1.3.6.1.4.1.161.19.3.3.2.20.0	Integer
removeVlanMember.0	.1.3.6.1.4.1.161.19.3.3.2.21.0	Integer
scheduling.0	.1.3.6.1.4.1.161.19.3.3.2.22.0	Integer
commStringRWrite.0	.1.3.6.1.4.1.161.19.3.3.2.36.0	OctetString
subnetMask.0	.1.3.6.1.4.1.161.19.3.3.2.37.0	Integer
mngtIP.0	.1.3.6.1.4.1.161.19.3.3.2.38.0	IpAddress
allowVIDAccess.0	.1.3.6.1.4.1.161.19.3.3.2.39.0	Integer
setDefaultPlug.0	.1.3.6.1.4.1.161.19.3.3.2.40.0	Integer
userName.0	.1.3.6.1.4.1.161.19.3.3.2.45.0	OctetString
userPassword.0	.1.3.6.1.4.1.161.19.3.3.2.46.0	OctetString
userAccessLevel.0	.1.3.6.1.4.1.161.19.3.3.2.47.0	Integer
deleteUser.0	.1.3.6.1.4.1.161.19.3.3.2.48.0	OctetString
lanDhcpState.0	.1.3.6.1.4.1.161.19.3.3.2.50.0	Integer
sessionTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.51.0	Integer
vlanMemberSource.0	.1.3.6.1.4.1.161.19.3.3.2.52.0	Integer
changeUsrPwd.0	.1.3.6.1.4.1.161.19.3.3.2.56.0	OctetString
mngtIP2.0	.1.3.6.1.4.1.161.19.3.3.2.57.0	IpAddress
subnetMask2.0	.1.3.6.1.4.1.161.19.3.3.2.58.0	Integer
mngtIP3.0	.1.3.6.1.4.1.161.19.3.3.2.59.0	IpAddress
subnetMask3.0	.1.3.6.1.4.1.161.19.3.3.2.60.0	Integer
mngtIP4.0	.1.3.6.1.4.1.161.19.3.3.2.61.0	IpAddress
subnetMask4.0	.1.3.6.1.4.1.161.19.3.3.2.62.0	Integer

mngtIP5.0	.1.3.6.1.4.1.161.19.3.3.2.63.0	IpAddress
subnetMask5.0	.1.3.6.1.4.1.161.19.3.3.2.64.0	Integer
mngtIP6.0	.1.3.6.1.4.1.161.19.3.3.2.65.0	IpAddress
subnetMask6.0	.1.3.6.1.4.1.161.19.3.3.2.66.0	Integer
mngtIP7.0	.1.3.6.1.4.1.161.19.3.3.2.67.0	IpAddress
subnetMask7.0	.1.3.6.1.4.1.161.19.3.3.2.68.0	Integer
mngtIP8.0	.1.3.6.1.4.1.161.19.3.3.2.69.0	IpAddress
subnetMask8.0	.1.3.6.1.4.1.161.19.3.3.2.70.0	Integer
mngtIP9.0	.1.3.6.1.4.1.161.19.3.3.2.71.0	IpAddress
subnetMask9.0	.1.3.6.1.4.1.161.19.3.3.2.72.0	Integer
mngtIP10.0	.1.3.6.1.4.1.161.19.3.3.2.73.0	IpAddress
subnetMask10.0	.1.3.6.1.4.1.161.19.3.3.2.74.0	Integer
lldpBroadcastEnable.0	.1.3.6.1.4.1.161.19.3.3.2.76.0	Integer
regionCode.0	.1.3.6.1.4.1.161.19.3.3.2.77.0	Integer
commStringROnly.0	.1.3.6.1.4.1.161.19.3.3.2.79.0	OctetString
ethernetLinkSpeed.0	.1.3.6.1.4.1.161.19.3.3.2.80.0	Integer
cyclicPrefix.0	.1.3.6.1.4.1.161.19.3.3.2.81.0	Integer
channelBandwidth.0	.1.3.6.1.4.1.161.19.3.3.2.83.0	OctetString
setDefaults.0	.1.3.6.1.4.1.161.19.3.3.2.84.0	Integer
siteInfoViewable.0	.1.3.6.1.4.1.161.19.3.3.2.86.0	Integer
largeVCQ.0	.1.3.6.1.4.1.161.19.3.3.2.87.0	Integer
latitude.0	.1.3.6.1.4.1.161.19.3.3.2.88.0	OctetString
longitude.0	.1.3.6.1.4.1.161.19.3.3.2.89.0	OctetString
height.0	.1.3.6.1.4.1.161.19.3.3.2.90.0	Integer
bandwidth.0	.1.3.6.1.4.1.161.19.3.3.2.91.0	Integer
providerVID.0	.1.3.6.1.4.1.161.19.3.3.2.95.0	Integer
mac1VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.96.0	OctetString
mac1VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.97.0	Integer
mac2VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.98.0	OctetString

mac2VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.99.0	Integer
mac3VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.100.0	OctetString
mac3VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.101.0	Integer
mac4VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.102.0	OctetString
mac4VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.103.0	Integer
mac5VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.104.0	OctetString
mac5VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.105.0	Integer
mac6VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.106.0	OctetString
mac6VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.107.0	Integer
mac7VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.108.0	OctetString
mac7VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.109.0	Integer
mac8VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.110.0	OctetString
mac8VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.111.0	Integer
mac9VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.112.0	OctetString
mac9VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.113.0	Integer
mac10VIDMapAddr.0	.1.3.6.1.4.1.161.19.3.3.2.114.0	OctetString
mac10VIDMapVid.0	.1.3.6.1.4.1.161.19.3.3.2.115.0	Integer
vlanPortType.0	.1.3.6.1.4.1.161.19.3.3.2.116.0	Integer
vlanAcceptQinQFrames.0	.1.3.6.1.4.1.161.19.3.3.2.117.0	Integer
whispWebUserAccessMode.0	.1.3.6.1.4.1.161.19.3.3.2.118.0	Integer
usrAccountEnableAccounting.0	.1.3.6.1.4.1.161.19.3.3.2.119.0	Integer
allowRejectThenLocal.0	.1.3.6.1.4.1.161.19.3.3.2.120.0	Integer
snrCalculation.0	.1.3.6.1.4.1.161.19.3.3.2.121.0	Integer
priorityPrecedence.0	.1.3.6.1.4.1.161.19.3.3.2.122.0	Integer
installationColorCode.0	.1.3.6.1.4.1.161.19.3.3.2.123.0	Integer
pppoeFilter.0	.1.3.6.1.4.1.161.19.3.2.1.33.0	Integer
smbFilter.0	.1.3.6.1.4.1.161.19.3.2.1.34.0	Integer
snmpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.35.0	Integer
userP1Filter.0	.1.3.6.1.4.1.161.19.3.2.1.36.0	Integer
userP2Filter.0	.1.3.6.1.4.1.161.19.3.2.1.37.0	Integer

userP3Filter.0	.1.3.6.1.4.1.161.19.3.2.1.38.0	Integer
allOtherIpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.39.0	Integer
allIpv4Filter.0	.1.3.6.1.4.1.161.19.3.2.1.116.0	Integer
arpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.41.0	Integer
allOthersFilter.0	.1.3.6.1.4.1.161.19.3.2.1.42.0	Integer
userDefinedPort1.0	.1.3.6.1.4.1.161.19.3.2.1.43.0	Integer
port1TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.44.0	Integer
port1UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.45.0	Integer
userDefinedPort2.0	.1.3.6.1.4.1.161.19.3.2.1.46.0	Integer
port2TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.47.0	Integer
port2UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.48.0	Integer
userDefinedPort3.0	.1.3.6.1.4.1.161.19.3.2.1.49.0	Integer
port3TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.50.0	Integer
port3UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.51.0	Integer
bootpcFilter.0	.1.3.6.1.4.1.161.19.3.2.1.52.0	Integer
bootpsFilter.0	.1.3.6.1.4.1.161.19.3.2.1.53.0	Integer
ip4MultFilter.0	.1.3.6.1.4.1.161.19.3.2.1.54.0	Integer
packetFilterDirection.0	.1.3.6.1.4.1.161.19.3.2.1.96.0	Integer
pppoeCtlPriority.0	.1.3.6.1.4.1.161.19.3.3.2.149.0	Integer
ftpPort.0	.1.3.6.1.4.1.161.19.3.3.2.150.0	Integer
httpPort.0	.1.3.6.1.4.1.161.19.3.3.2.151.0	Integer
snmpPort.0	.1.3.6.1.4.1.161.19.3.3.2.153.0	Integer
snmpTrapPort.0	.1.3.6.1.4.1.161.19.3.3.2.154.0	Integer
lan1DhcpRelease.0	.1.3.6.1.4.1.161.19.3.3.2.201.0	Integer
lan1DhcpRenew.0	.1.3.6.1.4.1.161.19.3.3.2.202.0	Integer
lan3DhcpRelease.0	.1.3.6.1.4.1.161.19.3.3.2.203.0	Integer
lan3DhcpRenew.0	.1.3.6.1.4.1.161.19.3.3.2.204.0	Integer
natDhcpRelease.0	.1.3.6.1.4.1.161.19.3.3.2.205.0	Integer
natDhcpRenew.0	.1.3.6.1.4.1.161.19.3.3.2.206.0	Integer

reboot.0	.1.3.6.1.4.1.161.19.3.3.3.2.0	Integer
clearEventLog.0	.1.3.6.1.4.1.161.19.3.3.3.3.0	Integer
rebootIfRequired.0	.1.3.6.1.4.1.161.19.3.3.3.4.0	Integer
clearBERStats.0	.1.3.6.1.4.1.161.19.3.3.3.5.0	Integer
updateDevice.0	.1.3.6.1.4.1.161.19.3.3.3.6.0	Integer
whispBridgeMacAddr.1	.1.3.6.1.4.1.161.19.3.3.4.1.1.1	OctetString
whispBridgeMacAddr.2	.1.3.6.1.4.1.161.19.3.3.4.1.1.2	OctetString
whispBridgeDesLuid.1	.1.3.6.1.4.1.161.19.3.3.4.1.2.1	Integer
whispBridgeDesLuid.2	.1.3.6.1.4.1.161.19.3.3.4.1.2.2	Integer
whispBridgeAge.1	.1.3.6.1.4.1.161.19.3.3.4.1.3.1	Integer
whispBridgeAge.2	.1.3.6.1.4.1.161.19.3.3.4.1.3.2	Integer
whispBridgeExt.1	.1.3.6.1.4.1.161.19.3.3.4.1.4.1	Integer
whispBridgeExt.2	.1.3.6.1.4.1.161.19.3.3.4.1.4.2	Integer
whispBridgeHash.1	.1.3.6.1.4.1.161.19.3.3.4.1.5.1	Integer
whispBridgeHash.2	.1.3.6.1.4.1.161.19.3.3.4.1.5.2	Integer
whispBoxEvntLog.0	.1.3.6.1.4.1.161.19.3.3.5.1.0	OctetString
whispBridgeTbUsed.0	.1.3.6.1.4.1.161.19.3.3.7.1.0	Integer
whispBridgeTbFree.0	.1.3.6.1.4.1.161.19.3.3.7.2.0	Integer
whispBridgeTbErr.0	.1.3.6.1.4.1.161.19.3.3.7.3.0	Integer
codePoint0.0	.1.3.6.1.4.1.161.19.3.3.9.1.0	Integer
codePoint1.0	.1.3.6.1.4.1.161.19.3.3.9.2.0	Integer
codePoint2.0	.1.3.6.1.4.1.161.19.3.3.9.3.0	Integer
codePoint3.0	.1.3.6.1.4.1.161.19.3.3.9.4.0	Integer
codePoint4.0	.1.3.6.1.4.1.161.19.3.3.9.5.0	Integer
codePoint5.0	.1.3.6.1.4.1.161.19.3.3.9.6.0	Integer
codePoint6.0	.1.3.6.1.4.1.161.19.3.3.9.7.0	Integer
codePoint7.0	.1.3.6.1.4.1.161.19.3.3.9.8.0	Integer
codePoint8.0	.1.3.6.1.4.1.161.19.3.3.9.9.0	Integer
codePoint9.0	.1.3.6.1.4.1.161.19.3.3.9.10.0	Integer
codePoint10.0	.1.3.6.1.4.1.161.19.3.3.9.11.0	Integer

codePoint11.0	.1.3.6.1.4.1.161.19.3.3.9.12.0	Integer
codePoint12.0	.1.3.6.1.4.1.161.19.3.3.9.13.0	Integer
codePoint13.0	.1.3.6.1.4.1.161.19.3.3.9.14.0	Integer
codePoint14.0	.1.3.6.1.4.1.161.19.3.3.9.15.0	Integer
codePoint15.0	.1.3.6.1.4.1.161.19.3.3.9.16.0	Integer
codePoint16.0	.1.3.6.1.4.1.161.19.3.3.9.17.0	Integer
codePoint17.0	.1.3.6.1.4.1.161.19.3.3.9.18.0	Integer
codePoint18.0	.1.3.6.1.4.1.161.19.3.3.9.19.0	Integer
codePoint19.0	.1.3.6.1.4.1.161.19.3.3.9.20.0	Integer
codePoint20.0	.1.3.6.1.4.1.161.19.3.3.9.21.0	Integer
codePoint21.0	.1.3.6.1.4.1.161.19.3.3.9.22.0	Integer
codePoint22.0	.1.3.6.1.4.1.161.19.3.3.9.23.0	Integer
codePoint23.0	.1.3.6.1.4.1.161.19.3.3.9.24.0	Integer
codePoint24.0	.1.3.6.1.4.1.161.19.3.3.9.25.0	Integer
codePoint25.0	.1.3.6.1.4.1.161.19.3.3.9.26.0	Integer
codePoint26.0	.1.3.6.1.4.1.161.19.3.3.9.27.0	Integer
codePoint27.0	.1.3.6.1.4.1.161.19.3.3.9.28.0	Integer
codePoint28.0	.1.3.6.1.4.1.161.19.3.3.9.29.0	Integer
codePoint29.0	.1.3.6.1.4.1.161.19.3.3.9.30.0	Integer
codePoint30.0	.1.3.6.1.4.1.161.19.3.3.9.31.0	Integer
codePoint31.0	.1.3.6.1.4.1.161.19.3.3.9.32.0	Integer
codePoint32.0	.1.3.6.1.4.1.161.19.3.3.9.33.0	Integer
codePoint33.0	.1.3.6.1.4.1.161.19.3.3.9.34.0	Integer
codePoint34.0	.1.3.6.1.4.1.161.19.3.3.9.35.0	Integer
codePoint35.0	.1.3.6.1.4.1.161.19.3.3.9.36.0	Integer
codePoint36.0	.1.3.6.1.4.1.161.19.3.3.9.37.0	Integer
codePoint37.0	.1.3.6.1.4.1.161.19.3.3.9.38.0	Integer
codePoint38.0	.1.3.6.1.4.1.161.19.3.3.9.39.0	Integer
codePoint39.0	.1.3.6.1.4.1.161.19.3.3.9.40.0	Integer

codePoint40.0	.1.3.6.1.4.1.161.19.3.3.9.41.0	Integer
codePoint41.0	.1.3.6.1.4.1.161.19.3.3.9.42.0	Integer
codePoint42.0	.1.3.6.1.4.1.161.19.3.3.9.43.0	Integer
codePoint43.0	.1.3.6.1.4.1.161.19.3.3.9.44.0	Integer
codePoint44.0	.1.3.6.1.4.1.161.19.3.3.9.45.0	Integer
codePoint45.0	.1.3.6.1.4.1.161.19.3.3.9.46.0	Integer
codePoint46.0	.1.3.6.1.4.1.161.19.3.3.9.47.0	Integer
codePoint47.0	.1.3.6.1.4.1.161.19.3.3.9.48.0	Integer
codePoint48.0	.1.3.6.1.4.1.161.19.3.3.9.49.0	Integer
codePoint49.0	.1.3.6.1.4.1.161.19.3.3.9.50.0	Integer
codePoint50.0	.1.3.6.1.4.1.161.19.3.3.9.51.0	Integer
codePoint51.0	.1.3.6.1.4.1.161.19.3.3.9.52.0	Integer
codePoint52.0	.1.3.6.1.4.1.161.19.3.3.9.53.0	Integer
codePoint53.0	.1.3.6.1.4.1.161.19.3.3.9.54.0	Integer
codePoint54.0	.1.3.6.1.4.1.161.19.3.3.9.55.0	Integer
codePoint55.0	.1.3.6.1.4.1.161.19.3.3.9.56.0	Integer
codePoint56.0	.1.3.6.1.4.1.161.19.3.3.9.57.0	Integer
codePoint57.0	.1.3.6.1.4.1.161.19.3.3.9.58.0	Integer
codePoint58.0	.1.3.6.1.4.1.161.19.3.3.9.59.0	Integer
codePoint59.0	.1.3.6.1.4.1.161.19.3.3.9.60.0	Integer
codePoint60.0	.1.3.6.1.4.1.161.19.3.3.9.61.0	Integer
codePoint61.0	.1.3.6.1.4.1.161.19.3.3.9.62.0	Integer
codePoint62.0	.1.3.6.1.4.1.161.19.3.3.9.63.0	Integer
codePoint63.0	.1.3.6.1.4.1.161.19.3.3.9.64.0	Integer
entryIndex.1	.1.3.6.1.4.1.161.19.3.3.10.1.1.1	Integer
entryIndex.2	.1.3.6.1.4.1.161.19.3.3.10.1.1.2	Integer
entryIndex.3	.1.3.6.1.4.1.161.19.3.3.10.1.1.3	Integer
entryIndex.4	.1.3.6.1.4.1.161.19.3.3.10.1.1.4	Integer
userLoginName.1	.1.3.6.1.4.1.161.19.3.3.10.1.2.1	OctetString
userLoginName.2	.1.3.6.1.4.1.161.19.3.3.10.1.2.2	OctetString

userLoginName.3	.1.3.6.1.4.1.161.19.3.3.10.1.2.3	OctetString
userLoginName.4	.1.3.6.1.4.1.161.19.3.3.10.1.2.4	OctetString
userPswd.1	.1.3.6.1.4.1.161.19.3.3.10.1.3.1	OctetString
userPswd.2	.1.3.6.1.4.1.161.19.3.3.10.1.3.2	OctetString
userPswd.3	.1.3.6.1.4.1.161.19.3.3.10.1.3.3	OctetString
userPswd.4	.1.3.6.1.4.1.161.19.3.3.10.1.3.4	OctetString
accessLevel.1	.1.3.6.1.4.1.161.19.3.3.10.1.4.1	Integer
accessLevel.2	.1.3.6.1.4.1.161.19.3.3.10.1.4.2	Integer
accessLevel.3	.1.3.6.1.4.1.161.19.3.3.10.1.4.3	Integer
accessLevel.4	.1.3.6.1.4.1.161.19.3.3.10.1.4.4	Integer
loginStatus.1	.1.3.6.1.4.1.161.19.3.3.10.1.5.1	Integer
loginStatus.2	.1.3.6.1.4.1.161.19.3.3.10.1.5.2	Integer
loginStatus.3	.1.3.6.1.4.1.161.19.3.3.10.1.5.3	Integer
loginStatus.4	.1.3.6.1.4.1.161.19.3.3.10.1.5.4	Integer
loginMethod.1	.1.3.6.1.4.1.161.19.3.3.10.1.6.1	Integer
loginMethod.2	.1.3.6.1.4.1.161.19.3.3.10.1.6.2	Integer
loginMethod.3	.1.3.6.1.4.1.161.19.3.3.10.1.6.3	Integer
loginMethod.4	.1.3.6.1.4.1.161.19.3.3.10.1.6.4	Integer
sessionTime.1	.1.3.6.1.4.1.161.19.3.3.10.1.7.1	Integer
sessionTime.2	.1.3.6.1.4.1.161.19.3.3.10.1.7.2	Integer
sessionTime.3	.1.3.6.1.4.1.161.19.3.3.10.1.7.3	Integer
sessionTime.4	.1.3.6.1.4.1.161.19.3.3.10.1.7.4	Integer
neighborMAC.1	.1.3.6.1.4.1.161.19.3.3.11.1.2.1	OctetString
neighborMAC.2	.1.3.6.1.4.1.161.19.3.3.11.1.2.2	OctetString
neighborMAC.3	.1.3.6.1.4.1.161.19.3.3.11.1.2.3	OctetString
neighborMAC.4	.1.3.6.1.4.1.161.19.3.3.11.1.2.4	OctetString
neighborMAC.5	.1.3.6.1.4.1.161.19.3.3.11.1.2.5	OctetString
neighborMAC.6	.1.3.6.1.4.1.161.19.3.3.11.1.2.6	OctetString
neighborMAC.7	.1.3.6.1.4.1.161.19.3.3.11.1.2.7	OctetString

neighborMAC.8	.1.3.6.1.4.1.161.19.3.3.11.1.2.8	OctetString
neighborMAC.9	.1.3.6.1.4.1.161.19.3.3.11.1.2.9	OctetString
neighborMAC.10	.1.3.6.1.4.1.161.19.3.3.11.1.2.10	OctetString
neighborMAC.11	.1.3.6.1.4.1.161.19.3.3.11.1.2.11	OctetString
neighborMAC.12	.1.3.6.1.4.1.161.19.3.3.11.1.2.12	OctetString
neighborMAC.13	.1.3.6.1.4.1.161.19.3.3.11.1.2.13	OctetString
neighborMAC.14	.1.3.6.1.4.1.161.19.3.3.11.1.2.14	OctetString
neighborMAC.15	.1.3.6.1.4.1.161.19.3.3.11.1.2.15	OctetString
neighborMAC.16	.1.3.6.1.4.1.161.19.3.3.11.1.2.16	OctetString
neighborMAC.17	.1.3.6.1.4.1.161.19.3.3.11.1.2.17	OctetString
neighborMAC.18	.1.3.6.1.4.1.161.19.3.3.11.1.2.18	OctetString
neighborMAC.19	.1.3.6.1.4.1.161.19.3.3.11.1.2.19	OctetString
neighborMAC.20	.1.3.6.1.4.1.161.19.3.3.11.1.2.20	OctetString
neighborIP.1	.1.3.6.1.4.1.161.19.3.3.11.1.3.1	OctetString
neighborIP.2	.1.3.6.1.4.1.161.19.3.3.11.1.3.2	OctetString
neighborIP.3	.1.3.6.1.4.1.161.19.3.3.11.1.3.3	OctetString
neighborIP.4	.1.3.6.1.4.1.161.19.3.3.11.1.3.4	OctetString
neighborIP.5	.1.3.6.1.4.1.161.19.3.3.11.1.3.5	OctetString
neighborIP.6	.1.3.6.1.4.1.161.19.3.3.11.1.3.6	OctetString
neighborIP.7	.1.3.6.1.4.1.161.19.3.3.11.1.3.7	OctetString
neighborIP.8	.1.3.6.1.4.1.161.19.3.3.11.1.3.8	OctetString
neighborIP.9	.1.3.6.1.4.1.161.19.3.3.11.1.3.9	OctetString
neighborIP.10	.1.3.6.1.4.1.161.19.3.3.11.1.3.10	OctetString
neighborIP.11	.1.3.6.1.4.1.161.19.3.3.11.1.3.11	OctetString
neighborIP.12	.1.3.6.1.4.1.161.19.3.3.11.1.3.12	OctetString
neighborIP.13	.1.3.6.1.4.1.161.19.3.3.11.1.3.13	OctetString
neighborIP.14	.1.3.6.1.4.1.161.19.3.3.11.1.3.14	OctetString
neighborIP.15	.1.3.6.1.4.1.161.19.3.3.11.1.3.15	OctetString
neighborIP.16	.1.3.6.1.4.1.161.19.3.3.11.1.3.16	OctetString
neighborIP.17	.1.3.6.1.4.1.161.19.3.3.11.1.3.17	OctetString

neighborIP.18	.1.3.6.1.4.1.161.19.3.3.11.1.3.18	OctetString
neighborIP.19	.1.3.6.1.4.1.161.19.3.3.11.1.3.19	OctetString
neighborIP.20	.1.3.6.1.4.1.161.19.3.3.11.1.3.20	OctetString
neighborSiteName.1	.1.3.6.1.4.1.161.19.3.3.11.1.4.1	OctetString
neighborSiteName.2	.1.3.6.1.4.1.161.19.3.3.11.1.4.2	OctetString
neighborSiteName.3	.1.3.6.1.4.1.161.19.3.3.11.1.4.3	OctetString
neighborSiteName.4	.1.3.6.1.4.1.161.19.3.3.11.1.4.4	OctetString
neighborSiteName.5	.1.3.6.1.4.1.161.19.3.3.11.1.4.5	OctetString
neighborSiteName.6	.1.3.6.1.4.1.161.19.3.3.11.1.4.6	OctetString
neighborSiteName.7	.1.3.6.1.4.1.161.19.3.3.11.1.4.7	OctetString
neighborSiteName.8	.1.3.6.1.4.1.161.19.3.3.11.1.4.8	OctetString
neighborSiteName.9	.1.3.6.1.4.1.161.19.3.3.11.1.4.9	OctetString
neighborSiteName.10	.1.3.6.1.4.1.161.19.3.3.11.1.4.10	OctetString
neighborSiteName.11	.1.3.6.1.4.1.161.19.3.3.11.1.4.11	OctetString
neighborSiteName.12	.1.3.6.1.4.1.161.19.3.3.11.1.4.12	OctetString
neighborSiteName.13	.1.3.6.1.4.1.161.19.3.3.11.1.4.13	OctetString
neighborSiteName.14	.1.3.6.1.4.1.161.19.3.3.11.1.4.14	OctetString
neighborSiteName.15	.1.3.6.1.4.1.161.19.3.3.11.1.4.15	OctetString
neighborSiteName.16	.1.3.6.1.4.1.161.19.3.3.11.1.4.16	OctetString
neighborSiteName.17	.1.3.6.1.4.1.161.19.3.3.11.1.4.17	OctetString
neighborSiteName.18	.1.3.6.1.4.1.161.19.3.3.11.1.4.18	OctetString
neighborSiteName.19	.1.3.6.1.4.1.161.19.3.3.11.1.4.19	OctetString
neighborSiteName.20	.1.3.6.1.4.1.161.19.3.3.11.1.4.20	OctetString
dnsIpState.0	.1.3.6.1.4.1.161.19.3.3.13.1.0	Integer
dnsPrimaryMgmtIP.0	.1.3.6.1.4.1.161.19.3.3.13.2.0	IpAddress
dnsAlternateMgmtIP.0	.1.3.6.1.4.1.161.19.3.3.13.3.0	IpAddress
dnsMgmtDomainName.0	.1.3.6.1.4.1.161.19.3.3.13.4.0	OctetString
trapDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.3.13.5.0	Integer
trap1.0	.1.3.6.1.4.1.161.19.3.3.13.6.0	OctetString

trap2.0	.1.3.6.1.4.1.161.19.3.3.13.7.0	OctetString
trap3.0	.1.3.6.1.4.1.161.19.3.3.13.8.0	OctetString
trap4.0	.1.3.6.1.4.1.161.19.3.3.13.9.0	OctetString
trap5.0	.1.3.6.1.4.1.161.19.3.3.13.10.0	OctetString
trap6.0	.1.3.6.1.4.1.161.19.3.3.13.11.0	OctetString
trap7.0	.1.3.6.1.4.1.161.19.3.3.13.12.0	OctetString
trap8.0	.1.3.6.1.4.1.161.19.3.3.13.13.0	OctetString
trap9.0	.1.3.6.1.4.1.161.19.3.3.13.14.0	OctetString
trap10.0	.1.3.6.1.4.1.161.19.3.3.13.15.0	OctetString
radioIndex.1	.1.3.6.1.4.1.161.19.3.3.15.1.1.1.1	Integer
radioType.1	.1.3.6.1.4.1.161.19.3.3.15.1.1.2.1	Integer
radioPaths.1	.1.3.6.1.4.1.161.19.3.3.15.1.1.3.1	Integer
pathIndex.1.1	.1.3.6.1.4.1.161.19.3.3.15.2.1.1.1.1	Integer
pathIndex.1.2	.1.3.6.1.4.1.161.19.3.3.15.2.1.1.1.2	Integer
frequency.1.5485000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5485000	Integer
frequency.1.5490000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5490000	Integer
frequency.1.5495000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5495000	Integer
frequency.1.5500000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5500000	Integer
frequency.1.5505000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5505000	Integer
frequency.1.5510000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5510000	Integer
frequency.1.5515000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5515000	Integer
frequency.1.5520000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5520000	Integer
frequency.1.5525000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5525000	Integer
frequency.1.5530000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5530000	Integer
frequency.1.5535000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5535000	Integer
frequency.1.5540000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5540000	Integer
frequency.1.5545000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5545000	Integer
frequency.1.5550000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5550000	Integer
frequency.1.5555000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5555000	Integer
frequency.1.5560000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5560000	Integer

frequency.1.5565000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5565000	Integer
frequency.1.5570000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5570000	Integer
frequency.1.5575000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5575000	Integer
frequency.1.5580000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5580000	Integer
frequency.1.5585000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5585000	Integer
frequency.1.5590000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5590000	Integer
frequency.1.5595000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5595000	Integer
frequency.1.5600000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5600000	Integer
frequency.1.5605000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5605000	Integer
frequency.1.5610000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5610000	Integer
frequency.1.5615000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5615000	Integer
frequency.1.5620000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5620000	Integer
frequency.1.5625000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5625000	Integer
frequency.1.5630000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5630000	Integer
frequency.1.5635000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5635000	Integer
frequency.1.5640000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5640000	Integer
frequency.1.5645000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5645000	Integer
frequency.1.5650000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5650000	Integer
frequency.1.5655000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5655000	Integer
frequency.1.5660000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5660000	Integer
frequency.1.5665000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5665000	Integer
frequency.1.5670000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5670000	Integer
frequency.1.5675000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5675000	Integer
frequency.1.5680000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5680000	Integer
frequency.1.5685000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5685000	Integer
frequency.1.5690000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5690000	Integer
frequency.1.5695000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5695000	Integer
frequency.1.5700000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5700000	Integer
frequency.1.5705000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5705000	Integer

frequency.1.5735000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5735000	Integer
frequency.1.5740000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5740000	Integer
frequency.1.5745000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5745000	Integer
frequency.1.5750000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5750000	Integer
frequency.1.5755000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5755000	Integer
frequency.1.5760000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5760000	Integer
frequency.1.5765000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5765000	Integer
frequency.1.5770000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5770000	Integer
frequency.1.5775000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5775000	Integer
frequency.1.5780000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5780000	Integer
frequency.1.5785000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5785000	Integer
frequency.1.5790000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5790000	Integer
frequency.1.5795000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5795000	Integer
frequency.1.5800000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5800000	Integer
frequency.1.5805000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5805000	Integer
frequency.1.5810000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5810000	Integer
frequency.1.5815000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5815000	Integer
frequency.1.5820000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5820000	Integer
frequency.1.5825000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5825000	Integer
frequency.1.5830000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5830000	Integer
frequency.1.5835000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5835000	Integer
frequency.1.5840000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5840000	Integer

AP MIB Objects

The objects that the Canopy Enterprise MIB defines for the AP are listed below:

Table 18 AP MIB Objects

Object Name	OID	Type
rfFreqCarrier.0	.1.3.6.1.4.1.161.19.3.1.1.2.0	Integer
dwnLnkData.0	.1.3.6.1.4.1.161.19.3.1.1.4.0	Integer

upLnkDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.62.0	Integer
upLnkLimit.0	.1.3.6.1.4.1.161.19.3.2.1.63.0	Integer
dwnLnkDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.64.0	Integer
dwnLnkLimit.0	.1.3.6.1.4.1.161.19.3.2.1.65.0	Integer
maxRange.0	.1.3.6.1.4.1.161.19.3.1.1.17.0	Integer
lanIpAp.0	.1.3.6.1.4.1.161.19.3.1.1.23.0	IpAddress
lanMaskAp.0	.1.3.6.1.4.1.161.19.3.1.1.24.0	IpAddress
defaultGwAp.0	.1.3.6.1.4.1.161.19.3.1.1.25.0	IpAddress
privateIp.0	.1.3.6.1.4.1.161.19.3.1.1.26.0	IpAddress
gpsTrap.0	.1.3.6.1.4.1.161.19.3.1.1.27.0	Integer
regTrap.0	.1.3.6.1.4.1.161.19.3.1.1.28.0	Integer
apBeaconInfo.0	.1.3.6.1.4.1.161.19.3.1.1.30.0	Integer
authMode.0	.1.3.6.1.4.1.161.19.3.1.1.31.0	Integer
authKeyAp.0	.1.3.6.1.4.1.161.19.3.1.1.32.0	OctetString
encryptionMode.0	.1.3.6.1.4.1.161.19.3.1.1.33.0	Integer
broadcastRetryCount.0	.1.3.6.1.4.1.161.19.3.1.1.35.0	Integer
updateAppAddress.0	.1.3.6.1.4.1.161.19.3.1.1.37.0	IpAddress
vlanEnable.0	.1.3.6.1.4.1.161.19.3.1.1.39.0	Integer
configSource.0	.1.3.6.1.4.1.161.19.3.1.1.40.0	Integer
numCtlSlotsHW.0	.1.3.6.1.4.1.161.19.3.1.1.42.0	Integer
displayAPEval.0	.1.3.6.1.4.1.161.19.3.1.1.43.0	Integer
smIsolation.0	.1.3.6.1.4.1.161.19.3.1.1.44.0	Integer
ipAccessFilterEnable.0	.1.3.6.1.4.1.161.19.3.2.1.68.0	Integer
allowedIPAccess1.0	.1.3.6.1.4.1.161.19.3.2.1.69.0	IpAddress
allowedIPAccess2.0	.1.3.6.1.4.1.161.19.3.2.1.70.0	IpAddress
allowedIPAccess3.0	.1.3.6.1.4.1.161.19.3.2.1.71.0	IpAddress
tslBridging.0	.1.3.6.1.4.1.161.19.3.1.1.49.0	Integer
untranslatedArp.0	.1.3.6.1.4.1.161.19.3.1.1.50.0	Integer
limitFreqBand900.0	.1.3.6.1.4.1.161.19.3.1.1.51.0	Integer
remoteSpectrumAnalysisDuration.0	.1.3.6.1.4.1.161.19.3.1.1.56.0	Integer

remoteSpectrumAnalyzerLUID.0	.1.3.6.1.4.1.161.19.3.1.1.57.0	Integer
dlnkBcastCIR.0	.1.3.6.1.4.1.161.19.3.1.1.59.0	Integer
verifyGPSChecksum.0	.1.3.6.1.4.1.161.19.3.1.1.60.0	Integer
apVlanOverride.0	.1.3.6.1.4.1.161.19.3.1.1.61.0	Integer
dhcpRelayAgentEnable.0	.1.3.6.1.4.1.161.19.3.1.1.62.0	Integer
colorCodeRescanTimer.0	.1.3.6.1.4.1.161.19.3.1.1.64.0	Integer
colorCodeRescanIdleTimer.0	.1.3.6.1.4.1.161.19.3.1.1.65.0	Integer
authKeyOptionAP.0	.1.3.6.1.4.1.161.19.3.1.1.66.0	Integer
onlyAllowVer95OrAbove.0	.1.3.6.1.4.1.161.19.3.1.1.69.0	Integer
apRxDelay.0	.1.3.6.1.4.1.161.19.3.1.1.70.0	Integer
qinqEthType.0	.1.3.6.1.4.1.161.19.3.1.1.71.0	Integer
authSharedSecret1.0	.1.3.6.1.4.1.161.19.3.1.1.74.0	OctetString
authSharedSecret2.0	.1.3.6.1.4.1.161.19.3.1.1.75.0	OctetString
authSharedSecret3.0	.1.3.6.1.4.1.161.19.3.1.1.76.0	OctetString
whispUsrAuthPhase1.0	.1.3.6.1.4.1.161.19.3.1.1.85.0	Integer
dropSession.0	.1.3.6.1.4.1.161.19.3.1.1.87.0	OctetString
uGPSPower.0	.1.3.6.1.4.1.161.19.3.1.1.88.0	Integer
timeZone.0	.1.3.6.1.4.1.161.19.3.1.1.89.0	Integer
ofdmSMRcvTargetLvl.0	.1.3.6.1.4.1.161.19.3.1.1.90.0	Integer
radiusPort.0	.1.3.6.1.4.1.161.19.3.1.1.91.0	Integer
radiusAcctPort.0	.1.3.6.1.4.1.161.19.3.1.1.92.0	Integer
lastSesStatsReset.0	.1.3.6.1.4.1.161.19.3.1.1.93.0	OctetString
resetSesStats.0	.1.3.6.1.4.1.161.19.3.1.1.94.0	Integer
rfOLTrap.0	.1.3.6.1.4.1.161.19.3.1.1.95.0	Integer
rfOLThreshold.0	.1.3.6.1.4.1.161.19.3.1.1.96.0	Integer
rfOLEnable.0	.1.3.6.1.4.1.161.19.3.1.1.97.0	Integer
actionListFilename.0	.1.3.6.1.4.1.161.19.3.1.1.98.0	OctetString
enableAutoupdate.0	.1.3.6.1.4.1.161.19.3.1.1.99.0	Integer
accountingSmReAuthInterval.0	.1.3.6.1.4.1.161.19.3.1.1.100.0	Integer
syslogDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.1.101.0	Integer
syslogServerAddr.0	.1.3.6.1.4.1.161.19.3.1.1.102.0	OctetString

syslogServerPort.0	.1.3.6.1.4.1.161.19.3.1.1.103.0	Integer
syslogXmitAP.0	.1.3.6.1.4.1.161.19.3.1.1.104.0	Integer
syslogXmitSMs.0	.1.3.6.1.4.1.161.19.3.1.1.105.0	Integer
accountingInterimUpdateInterval.0	.1.3.6.1.4.1.161.19.3.1.1.106.0	Integer
radioMode.0	.1.3.6.1.4.1.161.19.3.1.1.206.0	Integer
rfTelnetAccess.0	.1.3.6.1.4.1.161.19.3.1.1.207.0	Integer
linkTestLUID.0	.1.3.6.1.4.1.161.19.3.1.2.1.1.0	Integer
linkTestDuration.0	.1.3.6.1.4.1.161.19.3.1.2.1.2.0	Integer
linkTestAction.0	.1.3.6.1.4.1.161.19.3.1.2.1.3.0	Integer
linkTestPktLength.0	.1.3.6.1.4.1.161.19.3.1.2.1.4.0	Integer
linkTestMode.0	.1.3.6.1.4.1.161.19.3.1.2.1.5.0	Integer
linkTestSNRCalculation.0	.1.3.6.1.4.1.161.19.3.1.2.1.6.0	Integer
linkTestWithDualPath.0	.1.3.6.1.4.1.161.19.3.1.2.1.7.0	Integer
testLUID.0	.1.3.6.1.4.1.161.19.3.1.2.2.1.0	Integer
linkTestStatus.0	.1.3.6.1.4.1.161.19.3.1.2.2.2.0	OctetString
linkTestError.0	.1.3.6.1.4.1.161.19.3.1.2.2.3.0	OctetString
testDuration.0	.1.3.6.1.4.1.161.19.3.1.2.2.4.0	Integer
downLinkRate.0	.1.3.6.1.4.1.161.19.3.1.2.2.5.0	Integer
upLinkRate.0	.1.3.6.1.4.1.161.19.3.1.2.2.6.0	Integer
downLinkEff.0	.1.3.6.1.4.1.161.19.3.1.2.2.7.0	Integer
maxDwnLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.8.0	Integer
actDwnLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.9.0	Integer
expDwnFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.10.0	Gauge
actDwnFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.11.0	Gauge
upLinkEff.0	.1.3.6.1.4.1.161.19.3.1.2.2.12.0	Integer
expUpFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.13.0	Gauge
actUpFragCount.0	.1.3.6.1.4.1.161.19.3.1.2.2.14.0	Gauge
maxUpLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.15.0	Integer
actUpLinkIndex.0	.1.3.6.1.4.1.161.19.3.1.2.2.16.0	Integer
signalToNoiseRatioDownLink.0	.1.3.6.1.4.1.161.19.3.1.2.2.33.0	Integer

signalToNoiseRatioUpLink.0	.1.3.6.1.4.1.161.19.3.1.2.2.34.0	Integer
whispGPSStats.0	.1.3.6.1.4.1.161.19.3.1.3.1.0	Integer
gpsSyncSource.0	.1.3.6.1.4.1.161.19.3.1.3.2.0	OctetString
gpsSyncStatus.0	.1.3.6.1.4.1.161.19.3.1.3.3.0	OctetString
gpsTrackingMode.0	.1.3.6.1.4.1.161.19.3.1.3.4.0	OctetString
gpsTime.0	.1.3.6.1.4.1.161.19.3.1.3.5.0	OctetString
gpsDate.0	.1.3.6.1.4.1.161.19.3.1.3.6.0	OctetString
gpsSatellitesTracked.0	.1.3.6.1.4.1.161.19.3.1.3.7.0	OctetString
gpsSatellitesVisible.0	.1.3.6.1.4.1.161.19.3.1.3.8.0	OctetString
gpsHeight.0	.1.3.6.1.4.1.161.19.3.1.3.9.0	OctetString
gpsAntennaConnection.0	.1.3.6.1.4.1.161.19.3.1.3.10.0	OctetString
gpsLatitude.0	.1.3.6.1.4.1.161.19.3.1.3.11.0	OctetString
gpsLongitude.0	.1.3.6.1.4.1.161.19.3.1.3.12.0	OctetString
gpsInvalidMsg.0	.1.3.6.1.4.1.161.19.3.1.3.13.0	OctetString
gpsRestartCount.0	.1.3.6.1.4.1.161.19.3.1.3.14.0	Integer
gpsReInitCount.0	.1.3.6.1.4.1.161.19.3.1.3.15.0	Integer
gpsReceiverInfo.0	.1.3.6.1.4.1.161.19.3.1.3.16.0	OctetString
linkLUID.2	.1.3.6.1.4.1.161.19.3.1.4.1.1.2	Integer
linkDescr.2	.1.3.6.1.4.1.161.19.3.1.4.1.2.2	OctetString
linkPhysAddress.2	.1.3.6.1.4.1.161.19.3.1.4.1.3.2	OctetString
linkMtu.2	.1.3.6.1.4.1.161.19.3.1.4.1.4.2	Integer
linkSpeed.2	.1.3.6.1.4.1.161.19.3.1.4.1.5.2	Gauge
linkInOctets.2	.1.3.6.1.4.1.161.19.3.1.4.1.7.2	Counter32
linkInUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.8.2	Counter32
linkInNUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.9.2	Counter32
linkInDiscards.2	.1.3.6.1.4.1.161.19.3.1.4.1.10.2	Counter32
linkInError.2	.1.3.6.1.4.1.161.19.3.1.4.1.11.2	Counter32
linkInUnknownProtos.2	.1.3.6.1.4.1.161.19.3.1.4.1.12.2	Counter32
linkOutOctets.2	.1.3.6.1.4.1.161.19.3.1.4.1.13.2	Counter32
linkOutUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.14.2	Counter32
linkOutNUcastPkts.2	.1.3.6.1.4.1.161.19.3.1.4.1.15.2	Counter32

linkOutDiscards.2	.1.3.6.1.4.1.161.19.3.1.4.1.16.2	Counter32
linkOutError.2	.1.3.6.1.4.1.161.19.3.1.4.1.17.2	Counter32
linkOutQLen.2	.1.3.6.1.4.1.161.19.3.1.4.1.18.2	Gauge
linkSessState.2	.1.3.6.1.4.1.161.19.3.1.4.1.19.2	Integer
linkESN.2	.1.3.6.1.4.1.161.19.3.1.4.1.20.2	OctetString
linkAirDelay.2	.1.3.6.1.4.1.161.19.3.1.4.1.24.2	Integer
linkRegCount.2	.1.3.6.1.4.1.161.19.3.1.4.1.25.2	Integer
linkReRegCount.2	.1.3.6.1.4.1.161.19.3.1.4.1.26.2	Integer
linkTimeOut.2	.1.3.6.1.4.1.161.19.3.1.4.1.27.2	Integer
sessionCount.2	.1.3.6.1.4.1.161.19.3.1.4.1.29.2	Integer
softwareVersion.2	.1.3.6.1.4.1.161.19.3.1.4.1.30.2	OctetString
softwareBootVersion.2	.1.3.6.1.4.1.161.19.3.1.4.1.31.2	OctetString
fpgaVersion.2	.1.3.6.1.4.1.161.19.3.1.4.1.32.2	OctetString
linkSiteName.2	.1.3.6.1.4.1.161.19.3.1.4.1.33.2	OctetString
avgPowerLevel.2	.1.3.6.1.4.1.161.19.3.1.4.1.34.2	OctetString
lastPowerLevel.2	.1.3.6.1.4.1.161.19.3.1.4.1.35.2	OctetString
sesDownLinkRate.2	.1.3.6.1.4.1.161.19.3.1.4.1.36.2	Integer
sesDownLinkLimit.2	.1.3.6.1.4.1.161.19.3.1.4.1.37.2	Integer
sesUpLinkRate.2	.1.3.6.1.4.1.161.19.3.1.4.1.38.2	Integer
sesUpLinkLimit.2	.1.3.6.1.4.1.161.19.3.1.4.1.39.2	Integer
adaptRate.2	.1.3.6.1.4.1.161.19.3.2.2.20.0.2	OctetString
sesLoUpCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.41.2	Integer
sesLoDownCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.42.2	Integer
sesHiUpCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.43.2	Integer
sesHiDownCIR.2	.1.3.6.1.4.1.161.19.3.1.4.1.44.2	Integer
platformVer.2	.1.3.6.1.4.1.161.19.3.3.1.11.0.2	Integer
smSessionTmr.2	.1.3.6.1.4.1.161.19.3.1.4.1.46.2	TimeTicks
smSessionSeqNumMismatch.2	.1.3.6.1.4.1.161.19.3.1.4.1.47.2	Counter32
dataVCNum.2	.1.3.6.1.4.1.161.19.3.1.4.1.48.2	Integer
hiPriQEn.2	.1.3.6.1.4.1.161.19.3.1.4.1.49.2	Integer

dataVCNumHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.50.2	Integer
linkInOctetsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.51.2	Counter32
linkInUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.52.2	Counter32
linkInNUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.53.2	Counter32
linkInDiscardsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.54.2	Counter32
linkInErrorHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.55.2	Counter32
linkInUnknownProtosHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.56.2	Counter32
linkOutOctetsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.57.2	Counter32
linkOutUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.58.2	Counter32
linkOutNUcastPktsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.59.2	Counter32
linkOutDiscardsHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.60.2	Counter32
linkOutErrorHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.61.2	Counter32
vcQOverflow.2	.1.3.6.1.4.1.161.19.3.1.4.1.62.2	Counter32
vcQOverflowHiQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.63.2	Counter32
p7p8HiPriQEn.2	.1.3.6.1.4.1.161.19.3.1.4.1.64.2	Integer
p7p8HiPriQ.2	.1.3.6.1.4.1.161.19.3.1.4.1.65.2	Counter32
linkAirDelayns.2	.1.3.6.1.4.1.161.19.3.1.4.1.66.2	Integer
linkManagementIP.2	.1.3.6.1.4.1.161.19.3.1.4.1.69.2	IpAddress
signalToNoiseRatio.2	.1.3.6.1.4.1.161.19.3.1.4.1.74.2	Integer
radiusReplyMsg.2	.1.3.6.1.4.1.161.19.3.1.4.1.75.2	OctetString
autoUpdateStatus.2	.1.3.6.1.4.1.161.19.3.1.4.1.76.2	Integer
radiusFramedIPAddress.2	.1.3.6.1.4.1.161.19.3.1.4.1.77.2	IpAddress
radiusFramedIPNetmask.2	.1.3.6.1.4.1.161.19.3.1.4.1.78.2	IpAddress
radiusDefaultGateway.2	.1.3.6.1.4.1.161.19.3.1.4.1.79.2	IpAddress
regCount.0	.1.3.6.1.4.1.161.19.3.1.7.1.0	Gauge
gpsStatus.0	.1.3.6.1.4.1.161.19.3.1.7.2.0	OctetString
dataSlotDwn.0	.1.3.6.1.4.1.161.19.3.1.7.5.0	Integer
dataSlotUp.0	.1.3.6.1.4.1.161.19.3.1.7.6.0	Integer
numCtrSlot.0	.1.3.6.1.4.1.161.19.3.1.7.12.0	Gauge
maxRegSMCount.0	.1.3.6.1.4.1.161.19.3.1.7.18.0	Integer
systemTime.0	.1.3.6.1.4.1.161.19.3.1.7.19.0	OctetString

lastNTPTime.0	.1.3.6.1.4.1.161.19.3.1.7.20.0	OctetString
regulatoryStatus.0	.1.3.6.1.4.1.161.19.3.1.7.21.0	OctetString
dhcpRlyAgntStat-reqRecvd.0	.1.3.6.1.4.1.161.19.3.1.7.22.0	Counter32
dhcpRlyAgntStat-reqRelayed.0	.1.3.6.1.4.1.161.19.3.1.7.23.0	Counter32
dhcpRlyAgntStat-reqDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.24.0	Counter32
dhcpRlyAgntStat-respRecvd.0	.1.3.6.1.4.1.161.19.3.1.7.25.0	Counter32
dhcpRlyAgntStat-respRelayed.0	.1.3.6.1.4.1.161.19.3.1.7.26.0	Counter32
dhcpRlyAgntStat-respDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.27.0	Counter32
dhcpRlyAgntStat-untrustedDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.28.0	Counter32
dhcpRlyAgntStat-maxHopDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.29.0	Counter32
dhcpRlyAgntStat-pktTooBig.0	.1.3.6.1.4.1.161.19.3.1.7.30.0	Counter32
dhcpRlyAgntStat-invalidGiaddrDiscards.0	.1.3.6.1.4.1.161.19.3.1.7.31.0	Counter32
regFailureCount.0	.1.3.6.1.4.1.161.19.3.1.7.32.0	Counter32
ntpLogSNMP.0	.1.3.6.1.4.1.161.19.3.1.7.33.0	OctetString
uGPSPowerStatus.0	.1.3.6.1.4.1.161.19.3.1.7.34.0	OctetString
autoUpdateGlobalStatus.0	.1.3.6.1.4.1.161.19.3.1.7.36.0	Integer
ntpDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.1.0	Integer
ntpServer1.0	.1.3.6.1.4.1.161.19.3.1.9.2.0	OctetString
ntpServer2.0	.1.3.6.1.4.1.161.19.3.1.9.3.0	OctetString
ntpServer3.0	.1.3.6.1.4.1.161.19.3.1.9.4.0	OctetString
dhcprDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.5.0	Integer
dhcprServer.0	.1.3.6.1.4.1.161.19.3.1.9.6.0	OctetString
authDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.1.9.7.0	Integer
authServer1.0	.1.3.6.1.4.1.161.19.3.1.9.8.0	OctetString
authServer2.0	.1.3.6.1.4.1.161.19.3.1.9.9.0	OctetString
authServer3.0	.1.3.6.1.4.1.161.19.3.1.9.10.0	OctetString
authServer4.0	.1.3.6.1.4.1.161.19.3.1.9.11.0	OctetString
authServer5.0	.1.3.6.1.4.1.161.19.3.1.9.12.0	OctetString

radioFreqCarrier.1	.1.3.6.1.4.1.161.19.3.1.10.1.1.1.1	Integer
radioDownlinkPercent.1	.1.3.6.1.4.1.161.19.3.1.10.1.1.2.1	Integer
radioMaxRange.1	.1.3.6.1.4.1.161.19.3.1.10.1.1.3.1	Integer
radioControlSlots.1	.1.3.6.1.4.1.161.19.3.1.10.1.1.4.1	Integer
radioTransmitOutputPower.1	.1.3.6.1.4.1.161.19.3.1.10.1.1.5.1	Integer
radioColorCode.1	.1.3.6.1.4.1.161.19.3.1.10.1.1.6.1	Integer
protocol.1	.1.3.6.1.4.1.161.19.3.2.5.1.2.1	Integer
protocol.2	.1.3.6.1.4.1.161.19.3.2.5.1.2.2	Integer
protocol.3	.1.3.6.1.4.1.161.19.3.2.5.1.2.3	Integer
protocol.4	.1.3.6.1.4.1.161.19.3.2.5.1.2.4	Integer
protocol.5	.1.3.6.1.4.1.161.19.3.2.5.1.2.5	Integer
protocol.6	.1.3.6.1.4.1.161.19.3.2.5.1.2.6	Integer
protocol.7	.1.3.6.1.4.1.161.19.3.2.5.1.2.7	Integer
protocol.8	.1.3.6.1.4.1.161.19.3.2.5.1.2.8	Integer
protocol.9	.1.3.6.1.4.1.161.19.3.2.5.1.2.9	Integer
protocol.10	.1.3.6.1.4.1.161.19.3.2.5.1.2.10	Integer
port.1	.1.3.6.1.4.1.161.19.3.2.5.1.3.1	Integer
port.2	.1.3.6.1.4.1.161.19.3.2.5.1.3.2	Integer
port.3	.1.3.6.1.4.1.161.19.3.2.5.1.3.3	Integer
port.4	.1.3.6.1.4.1.161.19.3.2.5.1.3.4	Integer
port.5	.1.3.6.1.4.1.161.19.3.2.5.1.3.5	Integer
port.6	.1.3.6.1.4.1.161.19.3.2.5.1.3.6	Integer
port.7	.1.3.6.1.4.1.161.19.3.2.5.1.3.7	Integer
port.8	.1.3.6.1.4.1.161.19.3.2.5.1.3.8	Integer
port.9	.1.3.6.1.4.1.161.19.3.2.5.1.3.9	Integer
port.10	.1.3.6.1.4.1.161.19.3.2.5.1.3.10	Integer
localIp.1	.1.3.6.1.4.1.161.19.3.2.5.1.4.1	IpAddress
localIp.2	.1.3.6.1.4.1.161.19.3.2.5.1.4.2	IpAddress
localIp.3	.1.3.6.1.4.1.161.19.3.2.5.1.4.3	IpAddress
localIp.4	.1.3.6.1.4.1.161.19.3.2.5.1.4.4	IpAddress
localIp.5	.1.3.6.1.4.1.161.19.3.2.5.1.4.5	IpAddress

localIp.6	.1.3.6.1.4.1.161.19.3.2.5.1.4.6	IpAddress
localIp.7	.1.3.6.1.4.1.161.19.3.2.5.1.4.7	IpAddress
localIp.8	.1.3.6.1.4.1.161.19.3.2.5.1.4.8	IpAddress
localIp.9	.1.3.6.1.4.1.161.19.3.2.5.1.4.9	IpAddress
localIp.10	.1.3.6.1.4.1.161.19.3.2.5.1.4.10	IpAddress
whispBoxSoftwareVer.0	.1.3.6.1.4.1.161.19.3.3.1.1.0	OctetString
whispBoxFPGAVer.0	.1.3.6.1.4.1.161.19.3.3.1.2.0	OctetString
whispBoxEsn.0	.1.3.6.1.4.1.161.19.3.3.1.3.0	OctetString
whispBoxBoot.0	.1.3.6.1.4.1.161.19.3.3.1.4.0	OctetString
boxDeviceType.0	.1.3.6.1.4.1.161.19.3.3.1.6.0	OctetString
boxDeviceTypeID.0	.1.3.6.1.4.1.161.19.3.3.1.7.0	OctetString
boxEncryption.0	.1.3.6.1.4.1.161.19.3.3.1.8.0	OctetString
etherLinkStatus.0	.1.3.6.1.4.1.161.19.3.3.1.9.0	OctetString
boxFrequency.0	.1.3.6.1.4.1.161.19.3.3.1.10.0	OctetString
platformVer.0	.1.3.6.1.4.1.161.19.3.3.1.11.0	Integer
platformType.0	.1.3.6.1.4.1.161.19.3.3.1.12.0	OctetString
dhcpLanIp.0	.1.3.6.1.4.1.161.19.3.3.1.13.0	IpAddress
dhcpLanSubnetMask.0	.1.3.6.1.4.1.161.19.3.3.1.14.0	IpAddress
dhcpLanGateway.0	.1.3.6.1.4.1.161.19.3.3.1.15.0	IpAddress
dhcpRfPublicIp.0	.1.3.6.1.4.1.161.19.3.3.1.16.0	IpAddress
dhcpRfPublicSubnetMask.0	.1.3.6.1.4.1.161.19.3.3.1.17.0	IpAddress
dhcpRfPublicGateway.0	.1.3.6.1.4.1.161.19.3.3.1.18.0	IpAddress
lanDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.19.0	OctetString
rfPublicDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.20.0	OctetString
inSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.21.0	Integer
outSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.22.0	Integer
pllOutLockCount.0	.1.3.6.1.4.1.161.19.3.3.1.23.0	Integer
txCalFailure.0	.1.3.6.1.4.1.161.19.3.3.1.24.0	Integer
swVersion.0	.1.3.6.1.4.1.161.19.3.3.1.25.0	OctetString
pldVersion.0	.1.3.6.1.4.1.161.19.3.3.1.26.0	OctetString

platformInfo.0	.1.3.6.1.4.1.161.19.3.3.1.27.0	OctetString
packetOverloadCounter.0	.1.3.6.1.4.1.161.19.3.3.1.29.0	Counter32
whispBoxP11Personality.0	.1.3.6.1.4.1.161.19.3.3.1.30.0	OctetString
whispBoxP11FPGAType.0	.1.3.6.1.4.1.161.19.3.3.1.31.0	OctetString
whispBoxP11BstrapFPGAVer.0	.1.3.6.1.4.1.161.19.3.3.1.32.0	OctetString
rxOverrunPkts.0	.1.3.6.1.4.1.161.19.3.3.1.34.0	Counter32
boxTemperatureC.0	.1.3.6.1.4.1.161.19.3.3.1.35.0	Integer
boxTemperatureF.0	.1.3.6.1.4.1.161.19.3.3.1.36.0	Integer
bridgeCbFecStatbin.0	.1.3.6.1.4.1.161.19.3.3.1.37.0	Counter32
bridgeCbFecStatbout.0	.1.3.6.1.4.1.161.19.3.3.1.38.0	Counter32
bridgeCbFecStatbtoss.0	.1.3.6.1.4.1.161.19.3.3.1.39.0	Counter32
bridgeCbFecStatbtosscap.0	.1.3.6.1.4.1.161.19.3.3.1.40.0	Counter32
bridgeCbFecStatuin.0	.1.3.6.1.4.1.161.19.3.3.1.41.0	Counter32
bridgeCbFecStatuout.0	.1.3.6.1.4.1.161.19.3.3.1.42.0	Counter32
bridgeCbFecStatutoss.0	.1.3.6.1.4.1.161.19.3.3.1.43.0	Counter32
bridgeCbFecStatutosscap.0	.1.3.6.1.4.1.161.19.3.3.1.44.0	Counter32
bridgeCbRFStatbin.0	.1.3.6.1.4.1.161.19.3.3.1.45.0	Counter32
bridgeCbRFStatbout.0	.1.3.6.1.4.1.161.19.3.3.1.46.0	Counter32
bridgeCbRFStatbtoss.0	.1.3.6.1.4.1.161.19.3.3.1.47.0	Counter32
bridgeCbRFStatbtosscap.0	.1.3.6.1.4.1.161.19.3.3.1.48.0	Counter32
bridgeCbRFStatuin.0	.1.3.6.1.4.1.161.19.3.3.1.49.0	Counter32
bridgeCbRFStatuout.0	.1.3.6.1.4.1.161.19.3.3.1.50.0	Counter32
bridgeCbRFStatutoss.0	.1.3.6.1.4.1.161.19.3.3.1.51.0	Counter32
bridgeCbRFStatutosscap.0	.1.3.6.1.4.1.161.19.3.3.1.52.0	Counter32
bridgeCbErrStatNI1QSend.0	.1.3.6.1.4.1.161.19.3.3.1.53.0	Counter32
bridgeCbErrStatNI2QSend.0	.1.3.6.1.4.1.161.19.3.3.1.54.0	Counter32
bridgeCbErrStatBridgeFull.0	.1.3.6.1.4.1.161.19.3.3.1.55.0	Counter32
bridgeCbErrStatSendMsg.0	.1.3.6.1.4.1.161.19.3.3.1.56.0	Counter32
bridgeCbErrStatAPFecQSend.0	.1.3.6.1.4.1.161.19.3.3.1.57.0	Counter32
bridgeCbErrStatApRfQSend.0	.1.3.6.1.4.1.161.19.3.3.1.58.0	Counter32
rfStatXmtUDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.59.0	Counter32

rfStatXmtBDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.60.0	Counter32
rfStatRcvUDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.61.0	Counter32
rfStatRcvBDataCnt.0	.1.3.6.1.4.1.161.19.3.3.1.62.0	Counter32
rfStatXmtCntlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.63.0	Counter32
rfStatRcvCntlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.64.0	Counter32
rfStatInSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.65.0	Counter32
rfStatOutSyncCount.0	.1.3.6.1.4.1.161.19.3.3.1.66.0	Counter32
rfStatOverrunCount.0	.1.3.6.1.4.1.161.19.3.3.1.67.0	Counter32
rfStatUnderrunCount.0	.1.3.6.1.4.1.161.19.3.3.1.68.0	Counter32
rfStatRcvCorruptDataCount.0	.1.3.6.1.4.1.161.19.3.3.1.69.0	Counter32
rfStatBadBcastCtlCnt.0	.1.3.6.1.4.1.161.19.3.3.1.70.0	Counter32
rfStatPLLOutOfLockCnt.0	.1.3.6.1.4.1.161.19.3.3.1.71.0	Counter32
rfStatBeaconVerMismatchCnt.0	.1.3.6.1.4.1.161.19.3.3.1.72.0	Counter32
rfStatBadFreqBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.73.0	Counter32
rfStatnonLiteBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.74.0	Counter32
rfStatUnsupFeatBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.75.0	Counter32
rfStatUnkwnFeatBcnRcvCnt.0	.1.3.6.1.4.1.161.19.3.3.1.76.0	Counter32
rfStatTxCalFailCnt.0	.1.3.6.1.4.1.161.19.3.3.1.77.0	Counter32
rfStatBadInSyncIDRcv.0	.1.3.6.1.4.1.161.19.3.3.1.78.0	Counter32
rfStatTempOutOfRange.0	.1.3.6.1.4.1.161.19.3.3.1.79.0	Counter32
rfStatRSSIOutOfRange.0	.1.3.6.1.4.1.161.19.3.3.1.80.0	Counter32
rfStatRangeCapEnf.0	.1.3.6.1.4.1.161.19.3.3.1.81.0	Counter32
rfStatRcvLTStart.0	.1.3.6.1.4.1.161.19.3.3.1.82.0	Counter32
rfStatRcvLTStartHS.0	.1.3.6.1.4.1.161.19.3.3.1.83.0	Counter32
rfStatRcvLTResult.0	.1.3.6.1.4.1.161.19.3.3.1.84.0	Counter32
rfStatXmtLTResult.0	.1.3.6.1.4.1.161.19.3.3.1.85.0	Counter32
whispFeatureKeyOrigin.0	.1.3.6.1.4.1.161.19.3.3.1.86.0	OctetString
radioMSN.0	.1.3.6.1.4.1.161.19.3.3.1.87.0	OctetString
updateStatus.0	.1.3.6.1.4.1.161.19.3.3.1.88.0	Integer
syslogStatTxSuccesses.0	.1.3.6.1.4.1.161.19.3.3.1.89.0	Integer

syslogStatDropped.0	.1.3.6.1.4.1.161.19.3.3.1.90.0	Integer
fecStatLinkLost.0	.1.3.6.1.4.1.161.19.3.3.1.91.0	Counter32
fecStatLinkDetected.0	.1.3.6.1.4.1.161.19.3.3.1.92.0	Counter32
natDhcpStatus.0	.1.3.6.1.4.1.161.19.3.3.1.93.0	OctetString
fecInDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.94.0	Gauge
fecInErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.95.0	Gauge
fecOutDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.96.0	Gauge
fecOutErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.97.0	Gauge
rfInDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.98.0	Gauge
rfInErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.99.0	Gauge
rfOutDiscardsCount.0	.1.3.6.1.4.1.161.19.3.3.1.100.0	Gauge
rfOutErrorsCount.0	.1.3.6.1.4.1.161.19.3.3.1.101.0	Gauge
fecInDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.102.0	Counter32
fecOutDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.103.0	Counter32
rfInDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.104.0	Counter32
rfOutDiscardsOverloadCount.0	.1.3.6.1.4.1.161.19.3.3.1.105.0	Counter32
aggregateBandwidthCap.0	.1.3.6.1.4.1.161.19.3.3.1.108.0	Integer
colorCode.0	.1.3.6.1.4.1.161.19.3.3.2.2.0	Integer
fullAccess.0	.1.3.6.1.4.1.161.19.3.3.2.4.0	OctetString
webAutoUpdate.0	.1.3.6.1.4.1.161.19.3.3.2.5.0	Integer
pass1Status.0	.1.3.6.1.4.1.161.19.3.3.2.6.0	OctetString
pass2Status.0	.1.3.6.1.4.1.161.19.3.3.2.7.0	OctetString
bridgeEntryTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.8.0	Integer
snmpMibPerm.0	.1.3.6.1.4.1.161.19.3.3.2.9.0	Integer
antennaGain.0	.1.3.6.1.4.1.161.19.3.3.2.14.0	Integer
dynamicLearning.0	.1.3.6.1.4.1.161.19.3.3.2.16.0	Integer
managementVID.0	.1.3.6.1.4.1.161.19.3.3.2.17.0	Integer
agingTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.18.0	Integer
frameType.0	.1.3.6.1.4.1.161.19.3.3.2.19.0	Integer
addVlanMember.0	.1.3.6.1.4.1.161.19.3.3.2.20.0	Integer
removeVlanMember.0	.1.3.6.1.4.1.161.19.3.3.2.21.0	Integer

scheduling.0	.1.3.6.1.4.1.161.19.3.3.2.22.0	Integer
transmitterOP.0	.1.3.6.1.4.1.161.19.3.3.2.23.0	Integer
commStringRWrite.0	.1.3.6.1.4.1.161.19.3.3.2.36.0	OctetString
subnetMask.0	.1.3.6.1.4.1.161.19.3.3.2.37.0	Integer
mngtIP.0	.1.3.6.1.4.1.161.19.3.3.2.38.0	IpAddress
allowVIDAccess.0	.1.3.6.1.4.1.161.19.3.3.2.39.0	Integer
setDefaultPlug.0	.1.3.6.1.4.1.161.19.3.3.2.40.0	Integer
gpsInput.0	.1.3.6.1.4.1.161.19.3.3.2.42.0	Integer
userName.0	.1.3.6.1.4.1.161.19.3.3.2.45.0	OctetString
userPassword.0	.1.3.6.1.4.1.161.19.3.3.2.46.0	OctetString
userAccessLevel.0	.1.3.6.1.4.1.161.19.3.3.2.47.0	Integer
deleteUser.0	.1.3.6.1.4.1.161.19.3.3.2.48.0	OctetString
lanDhcpState.0	.1.3.6.1.4.1.161.19.3.3.2.50.0	Integer
sessionTimeout.0	.1.3.6.1.4.1.161.19.3.3.2.51.0	Integer
vlanMemberSource.0	.1.3.6.1.4.1.161.19.3.3.2.52.0	Integer
changeUsrPwd.0	.1.3.6.1.4.1.161.19.3.3.2.56.0	OctetString
mngtIP2.0	.1.3.6.1.4.1.161.19.3.3.2.57.0	IpAddress
subnetMask2.0	.1.3.6.1.4.1.161.19.3.3.2.58.0	Integer
mngtIP3.0	.1.3.6.1.4.1.161.19.3.3.2.59.0	IpAddress
subnetMask3.0	.1.3.6.1.4.1.161.19.3.3.2.60.0	Integer
mngtIP4.0	.1.3.6.1.4.1.161.19.3.3.2.61.0	IpAddress
subnetMask4.0	.1.3.6.1.4.1.161.19.3.3.2.62.0	Integer
mngtIP5.0	.1.3.6.1.4.1.161.19.3.3.2.63.0	IpAddress
subnetMask5.0	.1.3.6.1.4.1.161.19.3.3.2.64.0	Integer
mngtIP6.0	.1.3.6.1.4.1.161.19.3.3.2.65.0	IpAddress
subnetMask6.0	.1.3.6.1.4.1.161.19.3.3.2.66.0	Integer
mngtIP7.0	.1.3.6.1.4.1.161.19.3.3.2.67.0	IpAddress
subnetMask7.0	.1.3.6.1.4.1.161.19.3.3.2.68.0	Integer
mngtIP8.0	.1.3.6.1.4.1.161.19.3.3.2.69.0	IpAddress
subnetMask8.0	.1.3.6.1.4.1.161.19.3.3.2.70.0	Integer

mngtIP9.0	.1.3.6.1.4.1.161.19.3.3.2.71.0	IpAddress
subnetMask9.0	.1.3.6.1.4.1.161.19.3.3.2.72.0	Integer
mngtIP10.0	.1.3.6.1.4.1.161.19.3.3.2.73.0	IpAddress
subnetMask10.0	.1.3.6.1.4.1.161.19.3.3.2.74.0	Integer
lldpBroadcastEnable.0	.1.3.6.1.4.1.161.19.3.3.2.76.0	Integer
regionCode.0	.1.3.6.1.4.1.161.19.3.3.2.77.0	Integer
commStringROnly.0	.1.3.6.1.4.1.161.19.3.3.2.79.0	OctetString
ethernetLinkSpeed.0	.1.3.6.1.4.1.161.19.3.3.2.80.0	Integer
cyclicPrefix.0	.1.3.6.1.4.1.161.19.3.3.2.81.0	Integer
channelBandwidth.0	.1.3.6.1.4.1.161.19.3.3.2.83.0	OctetString
setDefaults.0	.1.3.6.1.4.1.161.19.3.3.2.84.0	Integer
siteInfoViewable.0	.1.3.6.1.4.1.161.19.3.3.2.86.0	Integer
latitude.0	.1.3.6.1.4.1.161.19.3.3.2.88.0	OctetString
longitude.0	.1.3.6.1.4.1.161.19.3.3.2.89.0	OctetString
height.0	.1.3.6.1.4.1.161.19.3.3.2.90.0	Integer
bandwidth.0	.1.3.6.1.4.1.161.19.3.3.2.91.0	Integer
whispWebUserAccessMode.0	.1.3.6.1.4.1.161.19.3.3.2.118.0	Integer
usrAccountEnableAccounting.0	.1.3.6.1.4.1.161.19.3.3.2.119.0	Integer
allowRejectThenLocal.0	.1.3.6.1.4.1.161.19.3.3.2.120.0	Integer
snrCalculation.0	.1.3.6.1.4.1.161.19.3.3.2.121.0	Integer
priorityPrecedence.0	.1.3.6.1.4.1.161.19.3.3.2.122.0	Integer
installationColorCode.0	.1.3.6.1.4.1.161.19.3.3.2.123.0	Integer
apSmMode.0	.1.3.6.1.4.1.161.19.3.3.2.124.0	Integer
pppoeFilter.0	.1.3.6.1.4.1.161.19.3.2.1.33.0	Integer
smbFilter.0	.1.3.6.1.4.1.161.19.3.2.1.34.0	Integer
snmpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.35.0	Integer
userP1Filter.0	.1.3.6.1.4.1.161.19.3.2.1.36.0	Integer
userP2Filter.0	.1.3.6.1.4.1.161.19.3.2.1.37.0	Integer
userP3Filter.0	.1.3.6.1.4.1.161.19.3.2.1.38.0	Integer
allOtherIpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.39.0	Integer
allIpv4Filter.0	.1.3.6.1.4.1.161.19.3.2.1.116.0	Integer

arpFilter.0	.1.3.6.1.4.1.161.19.3.2.1.41.0	Integer
allOthersFilter.0	.1.3.6.1.4.1.161.19.3.2.1.42.0	Integer
userDefinedPort1.0	.1.3.6.1.4.1.161.19.3.2.1.43.0	Integer
port1TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.44.0	Integer
port1UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.45.0	Integer
userDefinedPort2.0	.1.3.6.1.4.1.161.19.3.2.1.46.0	Integer
port2TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.47.0	Integer
port2UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.48.0	Integer
userDefinedPort3.0	.1.3.6.1.4.1.161.19.3.2.1.49.0	Integer
port3TCPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.50.0	Integer
port3UDPFilter.0	.1.3.6.1.4.1.161.19.3.2.1.51.0	Integer
bootpcFilter.0	.1.3.6.1.4.1.161.19.3.2.1.52.0	Integer
bootpsFilter.0	.1.3.6.1.4.1.161.19.3.2.1.53.0	Integer
ip4MultFilter.0	.1.3.6.1.4.1.161.19.3.2.1.54.0	Integer
packetFilterDirection.0	.1.3.6.1.4.1.161.19.3.2.1.96.0	Integer
pppoeCtlPriority.0	.1.3.6.1.4.1.161.19.3.3.2.149.0	Integer
ftpPort.0	.1.3.6.1.4.1.161.19.3.3.2.150.0	Integer
httpPort.0	.1.3.6.1.4.1.161.19.3.3.2.151.0	Integer
snmpPort.0	.1.3.6.1.4.1.161.19.3.3.2.153.0	Integer
snmpTrapPort.0	.1.3.6.1.4.1.161.19.3.3.2.154.0	Integer
lan1DhcpRelease.0	.1.3.6.1.4.1.161.19.3.3.2.201.0	Integer
lan1DhcpRenew.0	.1.3.6.1.4.1.161.19.3.3.2.202.0	Integer
lan3DhcpRelease.0	.1.3.6.1.4.1.161.19.3.3.2.203.0	Integer
lan3DhcpRenew.0	.1.3.6.1.4.1.161.19.3.3.2.204.0	Integer
natDhcpRelease.0	.1.3.6.1.4.1.161.19.3.3.2.205.0	Integer
natDhcpRenew.0	.1.3.6.1.4.1.161.19.3.3.2.206.0	Integer
reboot.0	.1.3.6.1.4.1.161.19.3.3.3.2.0	Integer
clearEventLog.0	.1.3.6.1.4.1.161.19.3.3.3.3.0	Integer
rebootIfRequired.0	.1.3.6.1.4.1.161.19.3.3.3.4.0	Integer
clearBERStats.0	.1.3.6.1.4.1.161.19.3.3.3.5.0	Integer

updateDevice.0	.1.3.6.1.4.1.161.19.3.3.3.6.0	Integer
whispBridgeMacAddr.1	.1.3.6.1.4.1.161.19.3.3.4.1.1.1	OctetString
whispBridgeMacAddr.2	.1.3.6.1.4.1.161.19.3.3.4.1.1.2	OctetString
whispBridgeMacAddr.3	.1.3.6.1.4.1.161.19.3.3.4.1.1.3	OctetString
whispBridgeDesLuid.1	.1.3.6.1.4.1.161.19.3.3.4.1.2.1	Integer
whispBridgeDesLuid.2	.1.3.6.1.4.1.161.19.3.3.4.1.2.2	Integer
whispBridgeDesLuid.3	.1.3.6.1.4.1.161.19.3.3.4.1.2.3	Integer
whispBridgeAge.1	.1.3.6.1.4.1.161.19.3.3.4.1.3.1	Integer
whispBridgeAge.2	.1.3.6.1.4.1.161.19.3.3.4.1.3.2	Integer
whispBridgeAge.3	.1.3.6.1.4.1.161.19.3.3.4.1.3.3	Integer
whispBridgeExt.1	.1.3.6.1.4.1.161.19.3.3.4.1.4.1	Integer
whispBridgeExt.2	.1.3.6.1.4.1.161.19.3.3.4.1.4.2	Integer
whispBridgeExt.3	.1.3.6.1.4.1.161.19.3.3.4.1.4.3	Integer
whispBridgeHash.1	.1.3.6.1.4.1.161.19.3.3.4.1.5.1	Integer
whispBridgeHash.2	.1.3.6.1.4.1.161.19.3.3.4.1.5.2	Integer
whispBridgeHash.3	.1.3.6.1.4.1.161.19.3.3.4.1.5.3	Integer
whispBoxEvntLog.0	.1.3.6.1.4.1.161.19.3.3.5.1.0	OctetString
whispBridgeTbUsed.0	.1.3.6.1.4.1.161.19.3.3.7.1.0	Integer
whispBridgeTbFree.0	.1.3.6.1.4.1.161.19.3.3.7.2.0	Integer
whispBridgeTbErr.0	.1.3.6.1.4.1.161.19.3.3.7.3.0	Integer
codePoint0.0	.1.3.6.1.4.1.161.19.3.3.9.1.0	Integer
codePoint1.0	.1.3.6.1.4.1.161.19.3.3.9.2.0	Integer
codePoint2.0	.1.3.6.1.4.1.161.19.3.3.9.3.0	Integer
codePoint3.0	.1.3.6.1.4.1.161.19.3.3.9.4.0	Integer
codePoint4.0	.1.3.6.1.4.1.161.19.3.3.9.5.0	Integer
codePoint5.0	.1.3.6.1.4.1.161.19.3.3.9.6.0	Integer
codePoint6.0	.1.3.6.1.4.1.161.19.3.3.9.7.0	Integer
codePoint7.0	.1.3.6.1.4.1.161.19.3.3.9.8.0	Integer
codePoint8.0	.1.3.6.1.4.1.161.19.3.3.9.9.0	Integer
codePoint9.0	.1.3.6.1.4.1.161.19.3.3.9.10.0	Integer
codePoint10.0	.1.3.6.1.4.1.161.19.3.3.9.11.0	Integer

codePoint11.0	.1.3.6.1.4.1.161.19.3.3.9.12.0	Integer
codePoint12.0	.1.3.6.1.4.1.161.19.3.3.9.13.0	Integer
codePoint13.0	.1.3.6.1.4.1.161.19.3.3.9.14.0	Integer
codePoint14.0	.1.3.6.1.4.1.161.19.3.3.9.15.0	Integer
codePoint15.0	.1.3.6.1.4.1.161.19.3.3.9.16.0	Integer
codePoint16.0	.1.3.6.1.4.1.161.19.3.3.9.17.0	Integer
codePoint17.0	.1.3.6.1.4.1.161.19.3.3.9.18.0	Integer
codePoint18.0	.1.3.6.1.4.1.161.19.3.3.9.19.0	Integer
codePoint19.0	.1.3.6.1.4.1.161.19.3.3.9.20.0	Integer
codePoint20.0	.1.3.6.1.4.1.161.19.3.3.9.21.0	Integer
codePoint21.0	.1.3.6.1.4.1.161.19.3.3.9.22.0	Integer
codePoint22.0	.1.3.6.1.4.1.161.19.3.3.9.23.0	Integer
codePoint23.0	.1.3.6.1.4.1.161.19.3.3.9.24.0	Integer
codePoint24.0	.1.3.6.1.4.1.161.19.3.3.9.25.0	Integer
codePoint25.0	.1.3.6.1.4.1.161.19.3.3.9.26.0	Integer
codePoint26.0	.1.3.6.1.4.1.161.19.3.3.9.27.0	Integer
codePoint27.0	.1.3.6.1.4.1.161.19.3.3.9.28.0	Integer
codePoint28.0	.1.3.6.1.4.1.161.19.3.3.9.29.0	Integer
codePoint29.0	.1.3.6.1.4.1.161.19.3.3.9.30.0	Integer
codePoint30.0	.1.3.6.1.4.1.161.19.3.3.9.31.0	Integer
codePoint31.0	.1.3.6.1.4.1.161.19.3.3.9.32.0	Integer
codePoint32.0	.1.3.6.1.4.1.161.19.3.3.9.33.0	Integer
codePoint33.0	.1.3.6.1.4.1.161.19.3.3.9.34.0	Integer
codePoint34.0	.1.3.6.1.4.1.161.19.3.3.9.35.0	Integer
codePoint35.0	.1.3.6.1.4.1.161.19.3.3.9.36.0	Integer
codePoint36.0	.1.3.6.1.4.1.161.19.3.3.9.37.0	Integer
codePoint37.0	.1.3.6.1.4.1.161.19.3.3.9.38.0	Integer
codePoint38.0	.1.3.6.1.4.1.161.19.3.3.9.39.0	Integer
codePoint39.0	.1.3.6.1.4.1.161.19.3.3.9.40.0	Integer
codePoint40.0	.1.3.6.1.4.1.161.19.3.3.9.41.0	Integer

codePoint41.0	.1.3.6.1.4.1.161.19.3.3.9.42.0	Integer
codePoint42.0	.1.3.6.1.4.1.161.19.3.3.9.43.0	Integer
codePoint43.0	.1.3.6.1.4.1.161.19.3.3.9.44.0	Integer
codePoint44.0	.1.3.6.1.4.1.161.19.3.3.9.45.0	Integer
codePoint45.0	.1.3.6.1.4.1.161.19.3.3.9.46.0	Integer
codePoint46.0	.1.3.6.1.4.1.161.19.3.3.9.47.0	Integer
codePoint47.0	.1.3.6.1.4.1.161.19.3.3.9.48.0	Integer
codePoint48.0	.1.3.6.1.4.1.161.19.3.3.9.49.0	Integer
codePoint49.0	.1.3.6.1.4.1.161.19.3.3.9.50.0	Integer
codePoint50.0	.1.3.6.1.4.1.161.19.3.3.9.51.0	Integer
codePoint51.0	.1.3.6.1.4.1.161.19.3.3.9.52.0	Integer
codePoint52.0	.1.3.6.1.4.1.161.19.3.3.9.53.0	Integer
codePoint53.0	.1.3.6.1.4.1.161.19.3.3.9.54.0	Integer
codePoint54.0	.1.3.6.1.4.1.161.19.3.3.9.55.0	Integer
codePoint55.0	.1.3.6.1.4.1.161.19.3.3.9.56.0	Integer
codePoint56.0	.1.3.6.1.4.1.161.19.3.3.9.57.0	Integer
codePoint57.0	.1.3.6.1.4.1.161.19.3.3.9.58.0	Integer
codePoint58.0	.1.3.6.1.4.1.161.19.3.3.9.59.0	Integer
codePoint59.0	.1.3.6.1.4.1.161.19.3.3.9.60.0	Integer
codePoint60.0	.1.3.6.1.4.1.161.19.3.3.9.61.0	Integer
codePoint61.0	.1.3.6.1.4.1.161.19.3.3.9.62.0	Integer
codePoint62.0	.1.3.6.1.4.1.161.19.3.3.9.63.0	Integer
codePoint63.0	.1.3.6.1.4.1.161.19.3.3.9.64.0	Integer
entryIndex.1	.1.3.6.1.4.1.161.19.3.3.10.1.1.1	Integer
entryIndex.2	.1.3.6.1.4.1.161.19.3.3.10.1.1.2	Integer
entryIndex.3	.1.3.6.1.4.1.161.19.3.3.10.1.1.3	Integer
entryIndex.4	.1.3.6.1.4.1.161.19.3.3.10.1.1.4	Integer
userLoginName.1	.1.3.6.1.4.1.161.19.3.3.10.1.2.1	OctetString
userLoginName.2	.1.3.6.1.4.1.161.19.3.3.10.1.2.2	OctetString
userLoginName.3	.1.3.6.1.4.1.161.19.3.3.10.1.2.3	OctetString
userLoginName.4	.1.3.6.1.4.1.161.19.3.3.10.1.2.4	OctetString

userPswd.1	.1.3.6.1.4.1.161.19.3.3.10.1.3.1	OctetString
userPswd.2	.1.3.6.1.4.1.161.19.3.3.10.1.3.2	OctetString
userPswd.3	.1.3.6.1.4.1.161.19.3.3.10.1.3.3	OctetString
userPswd.4	.1.3.6.1.4.1.161.19.3.3.10.1.3.4	OctetString
accessLevel.1	.1.3.6.1.4.1.161.19.3.3.10.1.4.1	Integer
accessLevel.2	.1.3.6.1.4.1.161.19.3.3.10.1.4.2	Integer
accessLevel.3	.1.3.6.1.4.1.161.19.3.3.10.1.4.3	Integer
accessLevel.4	.1.3.6.1.4.1.161.19.3.3.10.1.4.4	Integer
loginStatus.1	.1.3.6.1.4.1.161.19.3.3.10.1.5.1	Integer
loginStatus.2	.1.3.6.1.4.1.161.19.3.3.10.1.5.2	Integer
loginStatus.3	.1.3.6.1.4.1.161.19.3.3.10.1.5.3	Integer
loginStatus.4	.1.3.6.1.4.1.161.19.3.3.10.1.5.4	Integer
loginMethod.1	.1.3.6.1.4.1.161.19.3.3.10.1.6.1	Integer
loginMethod.2	.1.3.6.1.4.1.161.19.3.3.10.1.6.2	Integer
loginMethod.3	.1.3.6.1.4.1.161.19.3.3.10.1.6.3	Integer
loginMethod.4	.1.3.6.1.4.1.161.19.3.3.10.1.6.4	Integer
sessionTime.1	.1.3.6.1.4.1.161.19.3.3.10.1.7.1	Integer
sessionTime.2	.1.3.6.1.4.1.161.19.3.3.10.1.7.2	Integer
sessionTime.3	.1.3.6.1.4.1.161.19.3.3.10.1.7.3	Integer
sessionTime.4	.1.3.6.1.4.1.161.19.3.3.10.1.7.4	Integer
neighborMAC.1	.1.3.6.1.4.1.161.19.3.3.11.1.2.1	OctetString
neighborMAC.2	.1.3.6.1.4.1.161.19.3.3.11.1.2.2	OctetString
neighborMAC.3	.1.3.6.1.4.1.161.19.3.3.11.1.2.3	OctetString
neighborMAC.4	.1.3.6.1.4.1.161.19.3.3.11.1.2.4	OctetString
neighborMAC.5	.1.3.6.1.4.1.161.19.3.3.11.1.2.5	OctetString
neighborMAC.6	.1.3.6.1.4.1.161.19.3.3.11.1.2.6	OctetString
neighborMAC.7	.1.3.6.1.4.1.161.19.3.3.11.1.2.7	OctetString
neighborMAC.8	.1.3.6.1.4.1.161.19.3.3.11.1.2.8	OctetString
neighborMAC.9	.1.3.6.1.4.1.161.19.3.3.11.1.2.9	OctetString
neighborMAC.10	.1.3.6.1.4.1.161.19.3.3.11.1.2.10	OctetString

neighborMAC.11	.1.3.6.1.4.1.161.19.3.3.11.1.2.11	OctetString
neighborMAC.12	.1.3.6.1.4.1.161.19.3.3.11.1.2.12	OctetString
neighborMAC.13	.1.3.6.1.4.1.161.19.3.3.11.1.2.13	OctetString
neighborMAC.14	.1.3.6.1.4.1.161.19.3.3.11.1.2.14	OctetString
neighborMAC.15	.1.3.6.1.4.1.161.19.3.3.11.1.2.15	OctetString
neighborMAC.16	.1.3.6.1.4.1.161.19.3.3.11.1.2.16	OctetString
neighborMAC.17	.1.3.6.1.4.1.161.19.3.3.11.1.2.17	OctetString
neighborMAC.18	.1.3.6.1.4.1.161.19.3.3.11.1.2.18	OctetString
neighborMAC.19	.1.3.6.1.4.1.161.19.3.3.11.1.2.19	OctetString
neighborMAC.20	.1.3.6.1.4.1.161.19.3.3.11.1.2.20	OctetString
neighborIP.1	.1.3.6.1.4.1.161.19.3.3.11.1.3.1	OctetString
neighborIP.2	.1.3.6.1.4.1.161.19.3.3.11.1.3.2	OctetString
neighborIP.3	.1.3.6.1.4.1.161.19.3.3.11.1.3.3	OctetString
neighborIP.4	.1.3.6.1.4.1.161.19.3.3.11.1.3.4	OctetString
neighborIP.5	.1.3.6.1.4.1.161.19.3.3.11.1.3.5	OctetString
neighborIP.6	.1.3.6.1.4.1.161.19.3.3.11.1.3.6	OctetString
neighborIP.7	.1.3.6.1.4.1.161.19.3.3.11.1.3.7	OctetString
neighborIP.8	.1.3.6.1.4.1.161.19.3.3.11.1.3.8	OctetString
neighborIP.9	.1.3.6.1.4.1.161.19.3.3.11.1.3.9	OctetString
neighborIP.10	.1.3.6.1.4.1.161.19.3.3.11.1.3.10	OctetString
neighborIP.11	.1.3.6.1.4.1.161.19.3.3.11.1.3.11	OctetString
neighborIP.12	.1.3.6.1.4.1.161.19.3.3.11.1.3.12	OctetString
neighborIP.13	.1.3.6.1.4.1.161.19.3.3.11.1.3.13	OctetString
neighborIP.14	.1.3.6.1.4.1.161.19.3.3.11.1.3.14	OctetString
neighborIP.15	.1.3.6.1.4.1.161.19.3.3.11.1.3.15	OctetString
neighborIP.16	.1.3.6.1.4.1.161.19.3.3.11.1.3.16	OctetString
neighborIP.17	.1.3.6.1.4.1.161.19.3.3.11.1.3.17	OctetString
neighborIP.18	.1.3.6.1.4.1.161.19.3.3.11.1.3.18	OctetString
neighborIP.19	.1.3.6.1.4.1.161.19.3.3.11.1.3.19	OctetString
neighborIP.20	.1.3.6.1.4.1.161.19.3.3.11.1.3.20	OctetString
neighborSiteName.1	.1.3.6.1.4.1.161.19.3.3.11.1.4.1	OctetString

neighborSiteName.2	.1.3.6.1.4.1.161.19.3.3.11.1.4.2	OctetString
neighborSiteName.3	.1.3.6.1.4.1.161.19.3.3.11.1.4.3	OctetString
neighborSiteName.4	.1.3.6.1.4.1.161.19.3.3.11.1.4.4	OctetString
neighborSiteName.5	.1.3.6.1.4.1.161.19.3.3.11.1.4.5	OctetString
neighborSiteName.6	.1.3.6.1.4.1.161.19.3.3.11.1.4.6	OctetString
neighborSiteName.7	.1.3.6.1.4.1.161.19.3.3.11.1.4.7	OctetString
neighborSiteName.8	.1.3.6.1.4.1.161.19.3.3.11.1.4.8	OctetString
neighborSiteName.9	.1.3.6.1.4.1.161.19.3.3.11.1.4.9	OctetString
neighborSiteName.10	.1.3.6.1.4.1.161.19.3.3.11.1.4.10	OctetString
neighborSiteName.11	.1.3.6.1.4.1.161.19.3.3.11.1.4.11	OctetString
neighborSiteName.12	.1.3.6.1.4.1.161.19.3.3.11.1.4.12	OctetString
neighborSiteName.13	.1.3.6.1.4.1.161.19.3.3.11.1.4.13	OctetString
neighborSiteName.14	.1.3.6.1.4.1.161.19.3.3.11.1.4.14	OctetString
neighborSiteName.15	.1.3.6.1.4.1.161.19.3.3.11.1.4.15	OctetString
neighborSiteName.16	.1.3.6.1.4.1.161.19.3.3.11.1.4.16	OctetString
neighborSiteName.17	.1.3.6.1.4.1.161.19.3.3.11.1.4.17	OctetString
neighborSiteName.18	.1.3.6.1.4.1.161.19.3.3.11.1.4.18	OctetString
neighborSiteName.19	.1.3.6.1.4.1.161.19.3.3.11.1.4.19	OctetString
neighborSiteName.20	.1.3.6.1.4.1.161.19.3.3.11.1.4.20	OctetString
dnsIpState.0	.1.3.6.1.4.1.161.19.3.3.13.1.0	Integer
dnsPrimaryMgmtIP.0	.1.3.6.1.4.1.161.19.3.3.13.2.0	IpAddress
dnsAlternateMgmtIP.0	.1.3.6.1.4.1.161.19.3.3.13.3.0	IpAddress
dnsMgmtDomainName.0	.1.3.6.1.4.1.161.19.3.3.13.4.0	OctetString
trapDomainNameAppend.0	.1.3.6.1.4.1.161.19.3.3.13.5.0	Integer
trap1.0	.1.3.6.1.4.1.161.19.3.3.13.6.0	OctetString
trap2.0	.1.3.6.1.4.1.161.19.3.3.13.7.0	OctetString
trap3.0	.1.3.6.1.4.1.161.19.3.3.13.8.0	OctetString
trap4.0	.1.3.6.1.4.1.161.19.3.3.13.9.0	OctetString
trap5.0	.1.3.6.1.4.1.161.19.3.3.13.10.0	OctetString
trap6.0	.1.3.6.1.4.1.161.19.3.3.13.11.0	OctetString

trap7.0	.1.3.6.1.4.1.161.19.3.3.13.12.0	OctetString
trap8.0	.1.3.6.1.4.1.161.19.3.3.13.13.0	OctetString
trap9.0	.1.3.6.1.4.1.161.19.3.3.13.14.0	OctetString
trap10.0	.1.3.6.1.4.1.161.19.3.3.13.15.0	OctetString
radioIndex.1	.1.3.6.1.4.1.161.19.3.3.15.1.1.1.1	Integer
radioType.1	.1.3.6.1.4.1.161.19.3.3.15.1.1.2.1	Integer
radioPaths.1	.1.3.6.1.4.1.161.19.3.3.15.1.1.3.1	Integer
pathIndex.1.1	.1.3.6.1.4.1.161.19.3.3.15.2.1.1.1.1	Integer
pathIndex.1.2	.1.3.6.1.4.1.161.19.3.3.15.2.1.1.1.2	Integer
frequency.1.5485000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5485000	Integer
frequency.1.5490000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5490000	Integer
frequency.1.5495000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5495000	Integer
frequency.1.5500000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5500000	Integer
frequency.1.5505000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5505000	Integer
frequency.1.5510000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5510000	Integer
frequency.1.5515000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5515000	Integer
frequency.1.5520000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5520000	Integer
frequency.1.5525000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5525000	Integer
frequency.1.5530000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5530000	Integer
frequency.1.5535000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5535000	Integer
frequency.1.5540000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5540000	Integer
frequency.1.5545000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5545000	Integer
frequency.1.5550000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5550000	Integer
frequency.1.5555000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5555000	Integer
frequency.1.5560000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5560000	Integer
frequency.1.5565000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5565000	Integer
frequency.1.5570000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5570000	Integer
frequency.1.5575000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5575000	Integer
frequency.1.5580000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5580000	Integer
frequency.1.5585000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5585000	Integer
frequency.1.5590000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5590000	Integer

frequency.1.5660000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5660000	Integer
frequency.1.5665000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5665000	Integer
frequency.1.5670000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5670000	Integer
frequency.1.5675000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5675000	Integer
frequency.1.5680000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5680000	Integer
frequency.1.5685000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5685000	Integer
frequency.1.5690000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5690000	Integer
frequency.1.5695000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5695000	Integer
frequency.1.5700000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5700000	Integer
frequency.1.5705000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5705000	Integer
frequency.1.5735000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5735000	Integer
frequency.1.5740000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5740000	Integer
frequency.1.5745000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5745000	Integer
frequency.1.5750000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5750000	Integer
frequency.1.5755000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5755000	Integer
frequency.1.5760000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5760000	Integer
frequency.1.5765000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5765000	Integer
frequency.1.5770000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5770000	Integer
frequency.1.5775000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5775000	Integer
frequency.1.5780000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5780000	Integer
frequency.1.5785000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5785000	Integer
frequency.1.5790000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5790000	Integer
frequency.1.5795000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5795000	Integer
frequency.1.5800000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5800000	Integer
frequency.1.5805000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5805000	Integer
frequency.1.5810000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5810000	Integer
frequency.1.5815000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5815000	Integer
frequency.1.5820000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5820000	Integer
frequency.1.5825000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5825000	Integer
frequency.1.5830000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5830000	Integer

frequency.1.5835000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5835000	Integer
frequency.1.5840000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5840000	Integer

Configuring modules for SNMP access

Cambium modules provide the following Configuration web page parameters in the SNMP tab. These govern SNMP access from the manager to the agent:

- **Community String**, which specifies the password for security between managers and the agent.
- **Accessing Subnet**, which specifies the subnet mask that allows managers to poll the agents.

Cambium modules can also be configured to send traps to specified IP addresses (SNMP trap receiver servers), The parameter for this address is named **Trap Address**.

Interface designations in SNMP

SNMP identifies the ports of the module as follows:

- Interface 1 represents the Ethernet interface of the module. To monitor the status of Interface 1 is to monitor the traffic on the Ethernet interface.
- Interface 2 represents the RF interface of the module. To monitor the status of Interface 2 is to monitor the traffic on the RF interface.

These interfaces can be viewed on the NMS through definitions that are provided in the standard MIB files.

Traps provided in the Cambium Enterprise MIB

Cambium modules provide the following SNMP traps for automatic notifications to the NMS:

- coldStart, which signals that the SNMPv2 element is reinitializing itself and that its configuration may have been altered.
- warmStart, which signals that the SNMPv2 element is reinitializing such that its configuration is unaltered.
- authenticationFailure, which signals that the SNMPv2 element has received a protocol message that is not properly authenticated (contingent on the snmpEnableAuthenTraps object setting).
- linkDown, as defined in RFC 1573
- linkUp, as defined in RFC 1573
- egpNeighborLoss, as defined in RFC 1213
- whispGPSInSync, which signals a transition from not synchronized to synchronized.
- whispGPSOutSync, which signals a transition from synchronized to not synchronized.
- whispRegComplete, which signals registration completed.
- whispRegLost, which signals registration lost.

- whispRadarDetected, which signals that the one-minute scan has been completed, radar has been detected, and the radio will shutdown.
- whispRadarEnd, which signals that the one-minute scan has been completed, radar *has not* been detected, and the radio will resume normal operation.

MIB Viewers

Any of several commercially available MIB viewers can facilitate management of these objects through SNMP. Some are available as open source software. Cambium does not endorse, support, or discourage the use of any these viewers.

MIB viewers are available and/or described at the following web sites:

http://ns3.ndgsoftware.com/Products/NetBoy30/mibbrowser.html

http://www.adventnet.com/products/snmputilities/

http://www.dart.com/samples/mib.asp

http://www.edge-technologies.com/webFiles/products/nvision/index.cfm

http://www.ipswitch.com/products/whatsup/monitoring.html

http://www.koshna.com/products/KMB/index.asp

http://www.mg-soft.si/mgMibBrowserPE.html

http://www.mibexplorer.com

http://www.netmechanica.com/mibbrowser.html

http://www.networkview.com

http://www.newfreeware.com/search.php3?q=MIB+browser

http://www.nudesignteam.com/walker.html

http://www.oidview.com/oidview.html

http://www.solarwinds.net/Tools

http://www.stargus.com/solutions/xray.html

http://www.totilities.com/Products/MibSurfer/MibSurfer.htm

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.

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.
  - Cambium supplies.
- configurability of any of the following to be the file server for image files:
  - The AP, for traditional file serving via UDP commands and monitoring vai UDP messaging
  - CNUT HTTP Server, for upgrading via SNMP commands and monitoring via SNMP messaging. This also supports an option to either set the image order specifically for this file server or to allow the AP to determine the order.
  - Local TFTP Server ,for traditional file serving via UDP commands and monitoring via UDP messaging. This supports setting the number of simultaneous image transfers per AP
- the capability to launch a test of connectivity and operational status of the local HTTP and TFTP file servers
- an interface that supports efficient specification of the proper IP address for the local file server(s) where Network Updater resides on a multi-homed computer
- an md5 checksum calculator utility for identifying corruption of downloaded image files before Network Updater is set to apply them.

Network Element Groups

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

- 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 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, each layer lying 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.

IMPORTANT!

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:

- 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 or XP Professional
  - Windows 7
  - Red Hat Enterprise Linux (32-bit) Version 4 or 5
- Java™ Runtime Version 2.0 or later (installed by the CNUT installation tool)

CNUT Download

CNUT can be downloaded together with each system release that supports CNUT. Software for these system releases is available from
http://www.cambiumnetworks.com/support/planning/index.php?cat=3&type=1

as either

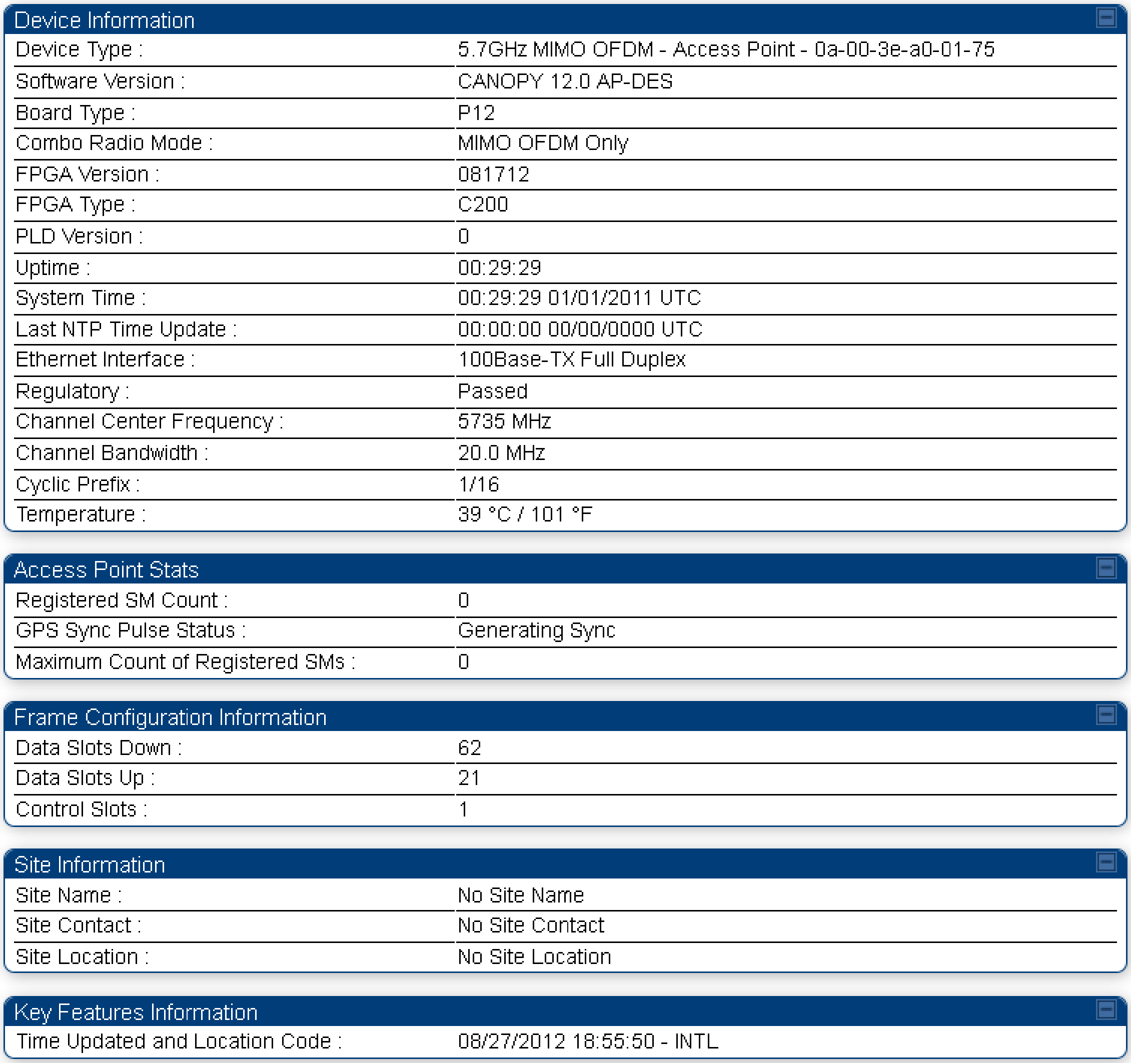
- a `.zip` file for use without the CNUT application.
- a `.pkg` file that the CNUT application can open.

Chapter 4: Using Informational Tabs in the GUI

Viewing General Status (AP)

The General Status tab provides information on the operation of this AP. This is the tab that opens by default when you access the GUI of the AP. Examples of AP General Status tabs are displayed below.

Figure 12 AP General Status page



Device Information	
Device Type :	5.7GHz MIMO OFDM - Access Point - 0a-00-3e-a0-01-75
Software Version :	CANOPY 12.0 AP-DES
Board Type :	P12
Combo Radio Mode :	MIMO OFDM Only
FPGA Version :	081712
FPGA Type :	C200
PLD Version :	0
Uptime :	00:29:29
System Time :	00:29:29 01/01/2011 UTC
Last NTP Time Update :	00:00:00 00/00/0000 UTC
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
Channel Center Frequency :	5735 MHz
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Temperature :	39 °C / 101 °F

Access Point Stats	
Registered SM Count :	0
GPS Sync Pulse Status :	Generating Sync
Maximum Count of Registered SMs :	0

Frame Configuration Information	
Data Slots Down :	62
Data Slots Up :	21
Control Slots :	1

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

Key Features Information	
Time Updated and Location Code :	08/27/2012 18:55:50 - INTL

The General Status tab provides the following read-only fields.

Table 19 AP General Status attributes

Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the AP, its module type, and its MAC address.
Software Version	This field indicates the system release, the time and date of the release. If you request technical support, provide the information from this field.
Board Type	This field indicates the series of hardware.

Attribute	Meaning
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.
FPGA Type	Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.
PLD Version	This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. If the AP is connected to a CMM, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.
Last NTP Time Update	This field displays when the AP last used time sent from an NTP server. If the AP has not been configured in the Time tab of the Configuration page to request time from an NTP server, then this field is populated by 00:00:00 00/00/00.
Ethernet Interface	This field indicates the speed and duplex state of the Ethernet interface to the AP.
Regulatory	This field indicates whether the configured Region Code and radio frequency are compliant with respect to their compatibility. For example, you may configure a 5.4-GHz AP with a **Region Code** set to **United States** and configure a frequency that lies within the weather notch. This is a compliant combination, the radio properly operates, and its **Regulatory** field displays Passed. If later you change its Region Code to Canada, then the combination becomes non-compliant (since frequencies within the weather notch are disallowed in Canada. In this case, the radio ceases to transmit, and its **Regulatory** field displays an error message.
Channel Center Frequency	The operating center frequency of the AP
Channel Bandwidth	The size in MHz of the operating channel
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.

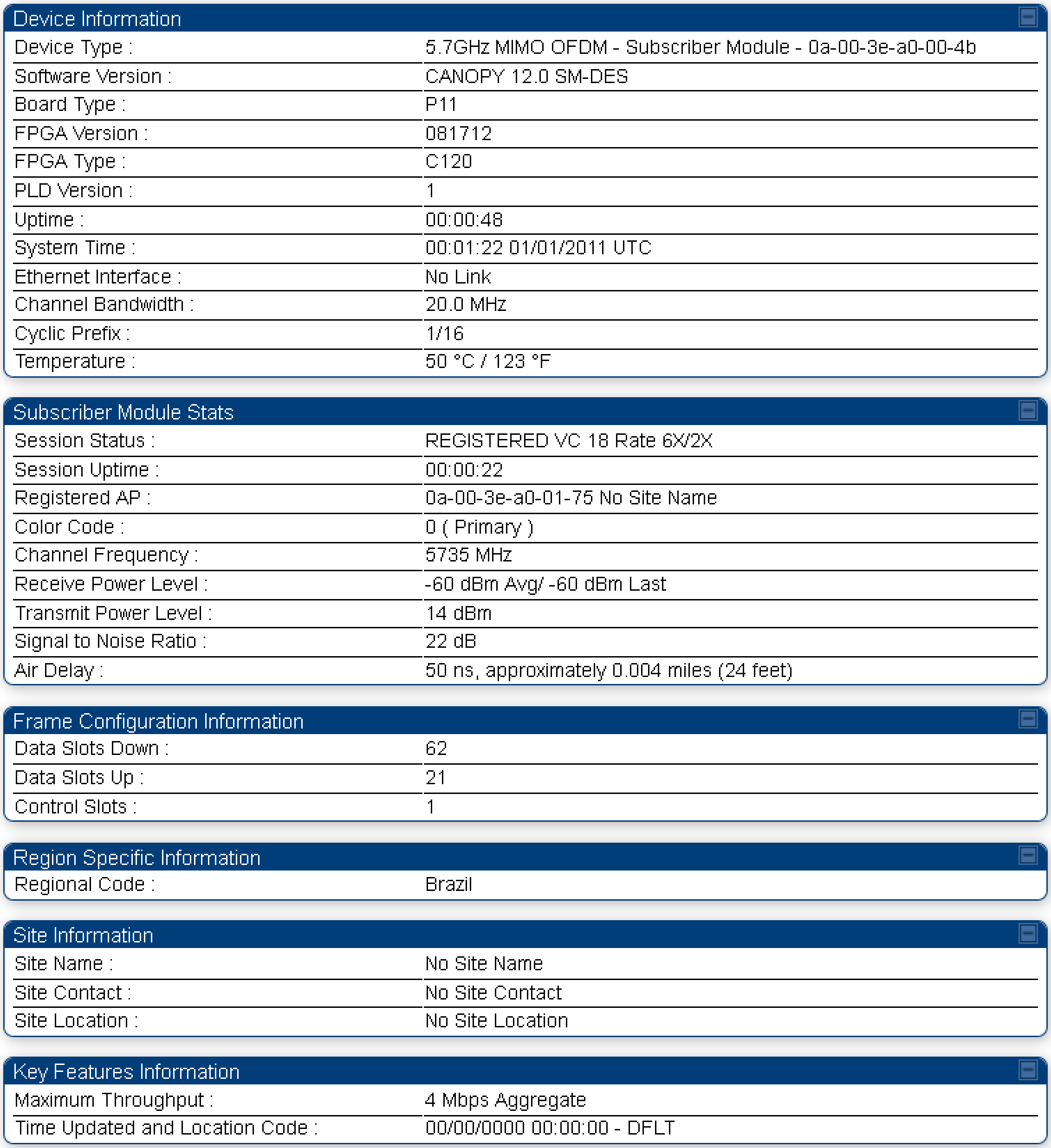
Attribute	**Meaning**
Temperature	The current operating temperature of the board
Registered SM Count	This field indicates how many SMs are registered to the AP
GPS Sync Pulse Status	This field indicates the status of synchronization as follows: **Generating sync** indicates that the module is set to *generate* the sync pulse. **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse. **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse. NOTE When this message is displayed, the AP transmitter is turned off to avoid self-interference within the system.
Max Registered SM Count	This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.
Data Slots Down	This field indicates the number of frame slots that are designated for use by data in the downlink (sent from the AP to the SM). The AP calculates the number of data slots based on the Max Range, Downlink Data, and (reserved) Control Slots configured by the operator. A + in this field (for example, 9+) indicates that there are additional bit times that the scheduler can take advantage of for control slots (which are half the size of data slots), but not enough for a full data slot.
Data Slots Up	This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data, and (reserved) Control Slots configured by the operator. A + in this field (for example, 9+) indicates that there are additional bit times that the scheduler can take advantage of for control slots (which are half the size of data slots), but not enough for a full data slot.
Control Slots	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.

Attribute	Meaning
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.
Time Updated and Location Code	This field displays information about the keying of the radio.

Viewing General Status (SM)

The General Status tab provides information on the operation of this SM. This is the tab that opens by default when you access the GUI of the SM. . An example of the General Status tab of an SM is displayed below.

Figure 13 General Status page of the SM



Device Information

Device Type :	5.7GHz MIMO OFDM - Subscriber Module - 0a-00-3e-a0-00-4b
Software Version :	CANOPY 12.0 SM-DES
Board Type :	P11
FPGA Version :	081712
FPGA Type :	C120
PLD Version :	1
Uptime :	00:00:48
System Time :	00:01:22 01/01/2011 UTC
Ethernet Interface :	No Link
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Temperature :	50 °C / 123 °F

Subscriber Module Stats

Session Status :	REGISTERED VC 18 Rate 6X/2X
Session Uptime :	00:00:22
Registered AP :	0a-00-3e-a0-01-75 No Site Name
Color Code :	0 (Primary)
Channel Frequency :	5735 MHz
Receive Power Level :	-60 dBm Avg/ -60 dBm Last
Transmit Power Level :	14 dBm
Signal to Noise Ratio :	22 dB
Air Delay :	50 ns, approximately 0.004 miles (24 feet)

Frame Configuration Information

Data Slots Down :	62
Data Slots Up :	21
Control Slots :	1

Region Specific Information

Regional Code :	Brazil

Site Information

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

Key Features Information

Maximum Throughput :	4 Mbps Aggregate
Time Updated and Location Code :	00/00/0000 00:00:00 - DFLT

The General Status tab provides the following read-only fields.

Table 20 SM General Status attributes

Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the SM, its module type, and its MAC address.
Software Version	This field indicates the system release, the time and date of the release. If you request technical support, provide the information from this field.
Board Type	This field indicates the series of hardware.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.
FPGA Type	Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.
PLD Version	This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).
Ethernet Interface	This field indicates the speed and duplex state of the Ethernet interface to the SM.
Channel Bandwidth	The size in MHz of the operating channel.
Temperature	The current operating temperature of the board.
Session Status	This field displays the following information about the current session: **Scanning** indicates that this SM currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page. **Syncing** indicates that this SM currently attempts to receive sync. **Registering** indicates that this SM has sent a registration request message to the AP and has not yet received a response. **Registered** indicates that this SM is both registered to an AP. ready to transmit and receive data packets.
Session Uptime	This field displays the duration of the current link. The syntax of the displayed time is *hh:mm:ss.*

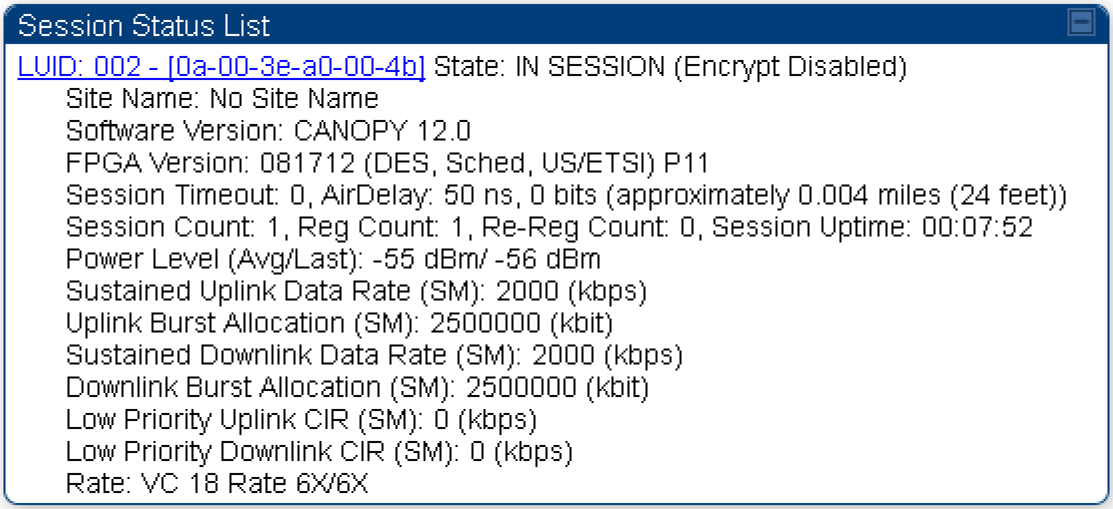
Attribute	Meaning
Registered AP	This field displays the MAC address of the AP to which this SM is registered.
Color Code	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Channel Frequency	This field lists the current operating frequency of the radio.
Receive Power Level	This field lists the current receive power level, in dBm.
Transmit Power Level	This field lists the current transmit power level, in dBm.
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor.
Air Delay	This field displays the distance in feet between this SM and the AP. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.
Data Slots Down	This field lists the number of slots used for downlink data transmission.
Data Slots Up	This field lists the number of slots used for uplink data transmission.
Control Slots	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. 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. 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. 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. Use care when changing the control slot configuration of only some APs, because changes affect the uplink/downlink ratio and can cause collocation issues. NOTE 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..

Attribute	Meaning
Region Code	A parameter that offers multiple fixed selections, each of which automatically implements frequency band range restrictions for the selected region. Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the SM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page.
Maximum Throughput	This field indicates the limit of aggregate throughput for the SM and is based on the default (factory) limit of the SM and any floating license that is currently assigned to it.
Time Updated and Location Code	This field displays information about the keying of the radio.

Viewing Session Status (AP)

The Session Status tab in the Home page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a system. This tab also includes the current active values on each SM for MIR, and VLAN, as well as the source of these values, representing the SM itself, Authentication Server, or the Authentication Server and SM.

Figure 14 Session Status tab data



Session Status List

LUID: 002 - [0a-00-3e-a0-00-4b] State: IN SESSION (Encrypt Disabled)
Site Name: No Site Name
Software Version: CANOPY 12.0
FPGA Version: 081712 (DES, Sched, US/ETSI) P11
Session Timeout: 0, AirDelay: 50 ns, 0 bits (approximately 0.004 miles (24 feet))
Session Count: 1, Reg Count: 1, Re-Reg Count: 0, Session Uptime: 00:07:52
Power Level (Avg/Last): -55 dBm/ -56 dBm
Sustained Uplink Data Rate (SM): 2000 (kbps)
Uplink Burst Allocation (SM): 2500000 (kbit)
Sustained Downlink Data Rate (SM): 2000 (kbps)
Downlink Burst Allocation (SM): 2500000 (kbit)
Low Priority Uplink CIR (SM): 0 (kbps)
Low Priority Downlink CIR (SM): 0 (kbps)
Rate: VC 18 Rate 6X/6X

Table 21 AP Session Status attributes

Attribute	Meaning
LUID	This field displays the LUID (logical unit ID) of the SM. As each SM registers to the AP, the system assigns an LUID of 2 or a higher unique number to the SM. If an SM loses registration with the AP and then regains registration, the SM will retain the same LUID. NOTE The LUID associated is lost when a power cycle of the AP occurs. Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
MAC	This field displays the MAC address (or electronic serial number) of the SM. Both the LUID and the MAC are hot links to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
State	This field displays the current status of the SM as either • **IN SESSION** to indicate that the SM is currently registered to the AP. • **IDLE** to indicate that the SM was registered to the AP at one time, but now is not. This field also indicates whether the encryption scheme in the module is enabled.

Attribute	Meaning
Site Name	This field indicates the name of the SM. You can assign or change this name on the Configuration web page of the SM. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Software Version	This field displays the software release that operates on the SM, the release date and time of the software.
Software Boot Version	This field indicates the CANOPYBOOT version number.
FPGA Version	This field displays the version of FPGA that runs on the SM.
Session Timeout	This field displays the timeout in seconds for management sessions via HTTP, ftp access to the SM. 0 indicates that no limit is imposed.
AirDelay	This field displays the distance of the SM from the AP. To derive the distance in meters, multiply the displayed number by 0.3048. At close distances, the value in this field is unreliable.
Session Count	This field displays how many sessions the SM has had with the AP. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum. If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.
Reg Count	When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field. If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).

Attribute	Meaning
Re-Reg Count	When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field. Typically, a Re-Reg is the case where both • an SM attempts to reregister for having lost communication with the AP. • the AP has not yet observed the link to the SM as being down. If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).
Sustained Uplink Data Rate	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified rate at which each SM registered to this AP is replenished with credits for transmission. The configuration source of the value is indicated in parentheses. The AP will display one of the following for the configuration source: • (SM) – QoS/VLAN parameters are derived from the SM's settings • (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps) • (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server. • (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server • (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server

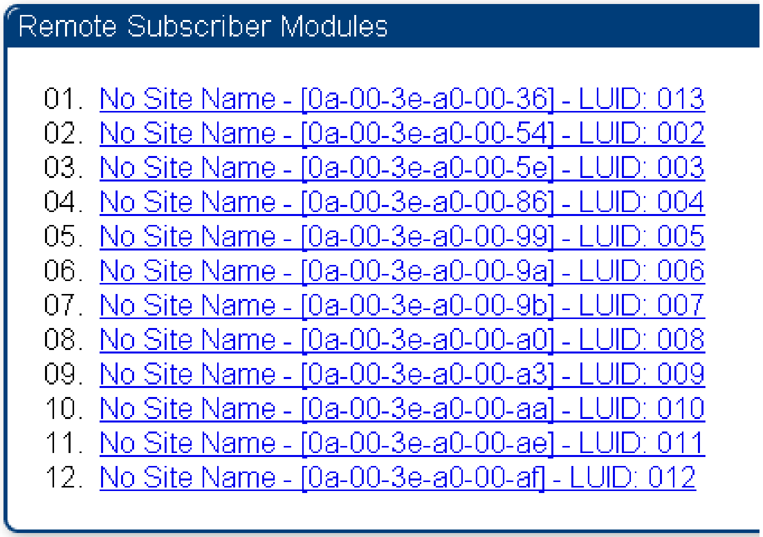
Attribute	**Meaning**
Uplink Burst Allocation	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified maximum amount of data that each SM is allowed to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. The configuration source of the value is indicated in parentheses. The AP will display one of the following for the configuration source: • (SM) – QoS/VLAN parameters are derived from the SM's settings • (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps) • (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server. • (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server • (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server
Sustained Downlink Data Rate	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. The configuration source of the value is indicated in parentheses. The AP will display one of the following for the configuration source: • (SM) – QoS/VLAN parameters are derived from the SM's settings • (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps) • (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server. • (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server • (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server

Attribute	Meaning
Downlink Burst Allocation	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is 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**. The configuration source of the value is indicated in parentheses. The AP will display one of the following for the configuration source: • (SM) – QoS/VLAN parameters are derived from the SM's settings • (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps) • (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server. • (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server • (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server
Rate	This field displays whether the high-priority channel is enabled in the SM and the status of rate adapt. For example, if "6X/4X" is listed, the radio is capable of operating at 6X but is currently operating at 4X, due to RF conditions.

Viewing Remote Subscribers (AP)

This tab allows you to view the web pages of registered SMs over the RF link. To view the pages for a selected SM, click its link. The General Status tab of the SM opens.

Figure 15 Remote Subscribers tab of the AP



Remote Subscriber Modules

01. No Site Name - [0a-00-3e-a0-00-36] - LUID: 013
02. No Site Name - [0a-00-3e-a0-00-54] - LUID: 002
03. No Site Name - [0a-00-3e-a0-00-5e] - LUID: 003
04. No Site Name - [0a-00-3e-a0-00-86] - LUID: 004
05. No Site Name - [0a-00-3e-a0-00-99] - LUID: 005
06. No Site Name - [0a-00-3e-a0-00-9a] - LUID: 006
07. No Site Name - [0a-00-3e-a0-00-9b] - LUID: 007
08. No Site Name - [0a-00-3e-a0-00-a0] - LUID: 008
09. No Site Name - [0a-00-3e-a0-00-a3] - LUID: 009
10. No Site Name - [0a-00-3e-a0-00-aa] - LUID: 010
11. No Site Name - [0a-00-3e-a0-00-ae] - LUID: 011
12. No Site Name - [0a-00-3e-a0-00-af] - LUID: 012

Interpreting messages in the Event Log

Each line in the Event Log of a module Home page begins with a time and date stamp. However, some of these lines wrap as a combined result of window width, browser preferences, and line length. You may find this tab easiest to use if you widen the window until all lines are shown as beginning with the time and date stamp.

Time and Date Stamp

The time and date stamp reflect either

- GPS time and date directly or indirectly received from the CMM.
- NTP time and date from an NTP server (CMM may serve as an NTP server)
- the running time and date that you have set in the Time & Date web page.

NOTE

In the Time & Date web page, if you have left any time field or date field unset and clicked the **Set Time and Date** button, then the time and date default to 00:00:00 UT : 01/01/00.

A reboot causes the preset time to pause or, in some cases, to run in reverse. Additionally, a power cycle resets the running time and date to the default 00:00:00 UT : 01/01/00. Thus, whenever either a reboot or a power cycle has occurred, you should reset the time and date in the Time & Date web page of any module that is not set to receive sync.

Event Log Data Collection

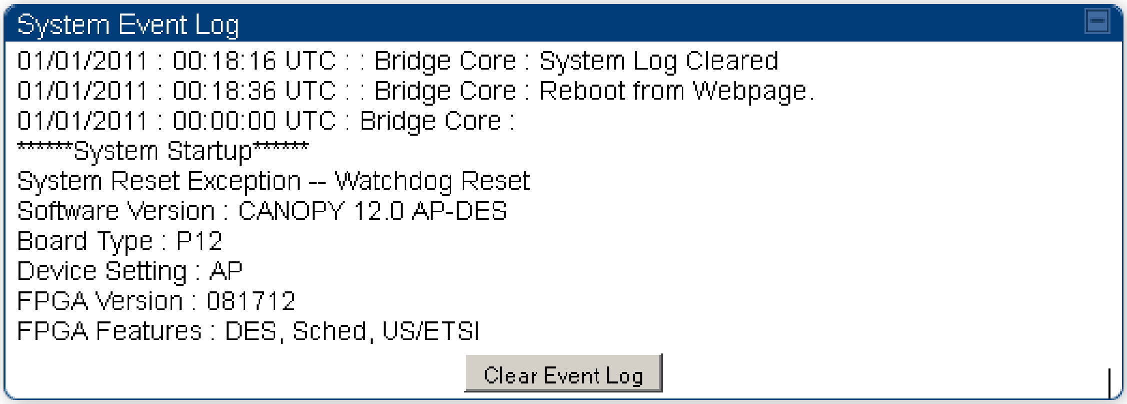
The collection of event data continues through reboots and power cycles. When the buffer allowance for event log data is reached, the system adds new data into the log and discards an identical amount of the oldest data.

Each line that contains the expression WatchDog flags an event that was both

- considered by the system software to have been an exception
- recorded in the *preceding* line.

Conversely, a Fatal Error() message flags an event that is recorded in the *next* line. Some exceptions and fatal errors may be significant and require either operator action or technical support.

Figure 16 Event log data



System Event Log

```
01/01/2011 : 00:18:16 UTC : : Bridge Core : System Log Cleared
01/01/2011 : 00:18:36 UTC : : Bridge Core : Reboot from Webpage.
01/01/2011 : 00:00:00 UTC : Bridge Core :
******System Startup******
System Reset Exception -- Watchdog Reset
Software Version : CANOPY 12.0 AP-DES
Board Type : P12
Device Setting : AP
FPGA Version : 081712
FPGA Features : DES, Sched, US/ETSI
```

Messages that Flag Abnormal Events

The messages listed below flag abnormal events and, case by case, may signal the need for corrective action or technical support.

Table 22 Event Log messages for abnormal events

Event Message	Meaning
Expected LUID = 6 Actual LUID = 7	Something is interfering with the control messaging of the module. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.

Event Message	Meaning
FatalError()	The event recorded on the line immediately beneath this message triggered the Fatal Error().
Loss of GPS Sync Pulse	Module has lost GPS sync signal.
Machine Check Exception	This is a symptom of a possible hardware failure. If this is a recurring message, begin the RMA process for the module.

RcvFrmNum = *0x00066d*
ExpFrmNum = *0x000799*
	Something is interfering with the control messaging of the module. Also ensure that you are using shielded cables to minimize interference. Consider trying different frequency options to eliminate or reduce interference.

System Reset Exception -- External Hard Reset	The unit lost power or was power cycled.
System Reset Exception -- External Hard Reset WatchDog	The event recorded on the preceding line triggered this WatchDog message.

Messages that Flag Normal Events

The messages listed below record normal events and typically *do not* signal a need for any corrective action or technical support.

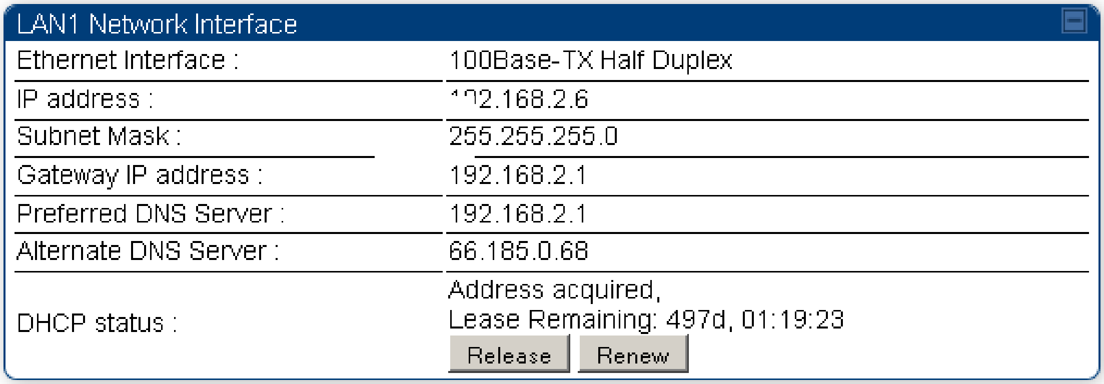
Figure 17 Event Log messages for normal events

Event Message	Meaning
Acquired GPS Sync Pulse.	Module has acquired GPS sync signal.
FPGA Features	Type of encryption.
FPGA Version	FPGA (JBC) version in the module.
GPS Date/Time Set	Module is now on GPS time.
Reboot from Webpage	Module was rebooted from management interface.
Software Boot Version	Boot version in the module.
Software Version	The software release and authentication method for the unit.
System Log Cleared	Event log was manually cleared.

Viewing the Network Interface Tab (All)

In any module, the LAN1 Network Interface section of this tab displays the defined Internet Protocol scheme for the Ethernet interface to the module. In SM devices, this tab also provides an RF Public Network Interface section, which displays the Internet Protocol scheme defined for network access through the master device (AP).

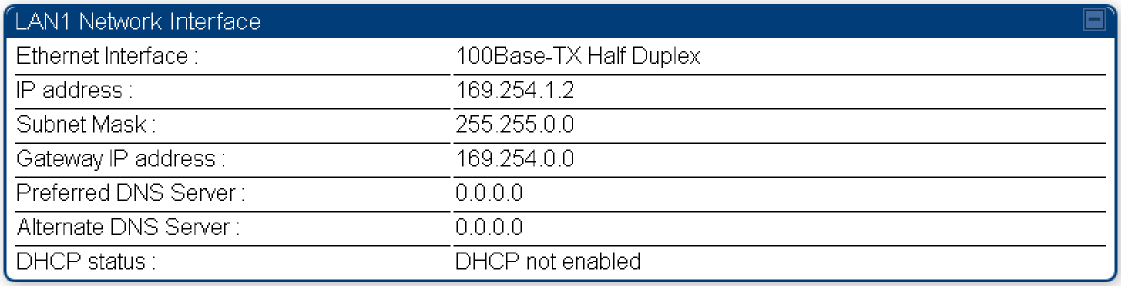
Figure 18 Network Interface tab of the AP



LAN1 Network Interface

Ethernet Interface :	100Base-TX Half Duplex
IP address :	192.168.2.6
Subnet Mask :	255.255.255.0
Gateway IP address :	192.168.2.1
Preferred DNS Server :	192.168.2.1
Alternate DNS Server :	66.185.0.68
DHCP status :	Address acquired, Lease Remaining: 497d, 01:19:23

Figure 19 Network Interface tab of the SM



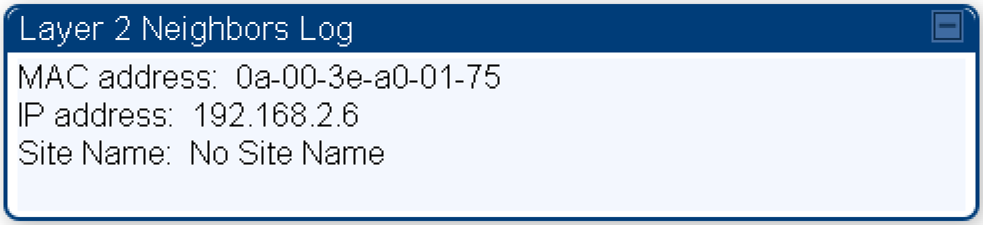
LAN1 Network Interface

Ethernet Interface :	100Base-TX Half Duplex
IP address :	169.254.1.2
Subnet Mask :	255.255.0.0
Gateway IP address :	169.254.0.0
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
DHCP status :	DHCP not enabled

Viewing the Layer 2 Neighbors Tab (AP and SM)

In the Layer 2 Neighbors tab, a module reports any device from which it has received a message in Link Layer Discovery Protocol within the previous two minutes. Given the frequency of LLDP messaging, this means that the connected device will appear in this tab 30 seconds after it is booted and remain until two minutes after its shutdown.

Figure 20 Layer 2 Neighbors tab



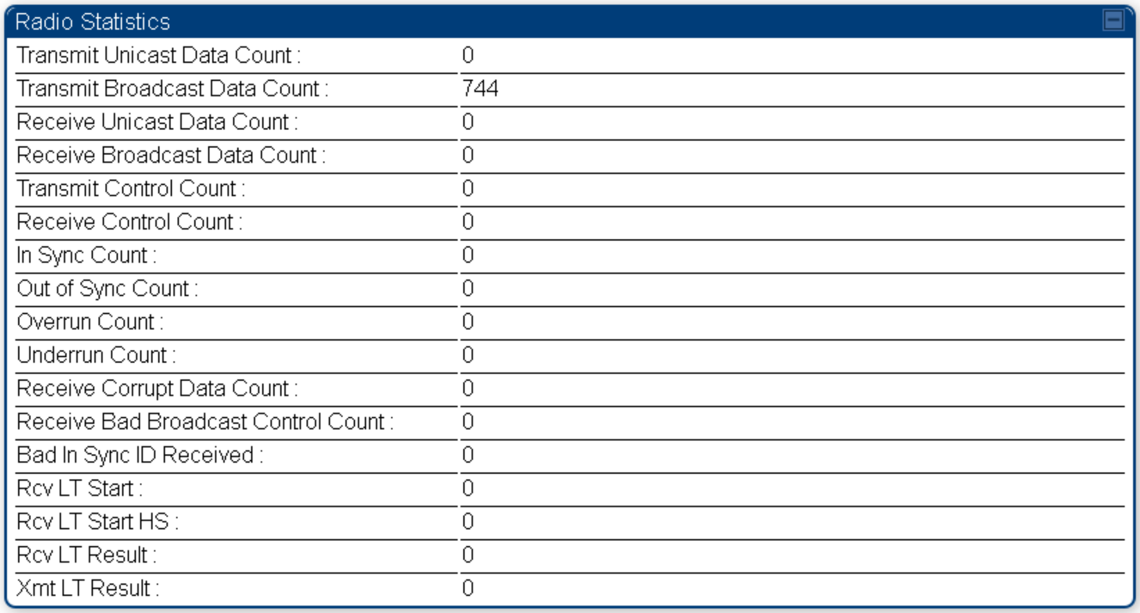
Layer 2 Neighbors Log

MAC address: 0a-00-3e-a0-01-75
IP address: 192.168.2.6
Site Name: No Site Name

Viewing the Scheduler Tab (AP and SM)

Statistics for the Scheduler are displayed as shown below.

Figure 21 Scheduler tab of the AP



Radio Statistics

Transmit Unicast Data Count :	0
Transmit Broadcast Data Count :	744
Receive Unicast Data Count :	0
Receive Broadcast Data Count :	0
Transmit Control Count :	0
Receive Control Count :	0
In Sync Count :	0
Out of Sync Count :	0
Overrun Count :	0
Underrun Count :	0
Receive Corrupt Data Count :	0
Receive Bad Broadcast Control Count :	0
Bad In Sync ID Received :	0
Rcv LT Start :	0
Rcv LT Start HS :	0
Rcv LT Result :	0
Xmt LT Result :	0

Table 23 Scheduler tab attributes

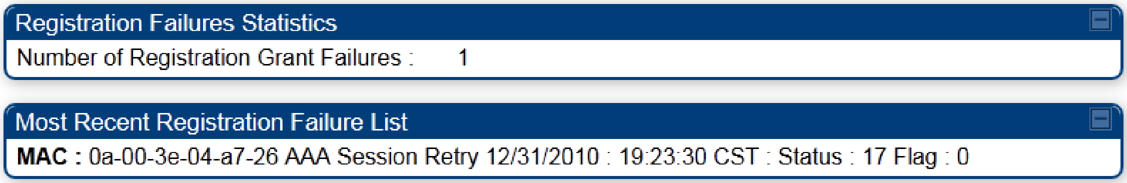
Event Message	Meaning
Transmit Unicast Data Count	The total amount of unicast packets transmitted from the radio
Transmit Broadcast Data Count	The total amount of broadcast packets transmitted from the radio
Receive Unicast Data Count	The total amount of unicast packets received by the radio
Receive Broadcast Data Count	The total amount of broadcast packets received by the radio
Transmit Control Count	The amount of radio control type messages transmitted (registration requests and grants, power adjust, etc.).
Receive Control Count	The amount of radio control type messages received (registration requests and grants, power adjust, etc.).

Event Message	Meaning
In Sync Count	Number of times the radio has acquired sync. In the case of an AP generating sync this is when generated sync has been locked, or if GPS synchronization is used it is number of times GPS sync acquired. For the SM, it is the number of times the SM successfully obtained sync with an AP.
Out of Sync Count	Number of times the radio lost same sync lock.
Overrun Count	Number of times FPGA frame has overrun its TX Frame
Underrun Count	Number of times FPGAs TX Frame aborted prematurely.
Receive Corrupt Data Count	Number of times a corrupt fragment has been received at the FPGA.
Receive Bad Broadcast Control Count	Number of times the radio has received an invalid control message via broadcast (SM only).
Bad In Sync ID Received	Currently unused
Rcv LT Start	Number of Link Test Start messages received. A remote radio has requested that this radio start a link test to it.
Rcv LT Start HS	Number of Link Test Start Handshake messages received. This radio requested that a remote radio start a link test and the remote radio has sent a handshake back acknowledging the start.
Rcv LT Result	This radio received Link Test results from the remote radio under test. When this radio initiates a link test, the remote radio will send its results to this radio for display.
Xmt LT Result	This radio transmitted its link test results to the remote radio under test. When the remote radio initiates a link test, this radio must send its results to the remote radio for display there.

List of Registration Failures (AP)

The SM Registration Failures tab identifies SMs that have recently attempted and failed to register to this AP. With its time stamps, these instances may suggest that a new or transient source of interference exists.

Figure 22 SM Registration Failures tab of the AP



Registration Failures Statistics

Number of Registration Grant Failures : 1

Most Recent Registration Failure List

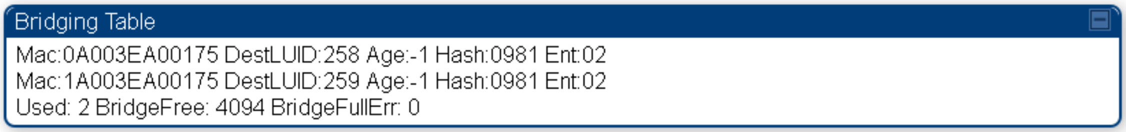
MAC : 0a-00-3e-04-a7-26 AAA Session Retry 12/31/2010 : 19:23:30 CST : Status : 17 Flag : 0

Interpreting Data in the Bridging Table (All)

If NAT (network address translation) is not active on the SM, then the Bridging Table tab provides the MAC address of all devices that are attached to registered SMs (identified by LUIDs). The bridging table allows data to be sent to the correct module as follows:

- For the AP, the uplink is from RF to Ethernet. Thus, when a packet arrives in the *RF* interface to the AP, the AP reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the *RF* interface.
- For the SM, the uplink is from Ethernet to RF. Thus, when a packet arrives in the *Ethernet* interface to one of these modules, the module reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the *Ethernet* interface.

Figure 23 Bridging Table tab of the AP



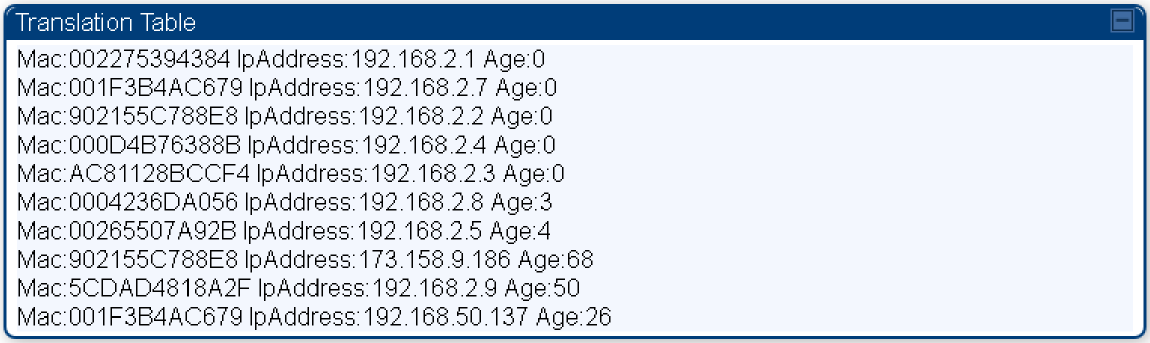
Bridging Table

```
Mac:0A003EA00175 DestLUID:258 Age:-1 Hash:0981 Ent:02
Mac:1A003EA00175 DestLUID:259 Age:-1 Hash:0981 Ent:02
Used: 2 BridgeFree: 4094 BridgeFullErr: 0
```

Translation Table (SM)

When Translation Bridging is enabled in the AP, each SM keeps a table mapping MAC addresses of devices attached to the AP to IP addresses, as otherwise the mapping of end-user MAC addresses to IP addresses is lost. (When Translation Bridging is enabled, an AP modifies all uplink traffic originating from registered SMs such that the source MAC address of every packet will be changed to that of the SM which bridged the packet in the uplink direction.)

Figure 24 Translation Table tab of the SM



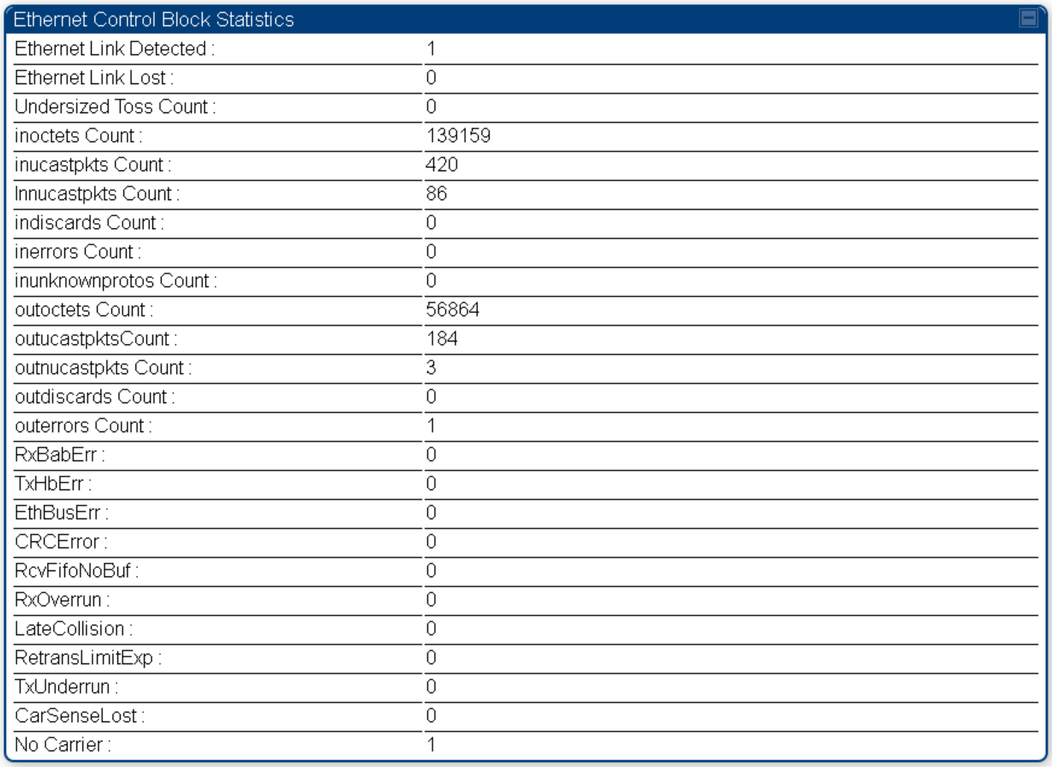
Translation Table

```
Mac:002275394384 IpAddress:192.168.2.1 Age:0
Mac:001F3B4AC679 IpAddress:192.168.2.7 Age:0
Mac:902155C788E8 IpAddress:192.168.2.2 Age:0
Mac:000D4B76388B IpAddress:192.168.2.4 Age:0
Mac:AC81128BCCF4 IpAddress:192.168.2.3 Age:0
Mac:0004236DA056 IpAddress:192.168.2.8 Age:3
Mac:00265507A92B IpAddress:192.168.2.5 Age:4
Mac:902155C788E8 IpAddress:173.158.9.186 Age:68
Mac:5CDAD4818A2F IpAddress:192.168.2.9 Age:50
Mac:001F3B4AC679 IpAddress:192.168.50.137 Age:26
```

Interpreting Data in the Ethernet Tab (All)

The Ethernet tab of the Statistics web page reports TCP throughput and error information for the Ethernet connection of the module.

Figure 25 Ethernet tab of AP



Ethernet Control Block Statistics

Ethernet Link Detected :	1
Ethernet Link Lost :	0
Undersized Toss Count :	0
inoctets Count :	139159
inucastpkts Count :	420
Innucastpkts Count :	86
indiscards Count :	0
inerrors Count :	0
inunknownprotos Count :	0
outoctets Count :	56864
outucastpktsCount :	184
outnucastpkts Count :	3
outdiscards Count :	0
outerrors Count :	1
RxBabErr :	0
TxHbErr :	0
EthBusErr :	0
CRCError :	0
RcvFifoNoBuf :	0
RxOverrun :	0
LateCollision :	0
RetransLimitExp :	0
TxUnderrun :	0
CarSenseLost :	0
No Carrier :	1

The Ethernet tab displays the following fields.

Table 24 Ethernet tab attributes

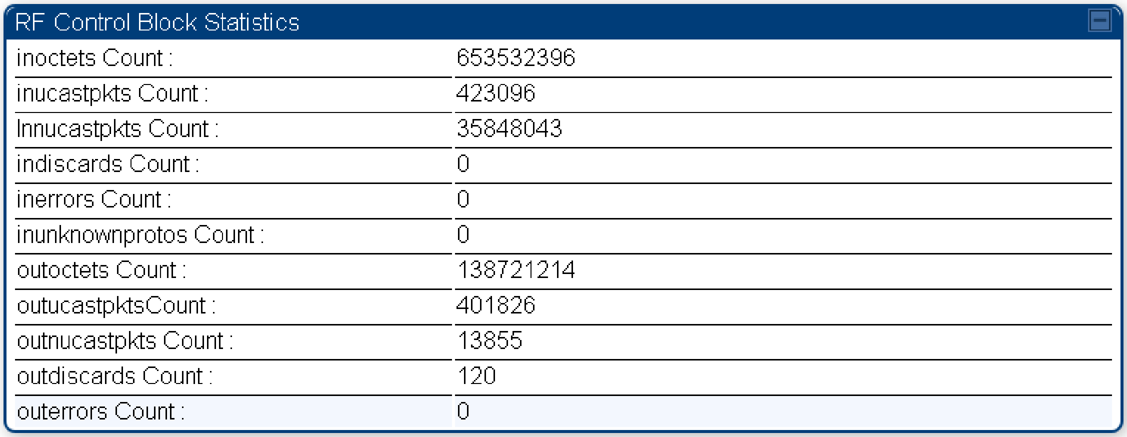
Attribute	Meaning
Ethernet Link Detected	1 indicates that an Ethernet link is established to the radio, 0 indicates that no Ethernet link is established
Ethernet Link Lost	This field indicates a count of how many times the Ethernet link was lost.
Undersized Toss Count	This field indicates the number of packets that were too small to process and hence discarded.
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.

Attribute	Meaning
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
indiscards Count	This field displays 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	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
inunknownprotos Count	This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.
outoctets Count	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts Count	This field displays 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.
outnucastpkts Count	This field displays 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.
outdiscards Count	This field displays 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.)
outerrrors Count	This field displays how many outbound packets contained errors that prevented their transmission.
RxBabErr	This field displays how many receiver babble errors occurred.
TxHbErr	This field displays how many transmit heartbeat errors have occured.
EthBusErr	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
CRCError	This field displays how many CRC errors occurred on the Ethernet controller.
RcvFifoNoBuf	This field displays the number of times no FIFO buffer space was able to be allocated
RxOverrun	This field displays how many receiver overrun errors occurred on the Ethernet controller.

Attribute	Meaning
Late Collision	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. *IMPORTANT!* 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.
RetransLimitExp	This field displays how many times the retransmit limit has expired.
TxUnderrun	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
CarSenseLost	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
No Carrier	This field displays how many no carrier errors occurred on the Ethernet controller.

Interpreting RF Control Block Statistics in the Radio Tab (All)

Figure 26 Radio tab of the Statistics page, SM



RF Control Block Statistics

inoctets Count :	653532396
inucastpkts Count :	423096
Innucastpkts Count :	35848043
indiscards Count :	0
inerrors Count :	0
inunknownprotos Count :	0
outoctets Count :	138721214
outucastpktsCount :	401826
outnucastpkts Count :	13855
outdiscards Count :	120
outerrors Count :	0

The Radio tab of the Statistics page displays the following fields.

Table 25 Radio (Statistics) tab attributes

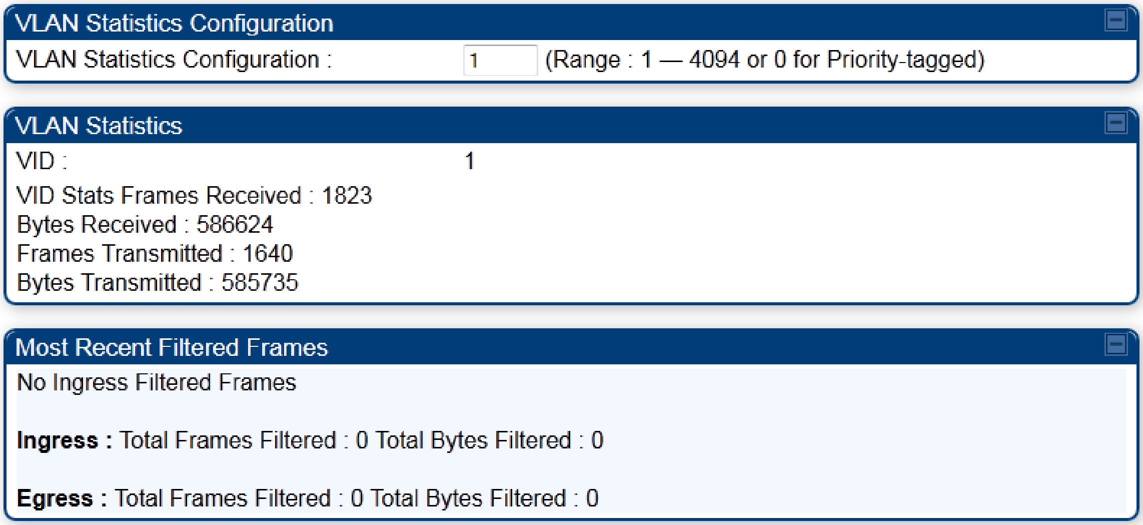
Attribute	Meaning
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
indiscards Count	This field displays 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	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
inunknownprotos Count	This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.

Attribute	Meaning
outoctets Count	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts Count	This field displays 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.
outnucastpkts Count	This field displays 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.
outdiscards Count	This field displays 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	This field displays how many outbound packets contained errors that prevented their transmission.

Interpreting Data in the VLAN Tab (ALL)

The VLAN tab in the Statistics web page provides a list of the most recent packets that were filtered because of VLAN membership violations.

Figure 27 VLAN tab of the AP



VLAN Statistics Configuration

VLAN Statistics Configuration : 1 (Range : 1 — 4094 or 0 for Priority-tagged)

VLAN Statistics

VID : 1

VID Stats Frames Received : 1823
Bytes Received : 586624
Frames Transmitted : 1640
Bytes Transmitted : 585735

Most Recent Filtered Frames

No Ingress Filtered Frames

Ingress : Total Frames Filtered : 0 Total Bytes Filtered : 0

Egress : Total Frames Filtered : 0 Total Bytes Filtered : 0

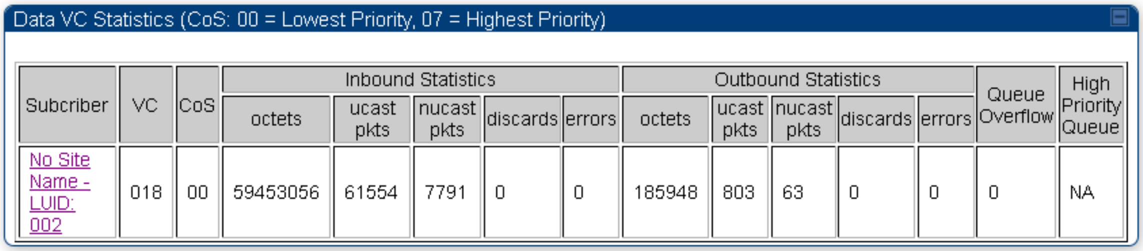
Interpret entries under **Most Recent Filtered Frames** as follows:

- **Unknown**—This should not occur. Contact Technical Support.
- **Only Tagged**—The packet was filtered because the configuration is set to accept only packets that have an 802.1Q header, and this packet did not.
- **Ingress**—When the packet entered through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
- **Local Ingress**—When the packet was received from the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership. This should not occur. Contact Technical Support.
- **Egress**—When the packet attempted to leave through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
- **Local Egress**—When the packet attempted to reach the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership.

Viewing Data VC Statistics (All)

The Data VC Statistics tab displays information about the virtual channel (VC) used for data communications.

Figure 28 Data VC tab of the AP



Data VC Statistics (CoS: 00 = Lowest Priority, 07 = Highest Priority)

Subcriber	VC	CoS	Inbound Statistics					Outbound Statistics					Queue Overflow	High Priority Queue
			octets	ucast pkts	nucast pkts	discards	errors	octets	ucast pkts	nucast pkts	discards	errors		
No Site Name - LUID: 002	018	00	59453056	61554	7791	0	0	185948	803	63	0	0	0	NA

The Data VC tab page displays the following fields.

Table 26 Data VC tab attributes

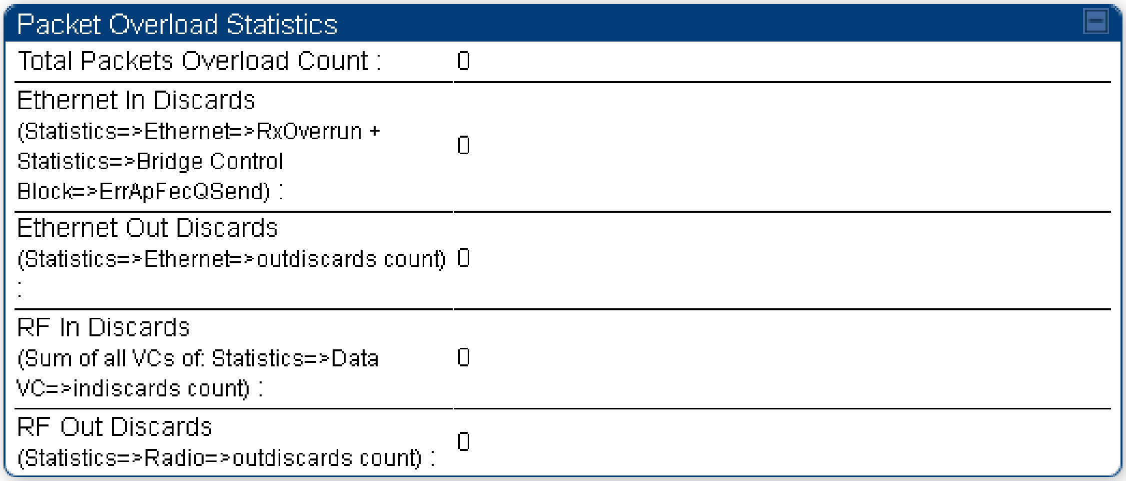
Attribute	Meaning
VC	This field displays the virtual channel number. Low priority channels start at VC18 and count up. High priority channels start at VC255 and count down. If one VC is displayed, the high-priority channel is disabled. If two are displayed, the high-priority channel is enabled.
CoS	This field displays the Class of Service for the virtual channel. The low priority channel is a CoS of 00, and the high priority channel is a CoS of 01. CoS of 02 through 07 are not currently used.
inoctets	This field displays how many octets were received on the interface, including those that deliver framing information.

Attribute	Meaning
inucastpkts	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
innucastpkts	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
indiscards	This field displays 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	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
outoctets	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts	This field displays 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.
outnucastpkts	This field displays 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.
outdiscards	This field displays 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.)
outerrrors	This field displays how many outbound packets contained errors that prevented their transmission.
Queue Overflo	This is a count of packets that were discarded because the queue for the VC was already full.

Viewing Summary Information in the Overload Tab (All)

The Overload tab displays statistics on packet overload and resultant packet discards. Unlike the other fields, the Total Packets Overload Count is expressed in only this tab. It is not a count of how many packets have been lost, but rather of how many discard events (packet loss bursts) have been detected due to overload condition.

Figure 29 Overload tab of the AP



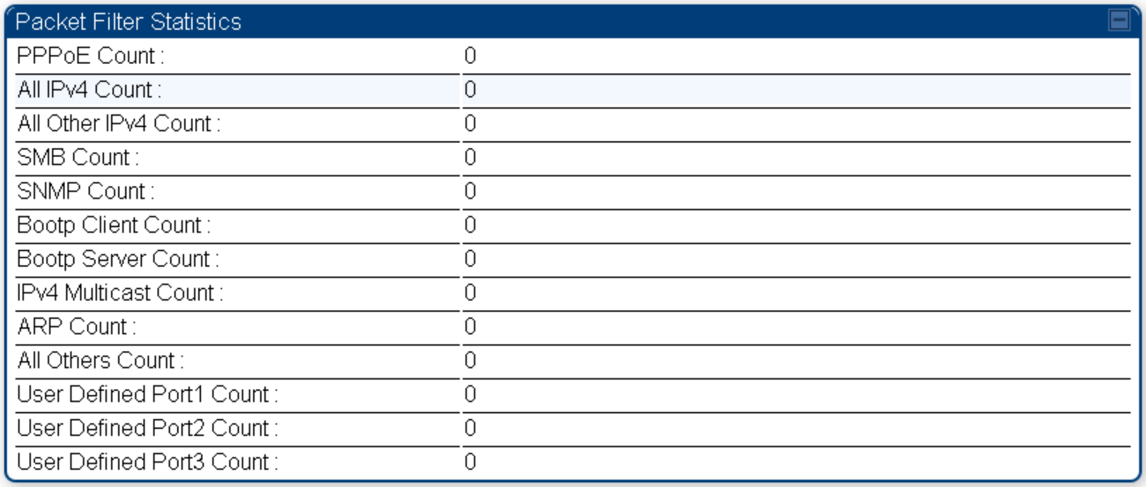
Packet Overload Statistics

Total Packets Overload Count :	0
Ethernet In Discards (Statistics=>Ethernet=>RxOverrun + Statistics=>Bridge Control Block=>ErrApFecQSend) :	0
Ethernet Out Discards (Statistics=>Ethernet=>outdiscards count) :	0
RF In Discards (Sum of all VCs of: Statistics=>Data VC=>indiscards count) :	0
RF Out Discards (Statistics=>Radio=>outdiscards count) :	0

Viewing Filter Statistics (SM)

The Filter tab displays statistics on packets that have been filtered (dropped) due to the filters set on the Protocol Filtering tab.

Figure 30 Filter tab of the SM



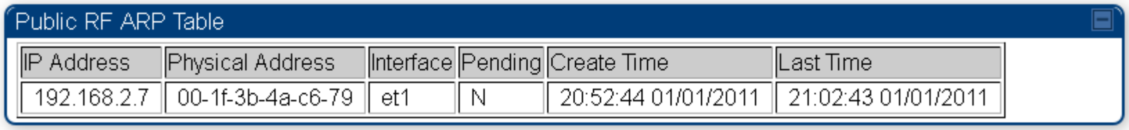
Packet Filter Statistics

PPPoE Count :	0
All IPv4 Count :	0
All Other IPv4 Count :	0
SMB Count :	0
SNMP Count :	0
Bootp Client Count :	0
Bootp Server Count :	0
IPv4 Multicast Count :	0
ARP Count :	0
All Others Count :	0
User Defined Port1 Count :	0
User Defined Port2 Count :	0
User Defined Port3 Count :	0

Viewing ARP Statistics (SM)

The ARP tab in an SM module correlated the IP address of the Ethernet-connected device to its MAC address and provides data about the connection.

Figure 31 ARP tab of the SM



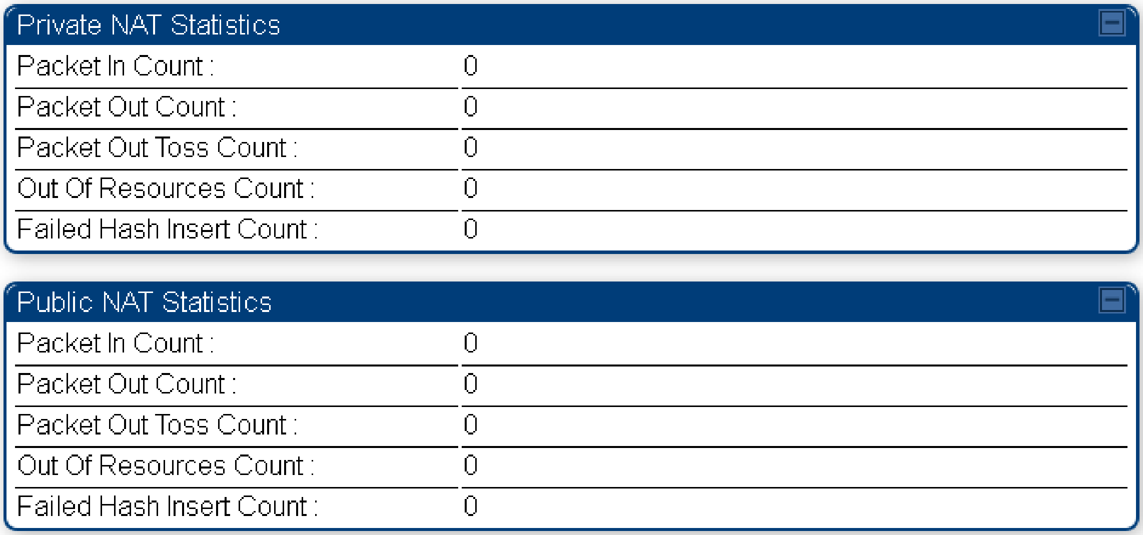
Public RF ARP Table

IP Address	Physical Address	Interface	Pending	Create Time	Last Time
192.168.2.7	00-1f-3b-4a-c6-79	et1	N	20:52:44 01/01/2011	21:02:43 01/01/2011

Viewing NAT Statistics (SM)

When NAT is enabled on an SM, statistics are kept on the Public and Private (WAN and LAN) sides of the NAT, and displayed on the NAT Stats tab.

Figure 32 NAT Stats tab of the SM



Private NAT Statistics

Packet In Count :	0
Packet Out Count :	0
Packet Out Toss Count :	0
Out Of Resources Count :	0
Failed Hash Insert Count :	0

Public NAT Statistics

Packet In Count :	0
Packet Out Count :	0
Packet Out Toss Count :	0
Out Of Resources Count :	0
Failed Hash Insert Count :	0

Table 27 NAT Stats attributes

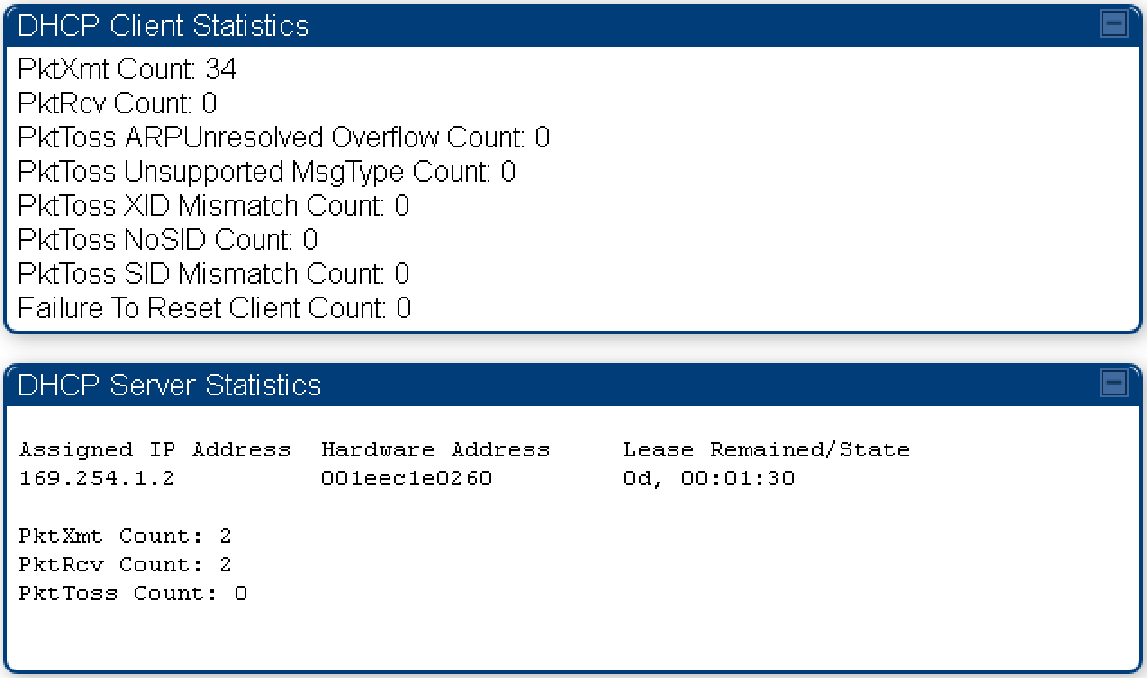
Attribute	Meaning
Private NAT Statistics, Packet In Count	This field represents the number of packets received on the SM's LAN/Ethernet interface
Private NAT Statistics, Packet Out Count	This field represents the number of packets sent from the SM's LAN/Ethernet interface
Private NAT Statistics, Packet Out Toss Count	This field represents the number of packets that we not sent from the SM's LAN/Ethernet interface due to addressing issues.
Private NAT Statistics, Out of Resources Count	This field represents the number of times the NAT table for the SM's LAN/Ethernet interfaces has been filled.
Private NAT Statistics, Failed Hash Insert Count	This field represents the number of times that the device failed to insert an address binding into the NAT hash table.
Public NAT Statistics, Packet In Count	This field represents the number of packets received on the SM's WAN/wireless interface
Public NAT Statistics, Packet Out Count	This field represents the number of packets sent from the SM's WAN/wireless interface
Public NAT Statistics, Out of Resources Count	This field represents the number of packets that we not sent from the SM's WAN/wireless interface due to addressing issues.

Attribute	Meaning
Public NAT Statistics, Failed Hash Insert Count	This field represents the number of times the NAT table for the SM's WAN/wireless interfaces has been filled.

Viewing NAT DHCP Statistics (SM)

When NAT is enabled on an SM with DHCP client (**DHCP** selected as the **Connection Type** of the WAN interface) and/or DHCP Server, statistics are kept for packets transmitted, received, and tossed, as well as a table of lease information for the DHCP server (Assigned IP Address, Hardware Address, and Lease Remained/State).

Figure 33 NAT DHCP Statistics of the SM



DHCP Client Statistics

PktXmt Count: 34
PktRcv Count: 0
PktToss ARPUnresolved Overflow Count: 0
PktToss Unsupported MsgType Count: 0
PktToss XID Mismatch Count: 0
PktToss NoSID Count: 0
PktToss SID Mismatch Count: 0
Failure To Reset Client Count: 0

DHCP Server Statistics

```
Assigned IP Address  Hardware Address     Lease Remained/State
169.254.1.2          001eec1e0260         0d, 00:01:30

PktXmt Count: 2
PktRcv Count: 2
PktToss Count: 0
```

Table 28 NAT DHCP Statistics tab of the SM

Attribute	Meaning
PktXmt Count	This field represents the number of DHCP packets transmitted from the client
PktRcv Count	This field represents the number of DHCP packets received by the client
PktToss ARPUnresolved Overflow Count	This field represents the number of packets tossed due to failed attempts to resolve an IP address into a physical MAC address

Attribute	Meaning
PktToss Unsupported MsgType Count	This field represents the number of packets tossed due to the receipt of an unsupported message type (cannot be interpreted by DHCP client)
PktToss XID Mismatch Count	The field represents the number of packets that were tossed due to a transaction ID mismatch
PktToss NoSID Count	This field represents the number of packets that were tossed due to lack of a DHCP session ID
PktToss SIT Mismatch Count	This field represents the number of packets that were tossed due to a session ID mismatch
Failure to Reset Client Count	This field represents the number of times the DHCP client was unable to be reset (resulting in no IP address being served).

Interpreting Data in the GPS Status Page (AP)

The GPS Status tab is only displayed when the Sync Input is set to Sync to Received Signal (Timing Port), which is the configuration desired when connecting an AP to a CMM or UGPS.

The page displays information similar to that available on the web pages of a CMM, including Pulse Status, GPS Time and Date, Satellites Tracked, Available Satellites, Height, Latitude, and Longitude. This page also displays the state of the antenna in the **Antenna Connection** field as

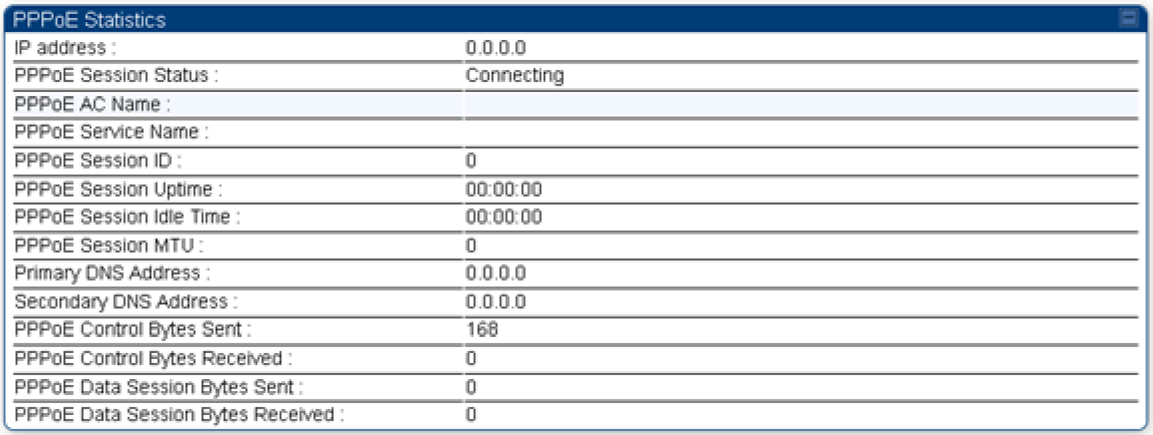
- Unknown—Shown for early CMM2s.
- OK—Shown for later CMM2s where no problem is detected in the signal.
- Overcurrent—Indicates a coax cable or connector problem, or a problem with the unit
- Undercurrent—Indicates a coax cable or connector problem, or a problem with the unit

This information may be helpful in a decision of whether to climb a tower to diagnose a perceived antenna problem.

Accessing PPPoE Statistics About Customer Activities (SM)

When the PPPoE feature has been enabled in the SM, the PPPoE statistics provide data about the activities of the customer.

Figure 34 PPPoE tab of the SM



PPPoE Statistics

IP address :	0.0.0.0
PPPoE Session Status :	Connecting
PPPoE AC Name :	
PPPoE Service Name :	
PPPoE Session ID :	0
PPPoE Session Uptime :	00:00:00
PPPoE Session Idle Time :	00:00:00
PPPoE Session MTU :	0
Primary DNS Address :	0.0.0.0
Secondary DNS Address :	0.0.0.0
PPPoE Control Bytes Sent :	168
PPPoE Control Bytes Received :	0
PPPoE Data Session Bytes Sent :	0
PPPoE Data Session Bytes Received :	0

Table 29 PPPoE Statistics tab of the SM

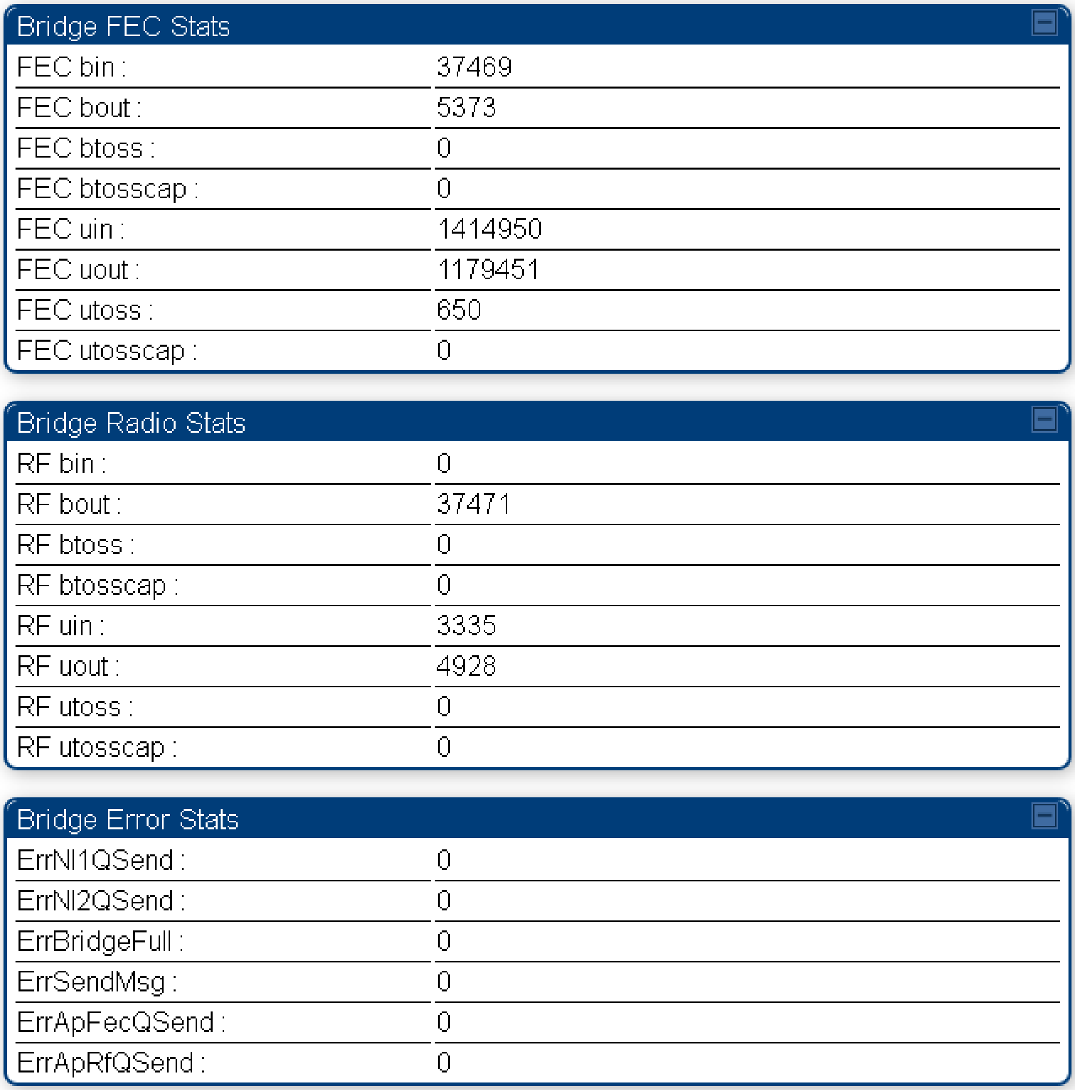
Attribute	Meaning
IP address	This field displays the IP address of the PPPoE session initiator (situated below the SM)
PPPoE Session Status	This field displays the operational status of the PPPoE Session
PPPoE AC Name	This field displays the access concentrator name used in the PPPoE session
PPPoE Service Name	This field displays the PPPoE service name associated with the PPPoE server in use
PPPoE Session ID	This field displays the current PPPoE session ID
PPPoE Session Uptime	This field displays the total session uptime for the PPPoE session
PPPoE Session Idle Time	This field displays the total idle time for the PPPoE session
PPPoE Session MTU	This field displays the Maximum Transmission Unit configured for the PPPoE session
Primary DNS Address	This field displays the primary DNS server used by the PPPoE session
Secondary DNS Address	This field displays the secondary DNS server used by the PPPoE session

Attribute	Meaning
PPPoE Control Bytes Sent	This field displays the total number of PPPoE session control bytes sent from the SM
PPPoE Control Bytes Received	This field displays the total number of PPPoE session control bytes received by the SM
PPPoE Data Session Bytes Sent	This field displays the total number of PPPoE data session (non-control/non-session management user data) sent by the SM
PPPoE Data Session Bytes Received	This field displays the total number of PPPoE data session (non-control/non-session management user data)

Viewing Bridge Control Block Statistics (All)

The AP and SM Bridge Control Block Statistics tab is shown below:

Figure 35 Bridge Control Block statistics



Bridge FEC Stats

FEC bin :	37469
FEC bout :	5373
FEC btoss :	0
FEC btosscap :	0
FEC uin :	1414950
FEC uout :	1179451
FEC utoss :	650
FEC utosscap :	0

Bridge Radio Stats

RF bin :	0
RF bout :	37471
RF btoss :	0
RF btosscap :	0
RF uin :	3335
RF uout :	4928
RF utoss :	0
RF utosscap :	0

Bridge Error Stats

ErrNI1QSend :	0
ErrNI2QSend :	0
ErrBridgeFull :	0
ErrSendMsg :	0
ErrApFecQSend :	0
ErrApRfQSend :	0

Table 30 Bridge Control Block Statistics attributes

Attribute	Meaning
FEC bin	This field indicates the number of broadcast packets received by the bridge control block on the Ethernet interface
FEC bout	This field indicates the number of broadcast packets sent by the bridge control block on the Ethernet interface

Attribute	Meaning
FEC btoss	This field indicates the number of broadcast packets tossed out by the bridge control block on the Ethernet interface
FEC btosscap	This field indicates the number of broadcast packets tossed out at the Ethernet interface due to MIR cap being exceeded.
FEC uin	This field indicates the number of unicast packets received by the bridge control block on the Ethernet interface
FEC uout	This field indicates the number of unicast packets sent by the bridge control block on the Ethernet interface
FEC utoss	This field indicates the number of unicast packets tossed by the bridge control block on the Ethernet interface
FEC utosscap	This field indicates the number of unicast packets tossed out at the Ethernet interface due to MIR cap being exceeded.
RF bin	This field indicates the number of broadcast packets received by the bridge control block on the radio interface
RF bout	This field indicates the number of broadcast packets sent by the bridge control block on the radio interface
RF btoss	This field indicates the number of broadcast packets tossed by the bridge control block on the radio interface
RF btosscap	This field indicates the number of broadcast packets tossed out at the radio interface due to MIR cap being exceeded.
RF uin	This field indicates the number of unicast packets received by the bridge control block on the radio interface
RF uout	This field indicates the number of unicast packets sent by the bridge control block on the radio interface
RF utoss	This field indicates the number of unicast packets tossed by the bridge control block on the radio interface
RF utosscap	This field indicates the number of unicast packets tossed out at the radio interface due to MIR cap being exceeded.
ErrNI1QSend	This field indicates that a packet which was sourced from the radio network stack interface 1 (Ethernet interface) could not be sent because the radio bridge queue was full. The packet was tossed out.
ErrNI2QSend	This field indicates that a packet which was sourced from the radio network stack interface 2 (RF interface) could not be sent because the radio bridge queue was full. The packet was tossed out.

Attribute	Meaning
ErrBridgeFull	This field indicates the total number of times the bridging table was full and could not accept new entries
ErrApFecQSend	This field indicates that a packet which was received on the Ethernet interface could not be processed because the radio bridge queue was full. The packet was tossed out.
ErrApRfQSend	This field indicates that a packet which was received on the RF interface could not be processed because the radio bridge queue was full. The packet was tossed out.

Chapter 5: Using Tools in the GUI

The AP and SM GUIs provide several tools to analyze the operating environment, system performance, and networking, including:

Using the Spectrum Analyzer Tool

The integrated spectrum analyzer can be very useful as a tool for troubleshooting and RF planning, but is not intended to replicate the accuracy and programmability of a high-end spectrum analyzer, which you may sometime need for other purposes.

⚠ CAUTION

When you enable the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. Scanning mode ends when either you click **Disable** on the Spectrum Analyzer page, or it times out after 15 minutes and returns to operational mode.

For this reason:

do not enable the spectrum analyzer on a module you are connected to via RF. The connection will drop for 15 minutes, and when the connection is re-established no readings will be displayed.

be advised that, if you enable the spectrum analyzer by Ethernet connection, the RF connection to that module drops.

You can use any module to see the frequency and power level of any detectable signal that is within, just above, or just below the frequency band range of the module.

NOTE

Vary the days and times when you analyze the spectrum in an area.
The RF environment can change throughout the day or throughout the week.

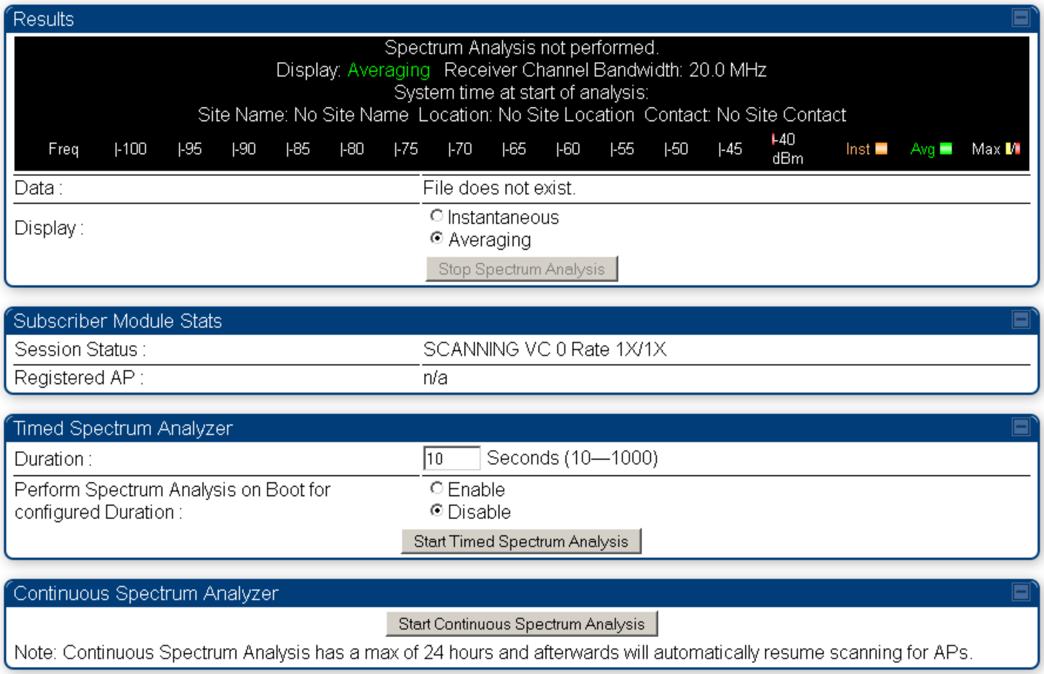
Temporarily deploy an SM for *each* frequency band range that you need to monitor and access the Spectrum Analyzer tab in the Tools web page of the module. To enter the scan mode and view readings, click **Enable**.

After clicking the **Enable** button on the Spectrum Analyzer page, the first "painting" may not display bars for all frequencies, especially on frequency bands with a large number of center channels, like the 5.8 GHz band. Clicking **Enable** again will display the entire spectrum bar graph. Alternatively, you can set the "Auto Refresh" time on the Configuration => General page to a few seconds to have the Spectrum Analyzer automatically fully displayed and refreshed. (Setting the "Auto Refresh" time back to 0 will disable refresh.)

Graphical spectrum analyzer display

The SM displays the graphical spectrum analyzer. An example of the Spectrum Analyzer tab is shown in Figure 36.

Figure 36 Spectrum Analyzer display



Results

Spectrum Analysis not performed.
Display: Averaging Receiver Channel Bandwidth: 20.0 MHz
System time at start of analysis:
Site Name: No Site Name Location: No Site Location Contact: No Site Contact

Freq |-100 |-95 |-90 |-85 |-80 |-75 |-70 |-65 |-60 |-55 |-50 |-45 |-40 dBm
Inst
Avg
Max

Data :	File does not exist.
Display :	○ Instantaneous ● Averaging

Stop Spectrum Analysis

Subscriber Module Stats

Session Status :	SCANNING VC 0 Rate 1X/1X
Registered AP :	n/a

Timed Spectrum Analyzer

Duration :	10 Seconds (10—1000)
Perform Spectrum Analysis on Boot for configured Duration :	○ Enable ● Disable

Start Timed Spectrum Analysis

Continuous Spectrum Analyzer

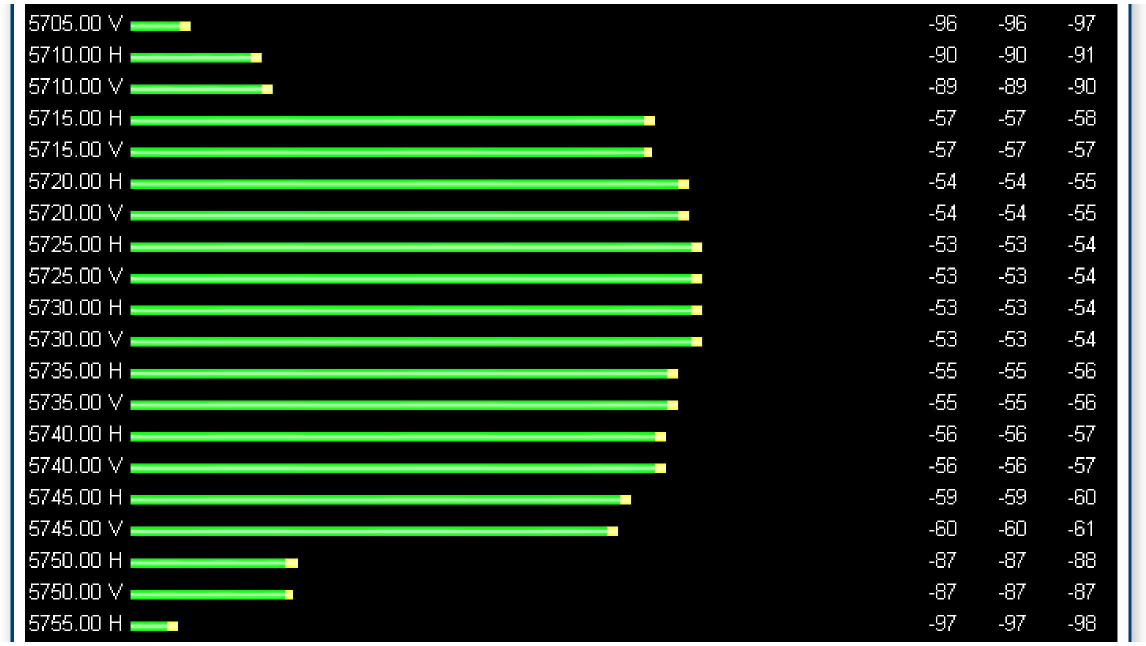
Start Continuous Spectrum Analysis

Note: Continuous Spectrum Analysis has a max of 24 hours and afterwards will automatically resume scanning for APs.

NOTE

Enabling "Perform Spectrum Analysis on Boot for configured Duration" will increase SM registration time by the amount of seconds specified for the SM to scan the spectrum upon boot.

Figure 37 Spectrum analyzer results



```
5705.00 V    -96  -96  -97
5710.00 H    -90  -90  -91
5710.00 V    -89  -89  -90
5715.00 H    -57  -57  -58
5715.00 V    -57  -57  -57
5720.00 H    -54  -54  -55
5720.00 V    -54  -54  -55
5725.00 H    -53  -53  -54
5725.00 V    -53  -53  -54
5730.00 H    -53  -53  -54
5730.00 V    -53  -53  -54
5735.00 H    -55  -55  -56
5735.00 V    -55  -55  -56
5740.00 H    -56  -56  -57
5740.00 V    -56  -56  -57
5745.00 H    -59  -59  -60
5745.00 V    -60  -60  -61
5750.00 H    -87  -87  -88
5750.00 V    -87  -87  -87
5755.00 H    -97  -97  -98
```

Colors in the display have the following meanings:

- Green bars show the most recent measurements.
- Yellow ticks show the maximum measurements from the current spectrum analysis session.
- Red ticks show measurements of −40 dBm or stronger.

To keep the displayed data current, either set "Auto Refresh" on the module's Configuration => General page to a few seconds, or repeatedly click the **Enable** button. When you are finished analyzing the spectrum, click the **Disable** button to return the module to normal operation.

Using the AP as a Spectrum Analyzer

You can temporarily change an AP into an SM and thereby use the spectrum analyzer functionality. This is the only purpose supported for the transformation.

⚠ CAUTION

When you change an AP into an SM, any connections to SMs off that AP are lost. Therefore, you should ensure you are connected to the AP through its *Ethernet* side (not RF side) before changing it into an SM.

If you are connected to an AP through one of its SMs and mistakenly change the AP into an SM, you will lose connectivity and will need to gain access to the Ethernet side of the AP through another part of your network to change it back into an AP.

To transform a VLAN-disabled AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 3 Converting a VLAN-disabled AP to an SM for spectrum analysis

1. Connect to the wired Ethernet interface of the AP.
2. Access the General tab of the Configuration page in the AP.
3. Set the **Device Setting** parameter to **SM**.
4. Click the **Save Changes** button.
5. Click the **Reboot** button.
6. When the module has rebooted as an SM, click the Tools navigation link on the left side of the Home page.
7. Click the Spectrum Analyzer tab.
   NOTE: If you simply click the **Enable** button on the Spectrum Analyzer tab, the display may include fewer than all frequencies that are detectable, especially in a band, such as 5.8 GHz, where the number of available center channels is great. If you then click the **Enable** button a second time or set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds, the display includes the entire spectrum. You can later reset **Webpage Auto Update** to `0`, to disable refresh.
8. Either set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds or repeatedly click the **Enable** button.
   RESULT: The module enters the scan mode.
9. When you are finished analyzing the spectrum, click the **Disable** button.
10. In the left-side navigation links, click Configuration.
11. Click the General tab.
12. Set the **Device Setting** parameter to **AP**.
13. Click the **Save Changes** button.
14. Click the **Reboot** button.
    RESULT: The AP boots with its previous frequency setting.

If you reboot an AP that has a configured **Management VID** parameter and **Device Type** parameter set to **SM**, you are automatically removing the AP from the Management VLAN. The following procedure enables you to successfully analyze the spectrum and return to management via the VLAN feature. In many cases, it is advisable to use this procedure to

- transform all APs in a cluster into SMs.
- perform spectrum analysis without Management VLAN, one sector at a time.
- return all APs in the cluster to their Management VLAN for access.

To transform a VLAN-enabled AP into an SM for spectrum analysis and then return the device to an AP, perform the following steps.

Procedure 4 Transforming a VLAN-enabled AP into an SM for spectrum analysis

1 Access the VLAN-enabled AP through its Management VLAN.
NOTE: How you do this depends on your local configuration.

2 Access the General tab of the Configuration page in the AP.

3 Set the **Device Setting** parameter to **SM**.

4 Click the **Save Changes** button.

5 Click the **Reboot** button.
RESULT: Connectivity to the module is lost.

6 Access the module without using the Management VLAN.
NOTE: How you do this depends on your local configuration. You may need to connect to a different, non-tagging port of the VLAN switch in your NOC.

7 Click the Tools navigation link on the left side of the Home page.

8 Click the Spectrum Analyzer tab.
NOTE: If you simply click the **Enable** button on the Spectrum Analyzer tab, the display may include fewer than all frequencies that are detectable, especially in a band, such as 5.8 GHz, where the number of available center channels is great. If you then click the **Enable** button a second time or set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds, then the display will include the entire spectrum.

9 Either set the **Webpage Auto Update** parameter in the Configuration => General tab to a few seconds or repeatedly click the **Enable** button.
RESULT: The module enters the scan mode.

10 When you are finished analyzing the spectrum, click the **Disable** button.

11 In the left-side navigation links, click Configuration.

12 Click the General tab.

13 Set the **Device Setting** parameter to AP.

14 Click the **Save Changes** button.

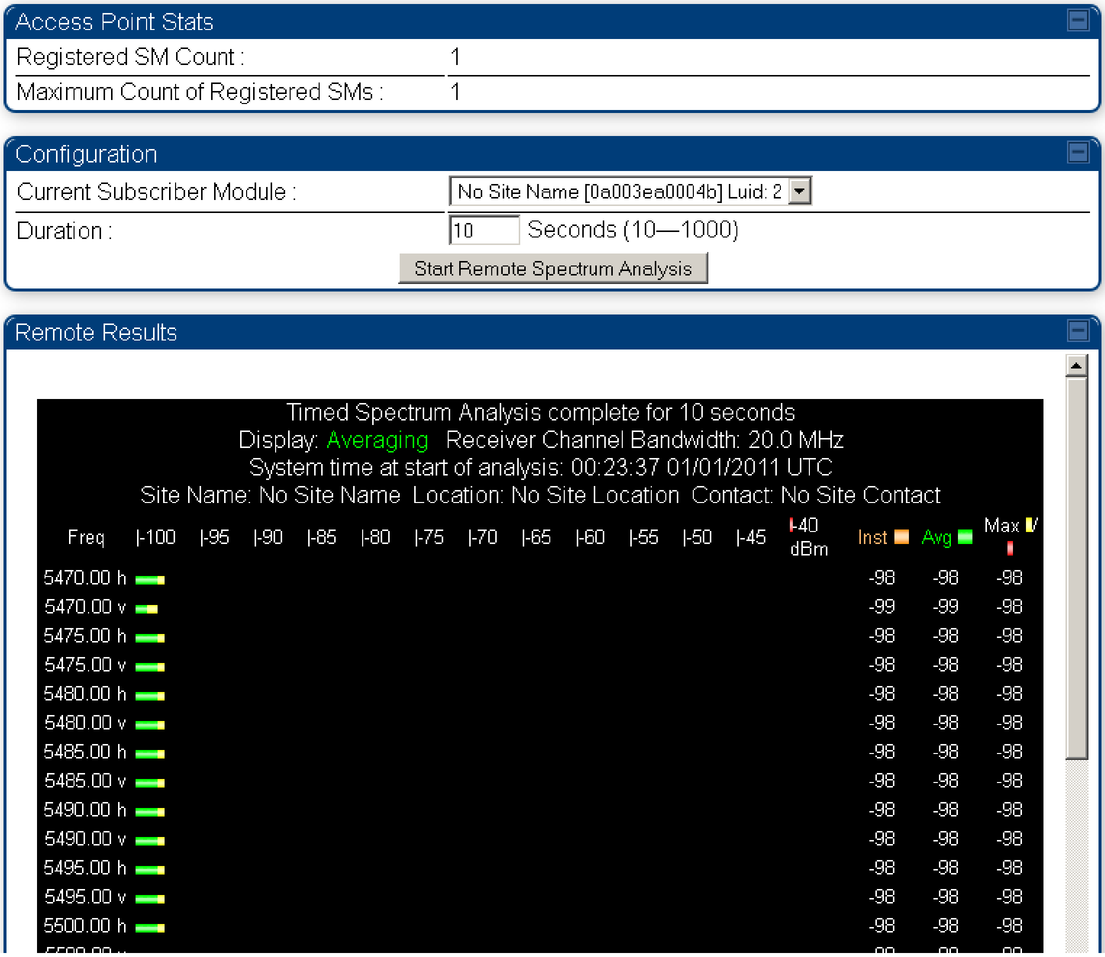
15 Click the **Reboot** button.
RESULT: Connectivity to the module is lost.

16 Access the AP through its Management VLAN.
NOTE: How you do this depends on your local configuration. You may need to connect to the appropriate tagging port of the VLAN switch in your NOC.

Using the Remote Spectrum Analyzer Tool (AP)

The Remote Spectrum Analyzer tool in the AP provides additional flexibility in the use of the spectrum analyzer in the SM. You can set a duration of 10 to 1000 seconds and select an SM from the drop-down list, then click the **Start Remote Spectrum Analysis** button to launch the analysis from that SM.

Figure 38 Remote Spectrum Analyzer tab of the AP



Access Point Stats

Registered SM Count :	1
Maximum Count of Registered SMs :	1

Configuration

Current Subscriber Module :	No Site Name [0a003ea0004b] Luid: 2
Duration :	10 Seconds (10—1000)

Remote Results

```
Timed Spectrum Analysis complete for 10 seconds
Display: Averaging   Receiver Channel Bandwidth: 20.0 MHz
System time at start of analysis: 00:23:37 01/01/2011 UTC
Site Name: No Site Name  Location: No Site Location  Contact: No Site Contact

Freq       |-100 |-95 |-90 |-85 |-80 |-75 |-70 |-65 |-60 |-55 |-50 |-45 |-40 dBm   Inst 🟧  Avg 🟩  Max 🟨
5470.00 h                                                                          -98      -98      -98
5470.00 v                                                                          -99      -99      -98
5475.00 h                                                                          -98      -98      -98
5475.00 v                                                                          -98      -98      -98
5480.00 h                                                                          -98      -98      -98
5480.00 v                                                                          -98      -98      -98
5485.00 h                                                                          -98      -98      -98
5485.00 v                                                                          -98      -98      -98
5490.00 h                                                                          -98      -98      -98
5490.00 v                                                                          -98      -98      -98
5495.00 h                                                                          -98      -98      -98
5495.00 v                                                                          -98      -98      -98
5500.00 h                                                                          -98      -98      -98
```

This feature proceeds in the following sequence:

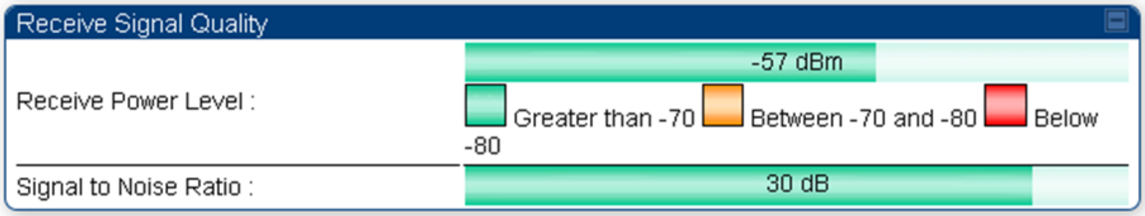
1. The AP de-registers the target SM.
2. The SM scans (for the duration set in the AP tool) to collect data for the bar graph.
3. The SM re-registers to the AP.
4. The AP displays the bar graph.

The bar graph is an HTML file, but can be changed to an XML file, which is then easy to analyze through the use of scripts that you may write for parsing the data. To transform the file to XML, click the "SpectrumAnalysis.xml" link below the spectrum results. Although the resulting display appears mostly unchanged, the bar graph is now coded in XML. You can now right-click on the bar graph for a **Save Target As** option to save the `Spectrum Analysis.xml` file.

Using the Alignment Tool (SM)

The SM's Alignment Tool may be used to maximize Receive Power Level and Signal to Noise Ratio to ensure a stable link. The Tool provides color coded readings to facilitate in judging link quality.

Figure 39 Alignment Tool of SM, good link example

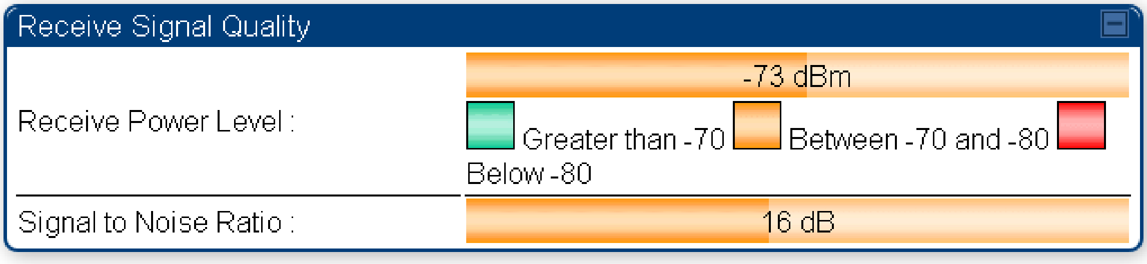


Receive Signal Quality

Receive Power Level : -57 dBm
🟩 Greater than -70 🟧 Between -70 and -80 🟥 Below -80

Signal to Noise Ratio : 30 dB

Figure 40 Alignment Tool tab of SM, acceptable link example

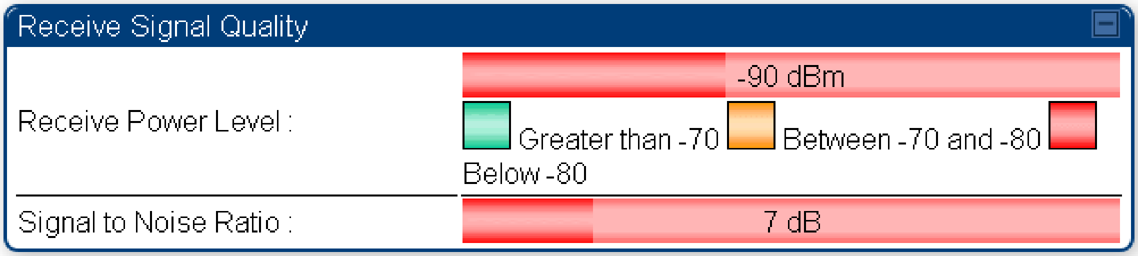


Receive Signal Quality

Receive Power Level : -73 dBm
🟩 Greater than -70 🟧 Between -70 and -80 🟥 Below -80

Signal to Noise Ratio : 16 dB

Figure 41 Alignment Tool tab of SM, poor RF environment



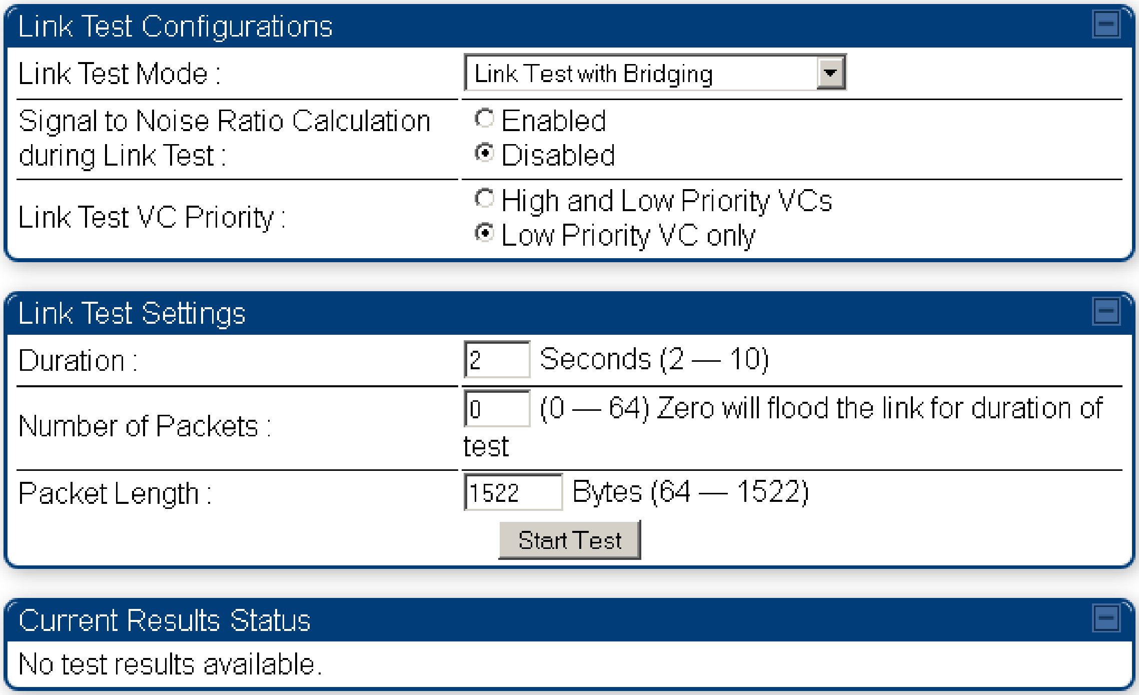
Receive Signal Quality

Receive Power Level :	-90 dBm 🟩 Greater than -70 🟧 Between -70 and -80 🟥 Below -80
Signal to Noise Ratio :	7 dB

Using the Link Capacity Test Tool (AP or SM)

The Link Capacity Test page allows you to measure the throughput and efficiency of the RF link between two modules. Many factors, including packet length, affect throughput. The Link Capacity Test tab contains the settable parameter **Packet Length** with a range of 64 to 1522 bytes. This allows you to compare throughput levels that result from various packet sizes.

Figure 42 Link Capacity Test tab of the AP



Link Test Configurations

Link Test Mode :	Link Test with Bridging
Signal to Noise Ratio Calculation during Link Test :	○ Enabled ● Disabled
Link Test VC Priority :	○ High and Low Priority VCs ● Low Priority VC only

Link Test Settings

Duration :	2 Seconds (2 — 10)
Number of Packets :	0 (0 — 64) Zero will flood the link for duration of test
Packet Length :	1522 Bytes (64 — 1522)

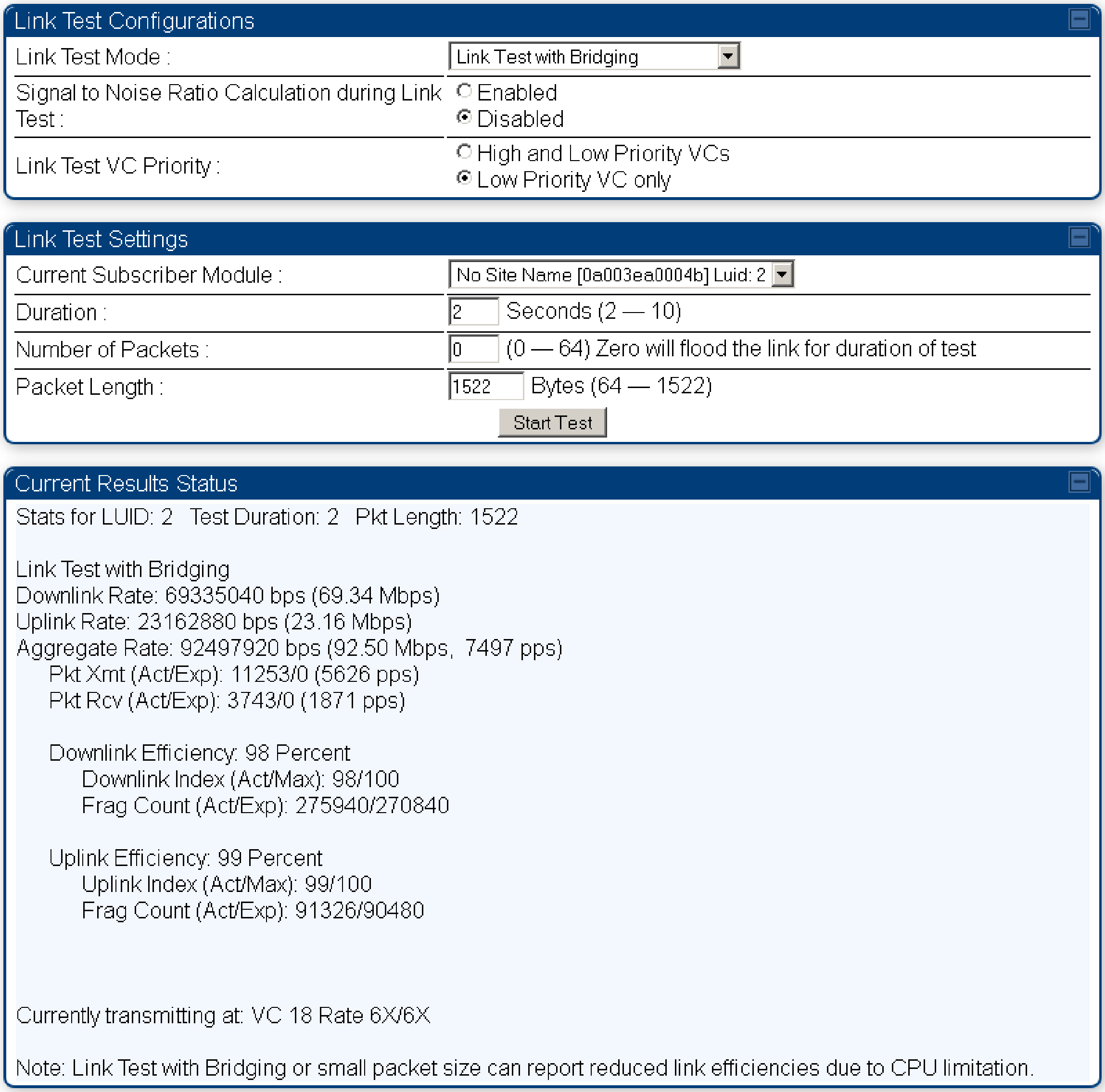
Current Results Status

No test results available.

Table 31 Link Capacity Test tab attributes

Attribute	Meaning
Link Test Mode	• RF Link Test: Fully tests radio-to-radio communication, but does not bridge traffic. • Link Test with Bridging: Bridges traffic to "simulated" Ethernet ports, providing a status of the bridged link. • Link Test with Bridging and MIR: Bridges traffic during the test but also adheres to any MIR (Maximum Information Rate) settings for the link. NOTE This mode setting must be equal on both the AP and the SM when running the link test for proper bridging and MIR handling.
Signal to Noise Ratio Calculation during Link Test	Enable this attribute to display Signal-to-Noise information for the downlink and uplink when running the link test.
Link Test VC Priority	This attribute may be used to enable/disable usage of the high priority virtual channel during the link test.
Current Subscriber Module	The SM with which the Link Capacity Test will be run.
Number of Packets	The total number of packets to send during the Link Capacity Test. When Link Test Mode is set to **RF Link Test** this field is not configurable.
Packet Length	The size of the packets in Bytes to send during the Link Capacity Test

Figure 43 Link Capacity Test tab with 1522-byte packet length



Link Test Configurations

Link Test Mode :	Link Test with Bridging
Signal to Noise Ratio Calculation during Link Test :	○ Enabled ● Disabled
Link Test VC Priority :	○ High and Low Priority VCs ● Low Priority VC only

Link Test Settings

Current Subscriber Module :	No Site Name [0a003ea0004b] Luid: 2
Duration :	2 Seconds (2 — 10)
Number of Packets :	0 (0 — 64) Zero will flood the link for duration of test
Packet Length :	1522 Bytes (64 — 1522)

Current Results Status

```
Stats for LUID: 2   Test Duration: 2   Pkt Length: 1522

Link Test with Bridging
Downlink Rate: 69335040 bps (69.34 Mbps)
Uplink Rate: 23162880 bps (23.16 Mbps)
Aggregate Rate: 92497920 bps (92.50 Mbps,  7497 pps)
    Pkt Xmt (Act/Exp): 11253/0 (5626 pps)
    Pkt Rcv (Act/Exp): 3743/0 (1871 pps)

    Downlink Efficiency: 98 Percent
        Downlink Index (Act/Max): 98/100
        Frag Count (Act/Exp): 275940/270840

    Uplink Efficiency: 99 Percent
        Uplink Index (Act/Max): 99/100
        Frag Count (Act/Exp): 91326/90480


Currently transmitting at: VC 18 Rate 6X/6X

Note: Link Test with Bridging or small packet size can report reduced link efficiencies due to CPU limitation.
```

To run a simple link capacity test that floods the link with 1522 byte packets for 10 seconds, perform the following procedure:

Procedure 5 Performing a simple Link Capacity Test

1 Access the Link Capacity Test tab in the Tools web page of the module.

2 Select Link Test Mode **Link Test with Bridging**

3 Select the subscriber module to test using the Current Subscriber Module parameter.

4 Type into the **Duration** field how long (in seconds) the RF link should be tested.

5 Type into the **Number of Packets** field a value of **0** to flood the link for the duration of the test.

6 Type into the **Packet Length** field a value of **1522** to send 1522-byte packets during the test.

7 Click the **Start Test** button.

8 In the Current Results Status block of this tab, view the results of the test.

\

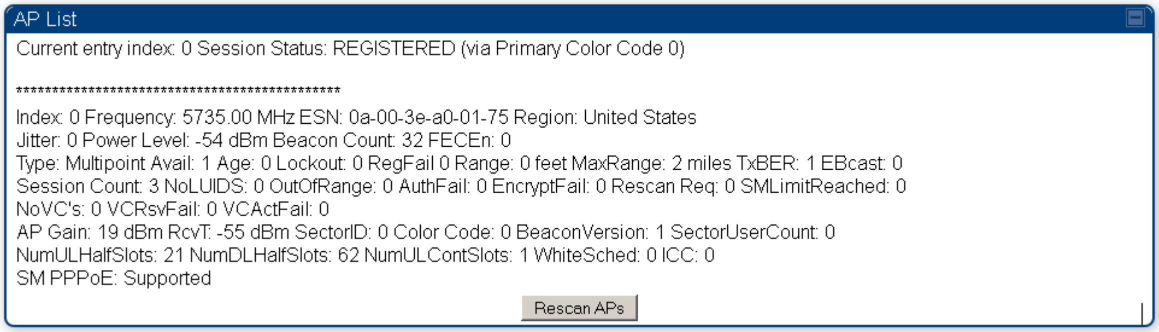
Using the AP Evaluation Tool (SM)

The AP Evaluation tab in the Tools web page of the SM provides information about the AP that the SM sees.

NOTE

The data for this page may be suppressed by the **SM Display of AP Evaluation Data** setting in the Configuration => Security tab of the AP.

Figure 44 AP Evaluation tab of SM



AP List

```
Current entry index: 0 Session Status: REGISTERED (via Primary Color Code 0)

************************************************
Index: 0 Frequency: 5735.00 MHz ESN: 0a-00-3e-a0-01-75 Region: United States
Jitter: 0 Power Level: -54 dBm Beacon Count: 32 FECEn: 0
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0 Range: 0 feet MaxRange: 2 miles TxBER: 1 EBcast: 0
Session Count: 3 NoLUIDS: 0 OutOfRange: 0 AuthFail: 0 EncryptFail: 0 Rescan Req: 0 SMLimitReached: 0
NoVC's: 0 VCRsvFail: 0 VCActFail: 0
AP Gain: 19 dBm RcvT: -55 dBm SectorID: 0 Color Code: 0 BeaconVersion: 1 SectorUserCount: 0
NumULHalfSlots: 21 NumDLHalfSlots: 62 NumULContSlots: 1 WhiteSched: 0 ICC: 0
SM PPPoE: Supported
```

The AP Evaluation tab provides the following fields that can be useful to manage and troubleshoot a system:

Table 32 AP Evaluation tab attributes

Attribute	Meaning
Index	This field displays the index value that the system assigns (for only this page) to the AP where this SM is registered.
Frequency	This field displays the frequency that the AP transmits.
ESN	This field displays the MAC address (electronic serial number) of the AP. For operator convenience during SM aiming, this tab retains each detected ESN for up to 15 minutes. If the broadcast frequency of a detected AP changes during a 15-minute interval in the aiming operation, then a multiple instance of the same ESN is possible in the list. Eventually, the earlier instance expires and disappears, and the later instance remains to the end of its interval, but you can ignore the early instance(s) whenever two or more are present.
Region	This field displays the AP's configured Region Code setting.
Power Level	This field displays the SM's received power level from the AP's transmission.
Beacon Count	A count of the beacons seen in a given time period.
FECEn	This field contains the SNMP value from the AP that indicates whether the Forward Error Correction feature is enabled. 0: FEC is disabled 1: FEC is enabled
Type	Multipoint indicates that the listing is for an AP.
Age	This is a counter for the number of minutes that the AP has been inactive. At 15 minutes of inactivity for the AP, this field is removed from the AP Evaluation tab in the SM.
Lockout	This field displays how many times the SM has been temporarily locked out of making registration attempts.
RegFail	This field displays how many registration attempts by this SM failed.
Range	This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.
MaxRange	
TxBER	A 1 in this field indicates the AP is sending Radio BER.

Attribute	Meaning
EBcast	A 1 in this field indicates the AP or BHM is encrypting broadcast packets. A 0 indicates it is not.
Session Count	This field displays how many sessions the SM (or BHS) has had with the AP (or BHM). Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum. In the case of a multipoint link, if the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.
NoLUIDs	This field indicates how many times the AP has needed to reject a registration request from an SM because its capacity to make LUID assignments is full. This then locks the SM out of making any valid attempt for the next 15 minutes. It is extremely unlikely that a non-zero number would be displayed here.
OutOfRange	This field indicates how many times the AP has rejected a registration request from an SM because the SM is a further distance away than the range that is currently configured in the AP. This then locks the SM out of making any valid attempt for the next 15 minutes.
AuthFail	This field displays how many times authentication attempts from this SM have failed in the AP.
EncryptFail	This field displays how many times an encryption mismatch has occurred between the SM and the AP.
Rescan Req	This field displays how many times a re-range request has occurred for the BHM that is being evaluated in the AP Eval page of a BHS.
SMLimitReached	This field displays 0 if additional SMs may be registered to the AP. If a 1 is displayed, the AP will not accept additional SM registrations.
NoVC's	This counter is incremented when the SM is registering to an AP which determines that no VC resources are available for allocation. This could be a primary data VC or a high priority data VC.
VCRsvFail	This counter is incremented when the SM is registering to an AP which has a VC resource available for allocation but cannot reserve the resource for allocation.
VCActFail	This counter is incremented when the SM is registering to an AP which has a VC resource available for allocation and has reserved the VC, but cannot activate the resource for allocation.

Attribute	Meaning
AP Gain	This field displays the total external gain (antenna) used by the AP.
RcvT	This field displays the AP's configured receive target for receiving SM transmissions (this field affects automatic SM power adjust).
Sector ID	This field displays the value of the **Sector ID** field that is provisioned for the AP.
Color Code	This field displays the value of the **Color Code** field that is provisioned for the AP.
BeaconVersion	This field indicates that the beacon is OFDM (value of 1).
Sector User Count	This field displays how many SMs are registered on the AP.
NumULHalfSlots	This is the number of uplink half slots in the frame for this AP. To find the number of slots, divide by 2.
NumDLHalfSlots	This is the number of downlink half slots in the frame for this. To find the number of slots, divide by 2.
NumULContSlots	This field displays how many control slots are being used in the uplink portion of the frame. The AP Evaluation tab also provides the following buttons.
PtoP VLAN	This field indicates whether VLAN is supported in the backhaul module.
Rescan APs	You can click this button to force the SM to rescan the frequencies that are selected in the Radio tab of the Configuration page.

Using the OFDM Frame Calculator Tool for Collocation (AP or SM)

The first step to avoid interference in wireless systems is to set all APs to receive timing from CMMs or UGPS units. This ensures that the modules are in sync and start transmitting at the same time each frame.

The second step to avoid interference is to configure parameters on all APs of the same frequency band in proximity such that they have compatible transmit/receive ratios (all stop transmitting each frame before any start receiving). This avoids the problem of one AP attempting to receive the signal from a distant SM while a nearby AP transmits, which could overpower that signal.

The following parameters on the AP determine the transmit/receive ratio:

- Max Range
- Downlink Data percentage
- (reserved) Control Slots

If OFDM (PMP 430, PMP 450, PTP 230) and FSK (PMP 1x0) APs of the same frequency band are in proximity, or if you want APs set to different parameters (differing in their Max Range values, for example), then you should use the Frame Calculator to identify compatible settings.

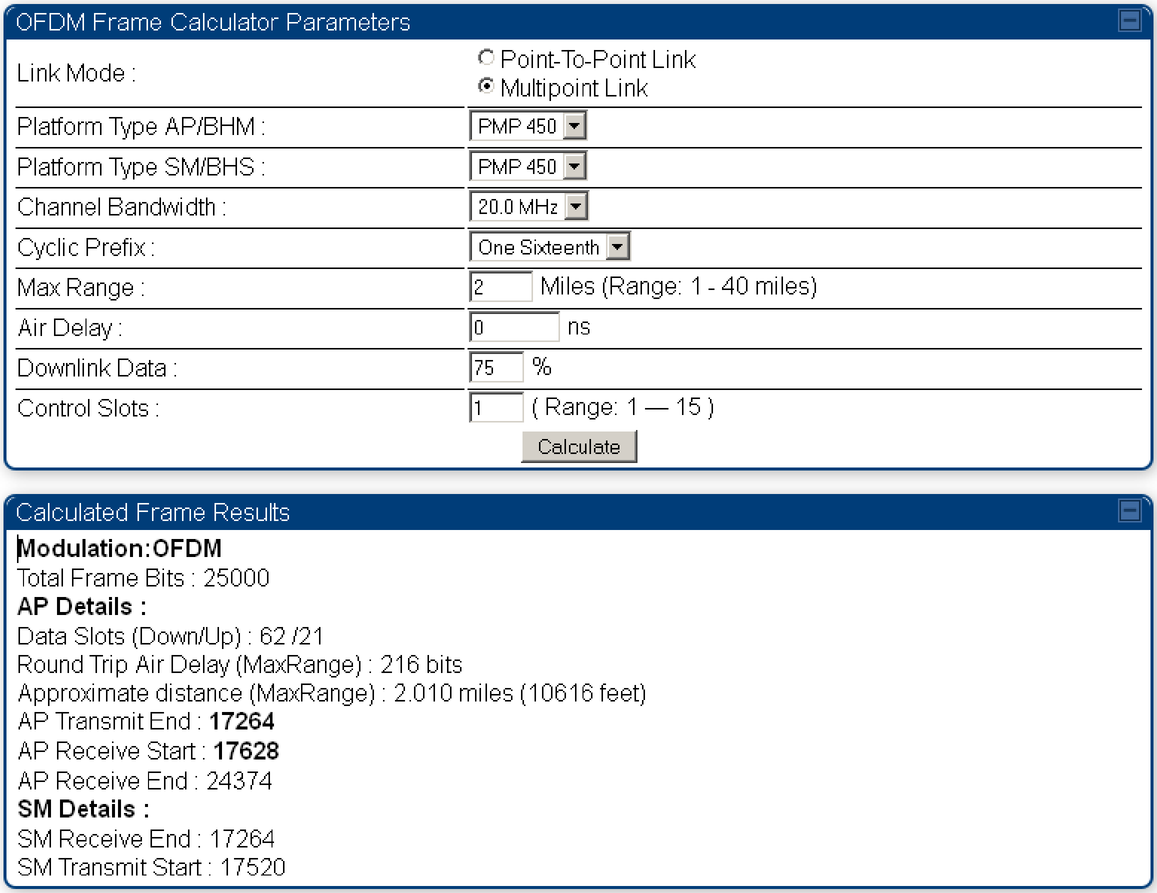
The frame calculator is available on the Frame Calculator tab of the Tools web page. To use the Frame Calculator, type into the calculator various configurable parameter values for each proximal AP, and then record the resulting **AP Receive Start** value. Next vary the **Downlink Data** percentage in each calculation and iterate until the calculated **AP Receive Start** for all collocated APs are within 300 bit times; if possible, within 150 bit times.

The calculator *does not* use values in the module or populate its parameters. It is merely a convenience application that runs on a module. For this reason, you can use any FSK module (AP, SM, BHM, BHS) to perform FSK frame calculations for setting the parameters on an FSK AP and any OFDM module (AP, SM, BHM, BHS) to perform OFDM frame calculations for setting the parameters on an OFDM AP.

IMPORTANT!

APs that have slightly mismatched transmit-to-receive ratios and low levels of data traffic may see little effect on throughput. A system that was not tuned for collocation may work fine at low traffic levels, but encounter problems at higher traffic levels. The conservative practice is to tune for collocation before traffic ultimately increases. This prevents problems that occur as sectors are built.

Figure 45 OFDM Frame Calculator tab



OFDM Frame Calculator Parameters

Link Mode :	○ Point-To-Point Link ● Multipoint Link
Platform Type AP/BHM :	PMP 450
Platform Type SM/BHS :	PMP 450
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	One Sixteenth
Max Range :	2 Miles (Range: 1 - 40 miles)
Air Delay :	0 ns
Downlink Data :	75 %
Control Slots :	1 (Range: 1 — 15)

Calculated Frame Results

Modulation:OFDM
Total Frame Bits : 25000
AP Details :
Data Slots (Down/Up) : 62 /21
Round Trip Air Delay (MaxRange) : 216 bits
Approximate distance (MaxRange) : 2.010 miles (10616 feet)
AP Transmit End : **17264**
AP Receive Start : **17628**
AP Receive End : 24374
SM Details :
SM Receive End : 17264
SM Transmit Start : 17520

In the Frame Calculator tab, you may set the following parameters.

Table 33 OFDM Frame Calculator tab attributes

Attribute	Meaning
Link Mode	For AP to SM frame calculations, select **Multipoint Link**
Platform Type AP/BHM	Use the drop-down list to select the hardware series (board type) of the AP.
Platform Type SM/BHS	Use the drop-down list to select the hardware series (board type) of the SM.
Channel Bandwidth	Set this to the channel bandwidth used in the AP.
Cyclic Prefix	Set this to the cyclic prefix used in the AP.
Max Range	Set to the same value as the **Max Range** parameter is set in the AP(s).
Air Delay	This field should be left at the default of 0 ns.

Attribute	Meaning
Downlink Data	Initially set this parameter to the same value that the AP has for its **Downlink Data** parameter (percentage). Then, as you use the Frame Calculator tool in Procedure 6, you will vary the value in this parameter to find the proper value to write into the **Downlink Data** parameter of all APs in the cluster. PMP 450 Series APs offer a range of 15% to 85%, and default to 75%. The value that you set in this parameter has the following interaction with the value of the **Max Range** parameter (above): • The default **Max Range** value is 5 miles and, at that distance, the maximum **Downlink Data** value (85% in PMP450) is functional.
Control Slots	Set this parameter to the value of the **Control Slot** parameter is set in the APs.

The Calculated Frame Results display several items of interest:

Table 34 OFDM Calculated Frame Results attributes

Attribute	Meaning
Modulation	The type of radio modulation used in the calculation (OFDM for PMP 450)
Total Frame Bits	The total number of bits used in the calculated frames
Data Slots (Down/Up)	A result within the typical range is 61/21, meaning 61 control (half) slots down and 21 control (half) slots up.
Round Trip Air Delay (MaxRange)	This is the roundtrip air delay in bit times for the **Max Range** value set in the calculator
Approximate distance (MaxRange)	The Max Range value used for frame calculation
AP Transmit End	In bit times, this is the frame position at which the AP ceases transmission.
AP Receive Start	In bit times, this is the frame position at which the AP is ready to receive transmission from the SM.
AP Receive End	In bit times, this is the frame position at which the AP will cease receiving transmission from the SM.
SM Receive End	In bit times, this is the frame position at which the SM will cease receiving transmission from the AP.
SM Transmit Start	In bit times, this is the frame position at which the SM will begin transmission.

To use the Frame Calculator to ensure that all APs are configured to transmit and receive at the same time, follow the procedure below:

Procedure 6 Using the Frame Calculator

1. Populate the OFDM Frame Calculator parameters with appropriate values as described above.
2. Click the **Calculate** button.
3. Scroll down the tab to the Calculated Frame Results section
4. Record the value of the **AP Receive Start** field
5. Enter a parameter set from another AP in the system – for example, an AP in the same cluster that has a higher **Max Range** value configured.
6. Click the **Calculate** button.
7. Scroll down the tab to the Calculated Frame Results section
8. If the recorded values of the **AP Receive Start** fields are within 150 bit times of each other, skip to step 10.
9. If the recorded values of the **AP Receive Start** fields are not within 150 bit times of each other, modify the **Downlink Data** parameter until the calculated results for **AP Receive Start** are within 300 bit time of each other, if possible, 150 bit time.
10. Access the Radio tab in the Configuration web page of each AP in the cluster and change its **Downlink Data** parameter (percentage) to the last value that was used in the Frame Calculator.

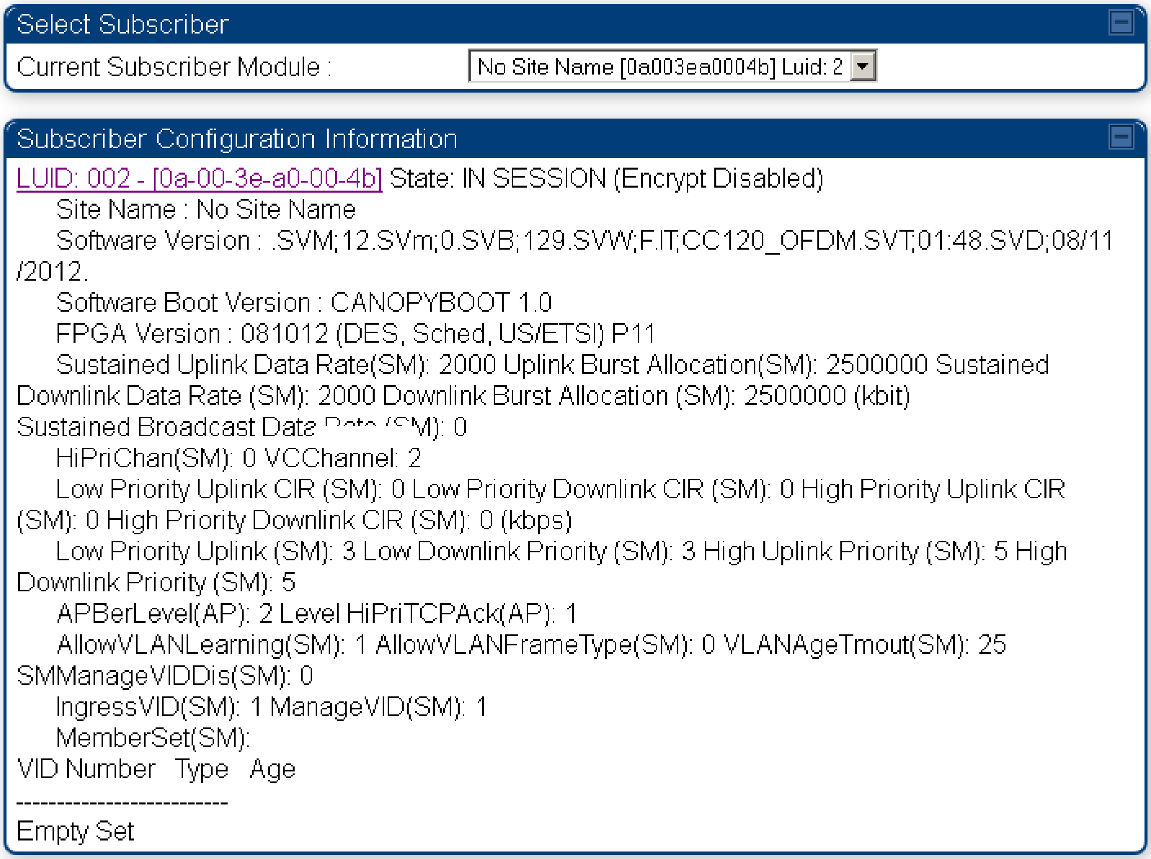
Using the Subscriber Configuration Tool (AP)

The SM Configuration tab in the Tools page of the AP displays:

- the current values whose control may be subject to the setting in the **Configuration Source** parameter.
- an indicator of the source for each value.

This tab may be referenced for information on how the link is behaving based on where the SM is retrieving certain QoS and VLAN parameters.

Figure 46 SM Configuration tab of AP



Select Subscriber

Current Subscriber Module : No Site Name [0a003ea0004b] Luid: 2

Subscriber Configuration Information

LUID: 002 - [0a-00-3e-a0-00-4b] State: IN SESSION (Encrypt Disabled)
Site Name : No Site Name
Software Version : .SVM;12.SVm;0.SVB;129.SVW;F.IT;CC120_OFDM.SVT;01:48.SVD;08/11/2012.
Software Boot Version : CANOPYBOOT 1.0
FPGA Version : 081012 (DES, Sched, US/ETSI) P11
Sustained Uplink Data Rate(SM): 2000 Uplink Burst Allocation(SM): 2500000 Sustained Downlink Data Rate (SM): 2000 Downlink Burst Allocation (SM): 2500000 (kbit)
Sustained Broadcast Data Rate (SM): 0
HiPriChan(SM): 0 VCChannel: 2
Low Priority Uplink CIR (SM): 0 Low Priority Downlink CIR (SM): 0 High Priority Uplink CIR (SM): 0 High Priority Downlink CIR (SM): 0 (kbps)
Low Priority Uplink (SM): 3 Low Downlink Priority (SM): 3 High Uplink Priority (SM): 5 High Downlink Priority (SM): 5
APBerLevel(AP): 2 Level HiPriTCPAck(AP): 1
AllowVLANLearning(SM): 1 AllowVLANFrameType(SM): 0 VLANAgeTmout(SM): 25 SMManageVIDDis(SM): 0
IngressVID(SM): 1 ManageVID(SM): 1
MemberSet(SM):
VID Number Type Age

Empty Set

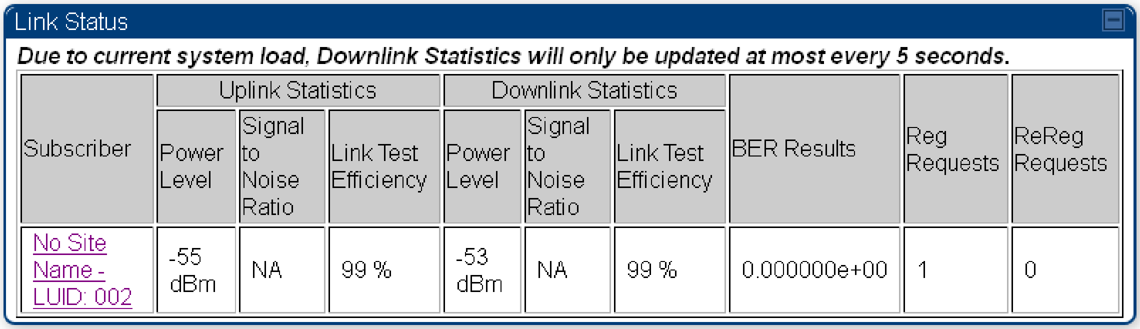
The AP will display one of the following for the configuration source:

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

Reviewing the Link Status Tool Results (AP)

The Link Status Tool displays information about the most-recent Link Test initiated on the SM. Link Tests initiated from the AP are not included in the Link Status table. This table is useful for monitoring link test results for all SMs in the system.

Figure 47 Link Status tab of AP



Link Status

Due to current system load, Downlink Statistics will only be updated at most every 5 seconds.

Subscriber	Uplink Statistics			Downlink Statistics			BER Results	Reg Requests	ReReg Requests
	Power Level	Signal to Noise Ratio	Link Test Efficiency	Power Level	Signal to Noise Ratio	Link Test Efficiency			
No Site Name - LUID: 002	-55 dBm	NA	99 %	-53 dBm	NA	99 %	0.000000e+00	1	0

The Link Status tool results include values for the following fields.

Table 35 OFDM Calculated Frame Results attributes

Attribute	Meaning
Uplink Statistics - Power Level	This field represents the received power level at the AP.
Uplink Statistics – Signal to Noise Ratio	This field represents the signal to noise ratio for the uplink (displayed when parameter Signal to Noise Ratio Calculation during Link Test is enabled)
Uplink Statistics – Link Test Efficiency	This field displays the efficiency of the radio link, expressed as a percentage, for the radio uplink.
Downlink Statistics – Power Level	This field represents the received power level at the SM.
Downlink Statistics – Signal to Noise Ratio	This field represents the signal to noise ratio for the downlink (displayed when parameter Signal to Noise Ratio Calculation during Link Test is enabled)
Downlink Statistics – Link Test Efficiency	This field displays the efficiency of the radio link, expressed as a percentage, for the radio downlink.

BER Results	This field displays the over-the-air Bit Error Rates for each downlink. (The ARQ [Automatic Resend reQuest] ensures that the transport BER [the BER seen end-to-end through a network] is essentially zero.) The level of acceptable over-the-air BER varies, based on operating requirements, but a reasonable value for a good link is a BER of 1e-4 (1 x 10^{-4}) or better, approximately a packet resend rate of 5%. BER is generated using unused bits in the downlink. During periods of peak load, BER data is not updated as often, because the system puts priority on transport rather than on BER calculation.
Reg Requests	A Reg Requests count is the number of times the SM registered after the AP determined that the link had been down. If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).
ReReg Requests	A ReReg Requests count is the number of times the AP received an SM registration request while the AP considered the link to be still up (and therefore did not expect registration requests). If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).

Using the BER Results Tool (SM)

Radio BER data represents bit errors at the RF link level. Due to CRC checks on fragments and packets and ARQ (Automatic Repeat reQuest), the BER of customer data is essentially zero. Radio BER gives one indication of link quality. Other important indications to consider include the received power level, signal to noise ratio, and link tests.

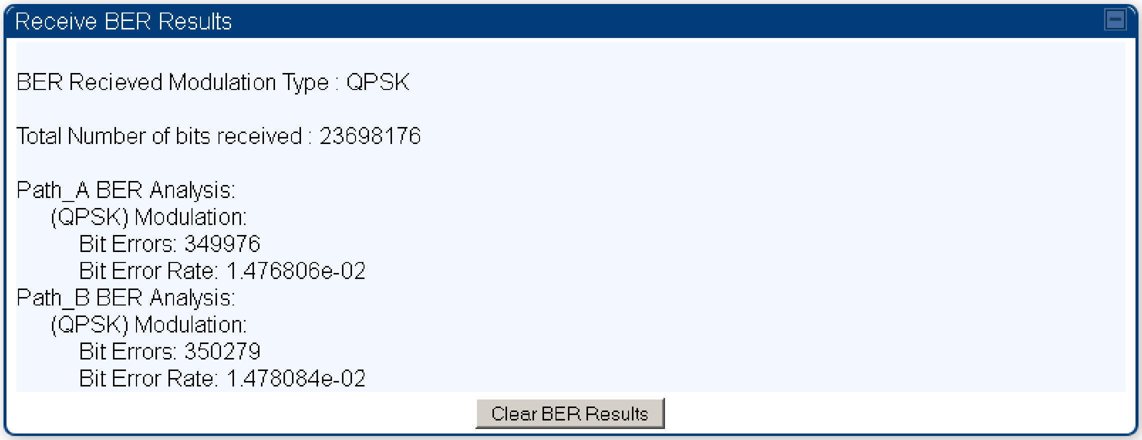
BER is only instrumented on the downlink and is displayed on the BER Results tab of the Tools page in any SM. Each time the tab is clicked, the current results are read, and counters are reset to zero.

The BER Results tab can be helpful in troubleshooting poor link performance.

The link is acceptable if the value of this field is less than 10^{-4}. If the BER is greater than 10^{-4}, re-evaluate the installation of both modules in the link.

The BER test signal is broadcast by the AP (and compared to the expected test signal by the SM) only when capacity in the sector allows it. This signal is the lowest priority for AP transmissions.

Figure 48 BER Results tab of the SM



Receive BER Results

BER Recieved Modulation Type : QPSK

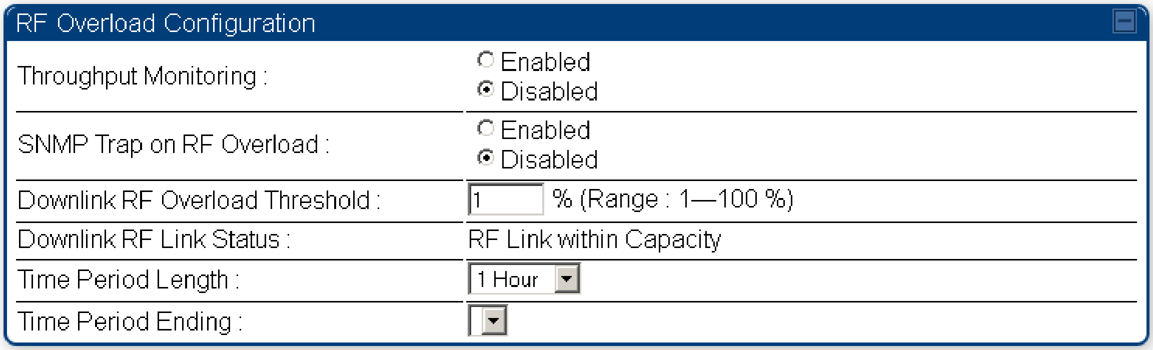
Total Number of bits received : 23698176

```
Path_A BER Analysis:
    (QPSK) Modulation:
        Bit Errors: 349976
        Bit Error Rate: 1.476806e-02
Path_B BER Analysis:
    (QPSK) Modulation:
        Bit Errors: 350279
        Bit Error Rate: 1.478084e-02
```

Using the Throughput Monitoring Tool (AP)

The PMP 450 AP has a tab **Throughput** under the **Statistics** category which shows historical information about sector throughput and packet discards. This information can be useful to identify an overloaded sector or heavy bandwidth users. This page also shows the user throughput in terms of data rate (kbps) and packet rate (packets per second, or PPS), as well as the average packet size during the sample period. Operators may set the AP to send an SNMP trap when it detects an RF overload condition based on a configurable threshold.

Figure 49 Throughput tab of the AP



RF Overload Configuration

Throughput Monitoring :	○ Enabled ● Disabled
SNMP Trap on RF Overload :	○ Enabled ● Disabled
Downlink RF Overload Threshold :	1 % (Range : 1—100 %)
Downlink RF Link Status :	RF Link within Capacity
Time Period Length :	1 Hour
Time Period Ending :	

The following configuration parameters are available on the Throughput tab GUI pane, and a radio reboot is not required when configuring these parameters:

Table 36 Congested AP Indicator attributes

Attribute	**Meaning**
Throughput Monitoring	This enables or disables the monitoring of sector throughput and packet discards. This parameter is disabled by default.
SNMP Trap on RF Overload	This enables or disables the sending of an SNMP trap when an AP overload condition is reached (based on Downlink RF Overload Threshold).
Downlink RF Overload Threshold	This parameter determines the overload threshold in percent of packets discarded that triggers the generation of an SNMP trap.
Downlink RF Link Status	This field displays the status of the capacity of the RF link.
Time Period Length Time Period Ending	These two configuration parameters determine what set of collection samples to show on the GUI display. The Time Period Length can be set from one to three hours. Time Period Ending allows the operator to set the end time for the set of collection samples to display.

Below the configuration settings are three tables that display the statistics that are collected.

Board Performance Statistics Table

This table contains a row that corresponds to each 1 minute statistics collection interval. Each row contains the following data aggregated for the entire AP:

- **Ethernet Throughput -** Statistics collected at the Ethernet port:
  - **kbps in** – average throughput over the collection interval in Kbps into the AP on the Ethernet Interface

  - **kbps out** – average throughput over the collection interval in Kbps out of the AP on the Ethernet Interface
  - **PPS in** – average packets per second over the collection interval into the AP on the Ethernet Interface
  - **PPS out** – average packets per second over the collection interval out of the AP on the Ethernet Interface
- **RF Throughput -** Statistics collected at the RF Interface:
  - **kbps in** – average throughput over the collection interval in Kbps into the AP on the RF Interface
  - **kbps out** – average throughput over the collection interval in Kbps out of the AP on the RF Interface
  - **PPS in** – average packets per second over the collection interval into the AP on the RF Interface
  - **PPS out** – average packets per second over the collection interval out of the AP on the RF Interface
- **Aggregate Through Board** – Sum of bidirectional data transferred *through* (not originating or terminating at) the AP:
  - **kbps** – average bidirectional throughput over the collection interval in Kbps
  - **PPS** – average bidirectional packets per second over the collection interval
  - **Ave Pkt Size** – Average Packet size over the collection interval of bidirectional data transferred

Board Throughput Statistics

This table contains a row that corresponds to each one minute statistics collection interval. This table may be used to determine if there are problems with any of the interfaces. For example, if the Ethernet in packets is much higher than the RF out packets it could indicate a denial of service (DoS) attack on the AP. Each row contains the following data aggregated for the entire AP:

- **Ethernet Statistics -** Statistics collected at the Ethernet port:
  - **inOctets** – Number of octets (bytes) received by the AP at the Ethernet Interface over the collection interval
  - **outOctets** – Number of octets (bytes) sent by the AP at the Ethernet Interface over the collection interval
  - **inPkts** – Number of packets received by the AP at the Ethernet Interface over the collection interval
  - **outPkts** – Number of packets sent by the AP at the Ethernet Interface over the collection interval
  - **Discards (in/out)** – Number of packets that had to be discarded by the AP at the respective Ethernet Interface Queue
- **RF Statistics -** Statistics collected at the RF Interface:
  - **inOctets** – Number of octets (bytes) received by the AP at the RF Interface over the collection interval
  - **outOctets** – Number of octets (bytes) sent by the AP at the RF Interface over the collection interval
  - **inPkts** – Number of packets received by the AP at the RF Interface over the collection interval

  - **outPkts** – Number of packets sent by the AP at the RF Interface over the collection interval
  - **Discards (in/out)** – Number of packets that had to be discarded by the AP at the respective RF Interface Queue during the collection interval
  - **Discards % (in/out)** – Percent of the total packets received / transmitted that had to be discarded during the collection interval

LUID RF Throughput Stats

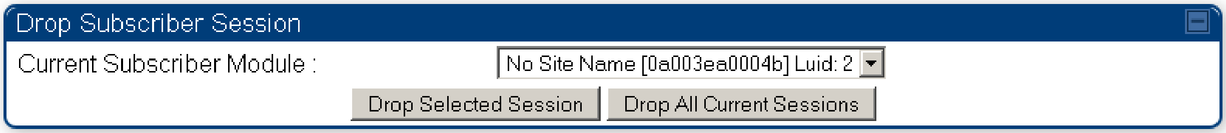
This table contains a row that corresponds to each active LUID served by the AP. Note that an LUID may be assigned 1 or 2 VCs. If the LUID is assigned 2 VCs, then the data in the table is the sum of the activity for both VCs. This table may be used to determine which LUIDs are experiencing overload so that corrective action can be taken (i.e. fixing a poor RF link or moving a heavily loaded link to a less congested AP). Each row contains counters and statistics related to the RF Interface that are updated once per minute:

- **Inbound Statistics** - Statistics collected at the RF Interface for the Uplink:
  - **octets** – Number of octets (bytes) received by the AP at the RF Interface for this LUID over the collection interval
  - **pkts** – Number of packets received by the AP at the RF Interface for this LUID over the collection interval
  - **Ave Pkt Size** – Average size of the packets received by the AP at the RF Interface for this LUID over the collection interval
  - **discards** – Number of packets received by the AP at the RF Interface for this LUID over the collection interval that had to be discarded because the RF In Queue was full
  - **discards %** – Percent of the total packets received by the AP at the RF Interface for this LUID over the collection interval that had to be discarded because the RF In Queue was full
- **Outbound Statistics** - Statistics collected at the RF Interface for the Downlink:
  - **octets** – Number of octets (bytes) transmitted by the AP at the RF Interface for this LUID over the collection interval
  - **pkts** – Number of packets transmitted by the AP at the RF Interface for this LUID over the collection interval
  - **Ave Pkt Size** – Average size of the packets transmitted by the AP at the RF Interface for this LUID over the collection interval
  - **discards** – Number of packets to be transmitted by the Access Point at the RF Interface for this LUID over the collection interval that had to be discarded because the RF Out Queue was full
  - **discards %** – Percent of the total packets to be transmitted by the AP at the RF Interface for this LUID over the collection interval that had to be discarded because the RF Out Queue was full.

Using the Sessions Tool (AP)

The PMP 450 AP has a tab **Sessions** under the Tools category which allows operators to drop one or all selected SM sessions and force an SM re-registration. This operation is useful to force QoS changes for SMs without losing AP logs or statistics. This operation may take at most 5 minutes to regain all SM registrations.

Figure 50 Sessions tab of the AP



Drop Subscriber Session

Current Subscriber Module : No Site Name [0a003ea0004b] Luid: 2

Chapter 6: Maintaining Your Software

Cambium provides release compatibility information and caveats about each release. For the latest information and caveats about each software release, see the release notes available for download from http://www.cambiumnetworks.com/support/pmp/software/index.php.

Typical Contents of Release Notes

Cambium supports each release with software release notes, which include

- description of features that are introduced in the new release.
- issues that the new release resolves.
- known issues and special notes for the new release.
- installation procedures for the new release.

Typical Upgrade Process

In a typical upgrade process, proceed as follows:

Procedure 7 Typical upgrade process

1. Visit http://www.cambiumnetworks.com/support/pmp/software/index.php.
2. Read the compatibility information and any caveats that Cambium associates with the release.
3. Read the software release notes from the web site.
4. On the basis of these, decide whether the release is appropriate for your network.
5. Download the software release and associated files.
6. Use CNUT to manage the upgrade across your network. For detailed software upgrade procedures, see section "Task 3: Upgrading the software version and using CNUT" in the *PMP 450 Configuration and User Guide*.

Rebranding Module Interface Screens

Distinctive fonts indicate

literal user input.
variable user input.
literal system responses.
variable system responses.

The interface screens on each module display the Cambium logo. The logo is a hyperlink, and clicking on it takes the user to the Canopy web site. A different site (perhaps the operator's support site) can be made the destination using the procedures below.

To replace logos and hyperlinks efficiently throughout your network, read the following two procedures, write a script, and execute your script through the Canopy Network Updater Tool (CNUT).[1] To replace them individually, use one of the following two procedures.

Procedure 8 Replacing the Cambium logo on the GUI

1 If the current logo is the Canopy logo, name your custom logo file on your computer canopy.jpg and put it in your home directory.

2 Use an FTP (File Transfer Protocol) session to transfer this file to the module:

```
 Connected to ModuleIPAddress
 220 FTP server ready
 Name (ModuleIPAddress:none): root
 331 Guest login ok
 Password: <password-if-configured>
 230 Guest login ok, access restrictions
 apply.

 ftp> binary
 200 Type set to I
 ftp> put canopy.jpg
OR
      put top.html
 ftp> quit
 221 Goodbye
```

3 Use a telnet session and the **addwebfile** command to add the new file to the file system.

> **NOTE**
>
> Supported telnet commands execute the following results:
>
> **addwebfile** adds a custom logo file to the file system.
>
> **clearwebfile** clears the logo file from the file system.
>
> **lsweb** lists the custom logo file and display the storage space available on the file system.

```
>telnet ModuleIPAddress
/---------\
C A N O P Y

Cambium Networks
(Copyright 2001-2012 Cambium Networks)

Login: root
Password: <password-if-configured>

Telnet +> addwebfile canopy.jpg
   OR
          addwebfile advantaged.jpg
   OR
          addwebfile top.html

Telnet +> lsweb

Flash Web files
/canopy.jpg     7867
free directory entries: 31
free file space: 55331

Telnet +> exit
```

Procedure 9 Changing the URL of the logo hyperlink

1 In the editor of your choice, create a file named `top.html`, consisting of one line:

<a href="*myurl*">

where ***myurl*** is the desired URL, for example, http://www.cambiumnetworks.com.

2 Save and close the file as `top.html`.

3 Use an FTP (File Transfer Protocol) session to transfer this file to the module.

4 Use a telnet session and the addwebfile command to add the new file (top.html) to the file system

If you need to restore the original logo and hyperlink in a module, perform the following steps.

Procedure 10 Returning a module to its original logo and hyperlink

1 Use a telnet session and the clearwebfile command to clear all custom files from the file system of the module

```
>telnet ModuleIPAddress
/---------\
C A N O P Y

Cambium Networks
(Copyright 2001-2012 Cambium Networks)
Login: root
Password: <password-if-configured>

Telnet +> lsweb
Flash Web files
canopy.jpg     7867
free directory entries: 31
free file space: 56468

Telnet +> clearwebfile
Telnet +> lsweb

Flash Web files
free directory entries: 32
free file space     64336 bytes

Telnet +> exit
```

Setting Up a Protocol Analyzer on Your Network

Selection of protocol analyzer software and location for a protocol analyzer depend on both the network topology and the type of traffic to capture. However, the examples in this section are based on free-of-charge Wireshark software, which is available at http://www.wireshark.com

The equipment required to set up a protocol analyzer includes:

- 1 hub

NOTE

Some Ethernet switches have a monitor mode (also called 'port mirroring', 'port monitoring'). To ensure that all packets are captured, set up a monitoring port on the hub/switch to monitor/mirror the ports to which the PMP 450 equipment and premises are connected.

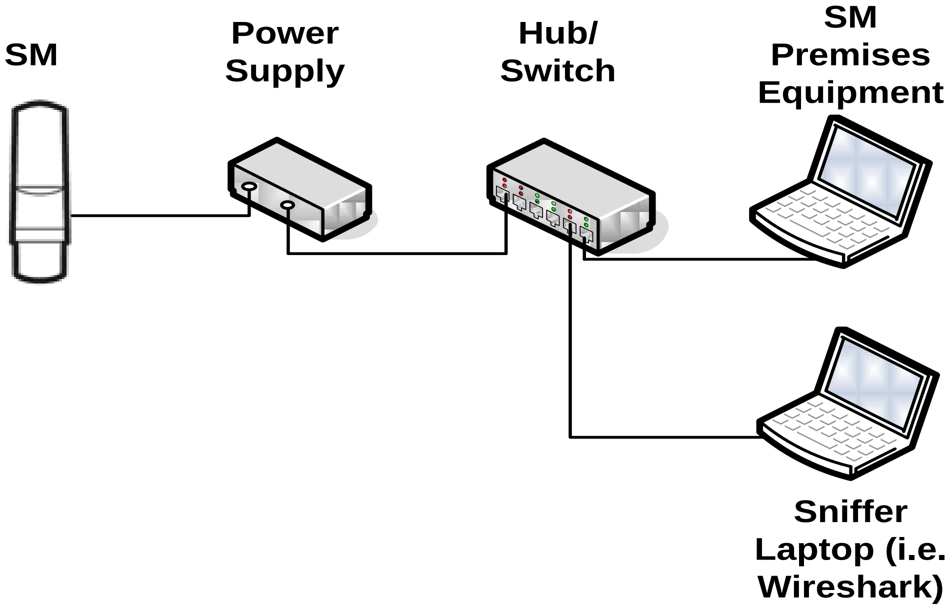
- 1 laptop computer with protocol analyzer software installed
- 2 straight-through Ethernet cables
- 1 power converter

Analyzing Traffic at an SM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the SM. If the SM has DHCP enabled, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the SM.

The configuration for analyzing traffic at an SM is shown below:

Figure 51 Protocol analysis at the SM

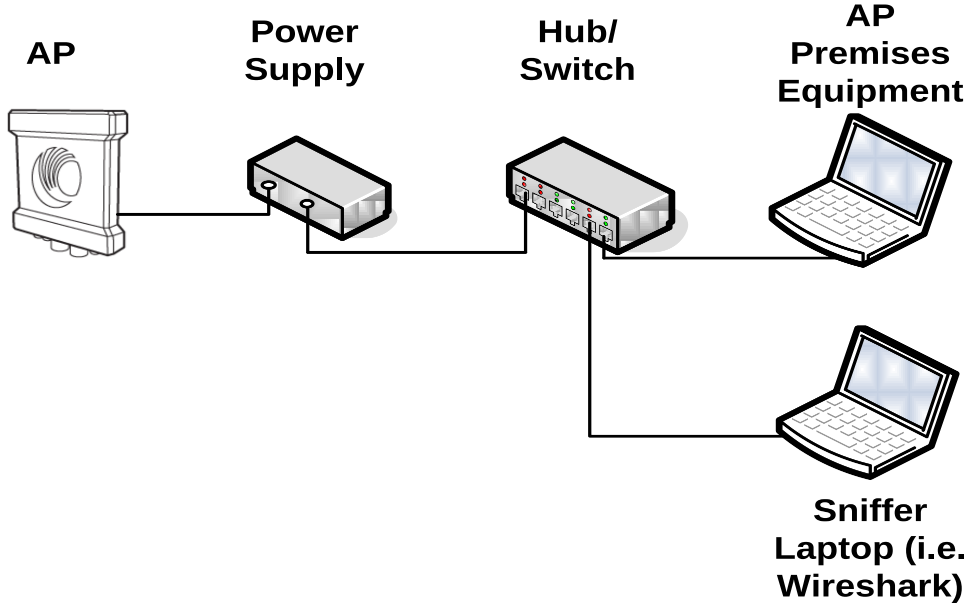


Analyzing traffic at an AP with no CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, then ensure that the laptop computer is configured with a static IP address in the same subnet as the AP.

The configuration for analyzing traffic at an AP that *is not* connected to a CMM is shown below:

Figure 52 Protocol analyzer at AP not connected to a CMM

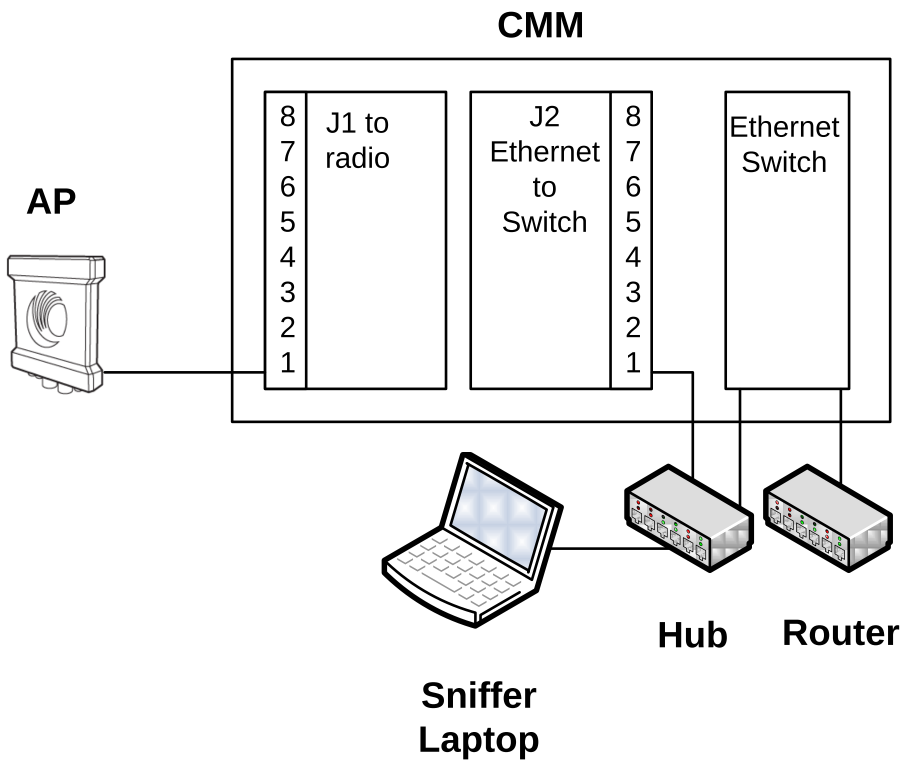


Analyzing Traffic at an AP or BH with a CMM

The IP address of the protocol analyzer laptop computer must match the IP addressing scheme of the AP. If the router is configured to be a DHCP server, then configure the laptop computer to automatically obtain an address. If DHCP is not enabled, ensure that the laptop computer is configured with a static IP address in the same subnet as the AP.

Connect the hub to the J2 Ethernet to Switch of the port that is associated with the AP. This example is of capturing traffic from AP 111, which is connected to
Port 1.

Figure 53 Protocol analysis at AP connected to a CMM



Example of a protocol analyzer setup for an SM

The following is an example of a network protocol analyzer setup using Wireshark software to capture traffic at the SM level. This example is based on the following assumptions:

- All required physical cabling has been completed.
- The hub, protocol analyzer laptop computer, and subscriber PC are successfully connected.
- Wireshark software is operational on the laptop computer.

Although these procedures involve the SM, the only difference in the procedure for analyzing traffic on an AP is the hub insertion point.

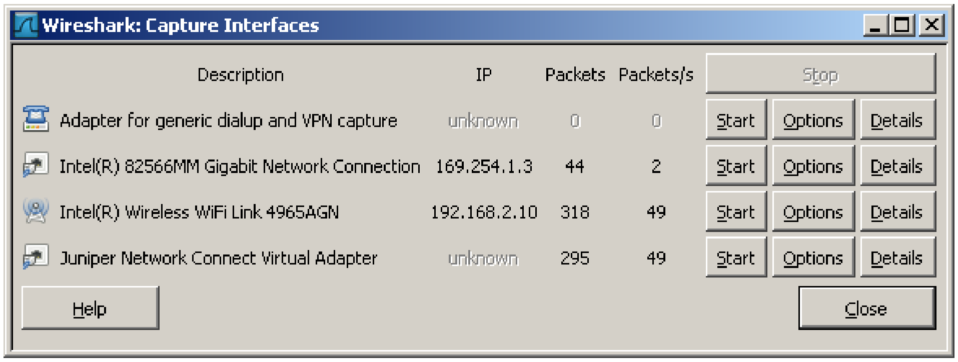
Procedure 11 Setting up a protocol analyzer

1 Verify that you have connectivity from the laptop computer to the SM

2 Launch the protocol analyzer software on the laptop computer

3 In the Capture menu, select Interfaces.

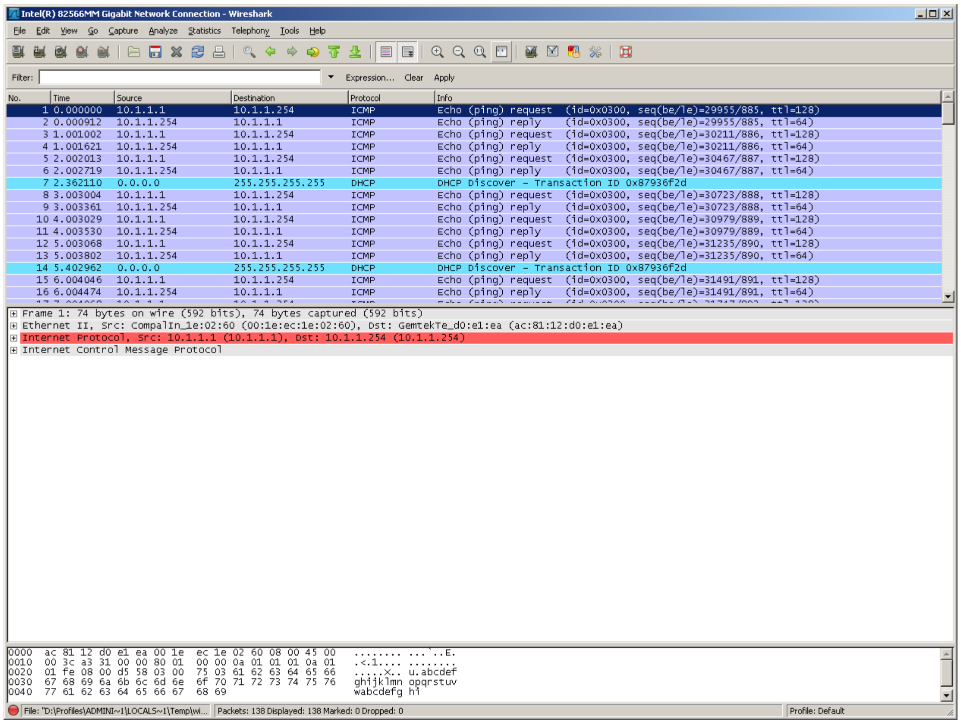
4 In the resulting dialog window, click the Start button corresponding to the Ethernet card connected to the SM



Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s			
Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
Intel(R) 82566MM Gigabit Network Connection	169.254.1.3	44	2	Start	Options	Details
Intel(R) Wireless WiFi Link 4965AGN	192.168.2.10	318	49	Start	Options	Details
Juniper Network Connect Virtual Adapter	unknown	295	49	Start	Options	Details

5 The captured packets are displayed in the main window:



```
No.  Time      Source       Destination      Protocol  Info
   1 0.000000  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=29955/885, ttl=128)
   2 0.000912  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=29955/885, ttl=64)
   3 1.001002  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=30211/886, ttl=128)
   4 1.001621  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=30211/886, ttl=64)
   5 2.002013  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=30467/887, ttl=128)
   6 2.002719  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=30467/887, ttl=64)
   7 2.362110  0.0.0.0      255.255.255.255  DHCP      DHCP Discover - Transaction ID 0x87936f2d
   8 3.003004  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=30723/888, ttl=128)
   9 3.003361  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=30723/888, ttl=64)
  10 4.003029  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=30979/889, ttl=128)
  11 4.003530  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=30979/889, ttl=64)
  12 5.003068  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=31235/890, ttl=128)
  13 5.003802  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=31235/890, ttl=64)
  14 5.402962  0.0.0.0      255.255.255.255  DHCP      DHCP Discover - Transaction ID 0x87936f2d
  15 6.004046  10.1.1.1     10.1.1.254       ICMP      Echo (ping) request  (id=0x0300, seq(be/le)=31491/891, ttl=128)
  16 6.004474  10.1.1.254   10.1.1.1         ICMP      Echo (ping) reply    (id=0x0300, seq(be/le)=31491/891, ttl=64)
```

```
⊞ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: CompalIn_1e:02:60 (00:1e:ec:1e:02:60), Dst: GemtekTe_d0:e1:ea (ac:81:12:d0:e1:ea)
⊞ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 10.1.1.254 (10.1.1.254)
⊞ Internet Control Message Protocol
```

```
0000  ac 81 12 d0 e1 ea 00 1e  ec 1e 02 60 08 00 45 00   ........ ...`..E.
0010  00 3c a3 31 00 00 80 01  00 00 0a 01 01 01 0a 01   .<.1.... ........
0020  01 fe 08 00 d5 58 03 00  75 03 61 62 63 64 65 66   .....X.. u.abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

File: "D:\Profiles\ADMINI~1\LOCALS~1\Temp\wi... | Packets: 138 Displayed: 138 Marked: 0 Dropped: 0 | Profile: Default

Chapter 7: Troubleshooting

General planning for troubleshooting

Effective troubleshooting depends in part on measures that you take before you experience trouble in your network. Cambium recommends the following measures for each site:

- Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
- Identify commands and other sources that can capture baseline data for the site. These may include
  - ping
  - tracert or traceroute
  - Link Capacity Test results
  - throughput data
  - Configuration tab captures
  - Status tab captures
  - session logs
  - web browser used
- Start a log for the site.
- Include the following information in the log:
  - operating procedures
  - site-specific configuration records
  - network topology
  - software releases, boot versions, and FPGA firmware versions
  - types of hardware deployed
  - site-specific troubleshooting processes
  - escalation procedures
- Capture baseline data into the log from the sources listed in bullet 2

General fault isolation process

Effective troubleshooting also requires an effective fault isolation methodology that includes

- attempting to isolate the problem to the level of a system, subsystem, or link, such as
  - AP to SM
  - AP to CMM
  - AP to GPS
  - CMM to GPS
  - BHM to BHS
  - BHM to CMM
  - power
- researching Event Logs of the involved equipment
- interpreting messages in the Event Log
- answering the questions listed in the following section.
- reversing the last previous corrective attempt before proceeding to the next.
- performing only one corrective attempt at a time.

Questions to help isolate the problem

When a problem occurs, attempt to answer the following questions:

- What is the history of the problem?
  - Have we changed something recently?
  - Have we seen other symptoms before this?
- How wide-spread is the symptom?
  - Is the problem on only a single SM? (If so, focus on that SM.)
  - Is the problem on multiple SMs? If so

    is the problem on one AP in the cluster? (If so, focus on that AP)

    is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs)

    is the problem on all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
- Based on data in the Event Log
  - does the problem correlate to External Hard Resets with no WatchDog timers? (If so, this indicates a loss of power. Correct your power problem.)
  - is intermittent connectivity indicated? (If so, verify your configuration, power level, jitter, cables and connections, and the speed duplex of both ends of the link).
  - does the problem correlate to loss-of-sync events?
- Are connections made via *shielded* cables?
- Does the GPS antenna have an *unobstructed* view of the entire horizon?
- Has the site grounding been verified?

Secondary Steps

After preliminary fault isolation through the above steps

- check the Canopy knowledge base (http://www.cambiumnetworks.com/forum/) to find whether other network operators have encountered a similar problem.
- proceed to any appropriate set of diagnostic steps. These are organized as follows:
  - Module Has lost or does not establish connectivity on Page 7-4
  - NAT/DHCP-configured SM has lost or does not establish connectivity on Page 7-6
  - SM Does Not Register to an AP on Page 7-7
  - Module has lost or does not gain sync on Page 7-8
  - Module does not establish Ethernet connectivity on Page 7-9
  - Module on Page 7-10
  - Power supply does not produce power on Page 7-10
  - CMM does not pass proper GPS sync to connected modules on Page 7-11

Procedures for Troubleshooting

Module Has lost or does not establish connectivity

To troubleshoot a loss of connectivity, perform the following steps.

Procedure 12 Troubleshooting loss of connectivity

1 Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.

2 Set up the minimal amount of equipment.

3 On each end of the link

- check the cables and connections.
- verify that the cable/connection scheme—straight-through or crossover—is correct.
- verify that the LED labeled LNK is green.
- access the General Status tab in the Home page of the module.
- verify that the SM is registered.
- verify that Received Power Level is -87 dBm or higher.
- access the IP tab in the Configuration page of the module.
- verify that IP addresses match and are in the same subnet.
- if RADIUS authentication is configured, ensure that the RADIUS server is operational

4 On the SM end of the link

- verify that the PC that is connected to the SM is correctly configured to obtain an IP address through DHCP.
- execute **`ipconfig`** (Windows) or **`ifconfig`** (linux)
- verify that the PC has an assigned IP address.

5 On each end of the link

- access the General tab in the Configuration page of each module.
- verify that the setting for **Link Speeds** (or negotiation) matches that of the other module.
- access the Radio tab in the Configuration page of each module.
- verify that the **Radio Frequency Carrier** setting is checked in the Custom Radio Frequency Scan Selection List.
- verify that the **Color Code** setting matches that of the other module.
- access the browser LAN settings (for example, at **Tools→Internet Options→Connections→LAN Settings** in Internet Explorer).
- verify that none of the settings are selected.
- access the Link Capacity Test tab in the Tools page of the module.
- perform a link test
- verify that the link test results show efficiency greater than 90% in both the uplink and downlink
- execute `ping`.
    - verify that no packet loss was experienced.
    - verify that response times are not significantly greater than

      4 ms from AP to SM

      15 ms from SM to AP
    - replace any cables that you suspect may be causing the problem.

> **NOTE**
>
> A ping size larger than 1494 Bytes to a module times out and fails. However, a ping of this size or larger to a system that is behind a Canopy module typically succeeds. It is generally advisable to ping such a system, since Canopy handles that ping with the same priority as is given all other transport traffic. The results are unaffected by ping size and by the load on the Canopy module that brokers this traffic.

6 After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

NAT/DHCP-configured SM has lost or does not establish connectivity

Before troubleshooting this problem, identify the NAT/DHCP configuration from the following list:

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

To troubleshoot a loss of connectivity for an SM configured for NAT/DHCP, perform the following steps.

Procedure 13 Troubleshooting loss of connectivity for NAT/DHCP-configured SM

1 Isolate the end user/SM from peripheral equipment and variables such as routers, switches, and firewalls.

2 Set up the minimal amount of equipment.

3 On each end of the link

- check the cables and connections.
- verify that the cable/connection scheme—straight-through or crossover—is correct.
- verify that the LED labeled LNK is green.

4 At the SM

- access the NAT Table tab in the Logs web page.
- verify that the correct NAT translations are listed.
  RESULT: NAT is eliminated as a possible cause if these translations are correct.

5 If this SM is configured for NAT with DHCP, then at the SM

- execute `ipconfig` (Windows) or `ifconfig` (Linux)
- verify that the PC has an assigned IP address.
- if the PC *does not* have an assigned IP address, then
  - ○ enter ipconfig /release *"Adapter Name"*.
  - ○ enter ipconfig /renew *"Adapter Name"*.
  - ○ reboot the PC.
  - ○ after the PC has completed rebooting, execute `ipconfig`
  - ○ if the PC has an assigned IP address, then
  - ○ access the NAT DHCP Statistics tab in the Statistics web page of the SM.
  - ○ verify that DHCP is operating as configured.

6 After connectivity has been re-established, reinstall network elements and variables that you removed in Step 1.

SM Does Not Register to an AP

To troubleshoot an SM failing to register to an AP, perform the following steps.

Procedure 14 Troubleshooting SM failing to register to an AP

1 Access the Radio tab in the Configuration page of the SM.

2 Note the **Color Code** of the SM.

3 Access the Radio tab in the Configuration page of the AP.

4 Verify that the **Color Code** of the AP matches that of the SM.

5 Note the **Radio Frequency Carrier** of the AP.

6 Verify that the value of the **RF Frequency Carrier** of the AP is selected in the **Custom Radio Frequency Scan Selection List** parameter in the SM.

7 In the AP, verify that the **Max Range** parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.

8 Verify that no obstruction significantly penetrates the Fresnel zone of the attempted link.

9 Access the General Status tab in the Home page of each module.

10 Remove the bottom cover of the SM to expose the LEDs.

11 Power cycle the SM.
RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the SM is in Alignment mode because the SM failed to establish the link.

12 If the AP is configured to require authentication, ensure proper configuration of RADIUS or preshared AP key.

13 In this latter case, and if the SM has encountered no customer-inflicted damage, then request an RMA for the SM.

Module has lost or does not gain sync

To troubleshoot a loss of sync, perform the following steps.

Procedure 15 Troubleshooting loss of sync

1 Access the Event Log tab in the Home page of the SM

2 Check for messages with the following format:

```
RcvFrmNum =
ExpFrmNum =
```

3 If these messages are present, check the Event Log tab of another SM that is registered to the same AP for messages of the same type.

4 If the Event Log of this second SM *does not* contain these messages, then the fault is isolated to the first SM.

If the Event Log page of this second SM contains these messages, access the GPS Status page of the AP.

5 If the **Satellites Tracked** field in the GPS Status page of the AP indicates fewer than 4 or the **Pulse Status** field does not indicate Generating Sync, check the GPS Status page of another AP in the same AP cluster for these indicators. GPS signal acquisition should take no longer than 5 minutes from unit startup.

6 If these indicators are present in the second AP

- verify that the GPS antenna still has an unobstructed view of the entire horizon.
- visually inspect the cable and connections between the GPS antenna and the CMM. If this cable is not shielded, replace the cable with shielded cable

7 If these indicators *are not* present in the second AP, visually inspect the cable and connections between the CMM and the AP antenna. If this cable is not shielded, replace the cable with shielded cable.

Module does not establish Ethernet connectivity

To troubleshoot a loss of Ethernet connectivity, perform the following steps.

Procedure 16 Troubleshooting loss of Ethernet connectivity

1 Verify that the connector crimps on the Ethernet cable are not loose.

2 Verify that the Ethernet cable is not damaged.

3 If the Ethernet cable connects the module to a network interface card (NIC), verify that the cable is pinned out as a straight-through cable.

4 If the Ethernet cable connects the module to a hub, switch, or router, verify that the cable is pinned out as a crossover cable.

5 Verify that the Ethernet port to which the cable connects the module is set to auto-negotiate speed.

6 Verify VLAN configuration in the network, which may cause loss of module access if the accessing device is on a separate VLAN from the radio.

7 Power cycle the module.
RESULT: Approximately 25 seconds after the power cycle, the green LED labeled LNK should light to indicate that the link has been established. If the orange LED labeled SYN is lit instead, then the module is in Alignment mode because the module failed to establish the link.

8 In this latter case, and if the module has encountered no customer-inflicted damage, then request an RMA for the module.

Module does not power on

To troubleshoot the failure of a module to power up, perform the following steps.

Procedure 17 Troubleshooting failure to power on

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided in *PMP 450 Installation Guide*
4. Connect the power supply to a known good module via a known good Ethernet cable.
5. Attempt to power up the known good module and
   - if the known good module fails to power up, request an RMA for the power supply.
   - if the known good module powers up, return to the module that does not power up.
6. Reconnect the power supply to the failing module.
7. Connect the power supply to a power source.
8. Verify that the red LED labeled PWR lights.
9. If this LED *does not* light, and the module has not been powered up since the last previous FPGA firmware upgrade was performed on the module, then request an RMA for the module.

Power supply does not produce power

To troubleshoot the failure of a power supply to produce power, perform the following steps.

Procedure 18 Troubleshooting failure of power supply to produce power

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. Verify that the cable is wired and pinned out according to the specifications provided in *PMP 450 Installation Guide*
4. Connect the power supply to a known good module via a known good Ethernet cable.
5. Attempt to power up the known good module.
6. If the known good module fails to power up, request an RMA for the power supply.

CMM does not pass proper GPS sync to connected modules

If the Event Log tabs in all connected modules contain `Loss of GPS Sync Pulse` messages, perform the following steps.

Procedure 19 Troubleshooting CMM not passing sync

1. Verify that the GPS antenna has an unobstructed view of the entire horizon.
2. Verify that the GPS coaxial cable meets specifications.
3. Verify that the GPS sync cable meets specifications for wiring and length.
4. If the web pages of connected modules indicate any of the following, then find and eliminate the source of noise that is being coupled into the GPS sync cable:
   - In the GPS Status page
     - anomalous number of **Satellites Tracked** (greater than 12, for example)
     - incorrect reported **Latitude** and/or **Longitude** of the antenna
   - In the Event Log page
     - garbled GPS messages
     - large number of `Acquired GPS Sync Pulse` messages

   GPS signal acquisition should take no longer than 5 minutes from unit startup.
5. If these efforts fail to resolve the problem, then request an RMA for the CMM.

Module Software Cannot be Upgraded

If your attempt to upgrade the software of a module fails, perform the following steps.

Procedure 20 Troubleshooting an unsuccessful software upgrade

1. Download the latest issue of the target release and the associated release notes.
2. Verify that the latest version of CNUT is installed.
3. Compare the files used in the failed attempt to the newly downloaded software.
4. Compare the procedure used in the failed attempt to the procedure in the newly downloaded release notes.
5. If these comparisons reveal a difference, retry the upgrade, this time with the newer file or newer procedure.
6. If, during attempts to upgrade the FPGA firmware, the following message is repeatable, then request an RMA for the module:

   ```
   Error code 6, unrecognized device
   ```

Module Functions Properly, Except Web Interface Became Inaccessible

If a module continues to pass traffic, and the SNMP interface to the module continues to function, but the web interface to the module does not display, perform the following steps.

Procedure 21 Restoring web management GUI access

1 Enter **`telnet`** ***`DottedIPAddress`***.
RESULT: A telnet session to the module is invoked.

2 At the `Login` prompt, enter **`root`**.

3 At the Password prompt, enter ***`PasswordIfConfigured`***.

4 At the `Telnet +>` prompt, enter **`reset`**.
RESULT: The web interface is accessible again, and this telnet connection is closed.

> **NOTE**
>
> he module may also be rebooted via an SNMP-based NMS (Wireless Manager, for example)

5 If the issue persists, turn off any SNMP-based network/radio monitoring software and repeat steps 1-4.

Chapter 8: Reference information

This chapter contains reference information and regulatory notices that apply to the PMP 450 Series products.

The following topics are described in this chapter:

- Equipment specifications on page 8-2 contains specifications of the AP, SM and other equipment required for PMP 450 installations.
- Wireless specifications on page 8-7 contains specifications of the PMP 450 wireless interface, including RF bands, channel width and link loss.
- Data network specifications on page 8-8 contains specifications of the PMP 450 Ethernet interface.
- Compliance with safety standards on page 8-9 lists the safety specifications against which the PMP 450 has been tested and certified. It also describes how to keep RF exposure within safe limits.
- Compliance with radio regulations on page 8-14 describes how the PMP 450 complies with the radio regulations that are enforced in various countries.
- Notifications on page 8-18 contains notifications made to regulatory bodies for the PMP 450.

Equipment specifications

This section contains specifications of the AP, SM, associated supplies required for PMP 450 installations.

AP specifications

The PMP 450 AP conforms to the specifications listed in the table below. These specifications apply to all PMP 450 product variants.

Table 37 Connectorized AP physical specifications

Category	Specification
Product	
Model Number	C054045A001A, C054045A002A (US Only)
Spectrum	
Channel Spacing	Configurable on 5 MHz increments
Frequency Range	5725 – 5875 MHz (dependent upon Region Code setting)
Channel Width	20 MHz
Interface	
MAC (Media Access Control) Layer	Cambium Proprietary
Physical Layer	2x2 MIMO OFDM
Ethernet Interface	10/100BaseT, half/full duplex, rate auto negotiated (802.3 compliant)
Protocols Used	IPv4, UDP, TCP, IP, ICMP, SNMP, HTTP, FTP, RADIUS
Network Management	HTTP, FTP, SNMP v2c, Syslog
VLAN	802.1ad (DVLAN Q-inQ), 802.1Q with 802.1p priority, dynamic port VID
Performance	
Nominal Receive Sensitivity (w/ FEC) @ 20 MHz Channel, Single Branch	OFDM: 2x = -83 dBm, 4x = -76 dBm, 6x = -69 dBm

Category	Specification
Maximum Deployment Range	Up to 40 km (25 mi)
Subscribers Per Sector	Up to 46 (Release 12.0)
ARQ	Yes
Cyclic Prefix	1/16
Modulation Levels (Adaptive)	OFDM: QPSK, QPSK (MIMO-B), 16-QAM (MIMO-B), 64-QAM (MIMO-B)
Latency	5 – 7 ms
Packets Per Second	12, 500
GPS Synchronization	Yes, via CMM3, CMM4, or UGPS
Quality of Service	Diffserv QoS
Link Budget	
Antenna Beam Width	60º sectors
Combined Transmit Power	-30 to +22 dBm (to EIRP limit by region) in 1 dB-configurable intervals
Antenna Gain	17 dBi Horizontal and Vertical
Maximum Transmit Power	22 dBm combined OFDM
Physical	
Wind Loading	190 km/hour (118 mi/hour)
Antenna Connection	50 ohm, N-type
Environmental	IP67
Temperature	-40ºC to +55ºC (-40ºF to +131ºF)
Weight	5.9 kg (13 lbs) with antenna 2.5 kg (5.5 lbs) without antenna
Dimensions (H x W x D)	Radio: 27 x 21 x 7 cm (10.6" x 8.3" x 2.8") Antenna: 51 x 13 x 7.3 cm (20.2" x 5.1" x 2.9")

Category	Specification
Maximum Power Consumption	18 W
Input Voltage	29 V
Security	
Encryption	56-bit DES
Certifications	
FCC ID	Z8H89FT0002
Industry Canada Cert	109W-0002

SM specifications

The PMP 450 SM conforms to the specifications below. These specifications apply to all PMP 450 product variants.

Table 38 SM specifications

Category	Specification
Product	
Model Number	C054045C001A (4 Mbps Cap), C054045C002A (10 Mbps Cap), C054045C003A (20 Mbps Cap), C054045C004A (Uncapped)
Spectrum	
Channel Spacing	Configurable on 5 MHz increments
Frequency Range	5725 – 5875 MHz (dependent upon Region Code setting)
Channel Width	20 MHz
Interface	
MAC (Media Access Control) Layer	Cambium Proprietary
Physical Layer	2x2 MIMO OFDM
Ethernet Interface	10/100BaseT, half/full duplex, rate auto negotiated (802.3 compliant)

Category	Specification
Protocols Used	IPv4, UDP, TCP, IP, ICMP, SNMP, HTTP, FTP, RADIUS
Network Management	HTTP, FTP, SNMP v2c, Syslog
VLAN	802.1ad (DVLAN Q-in-Q), 802.1Q with 802.1p priority, dynamic port VID
Performance	
Maximum Deployment Range	Up to 40 km (25 mi)
ARQ	Yes
Cyclic Prefix	1/16
Modulation Levels (Adaptive)	OFDM: 1x = QPSK, 2x = QPSK-MIMO-B, 4x = 16-QAM-MIMO-B, 6x = 64-QAM-MIMO-B
Latency	5 - 7 ms
GPS Synchronization	Yes
Quality of Service	Diffserv QoS
Link Budget	
Antenna Beam Width	55° azimuth, 55° elevation (both horizontal and vertical)
Combined Transmit Power	-30 to +22 dBm (to EIRP limit by region)
Antenna Gain	9 dBi H+V, integrated patch
Maximum Transmit Power	22 dBm combined
Reflector Gain	+14 dBi
LENS Gain	+5.5 dBi
Physical	
Wind Loading	190 km/hour (118 mi/hour)
Environmental	IP55
Temperature	-40°C to +55°C (-40°F to +131°F)
Weight	0.45 kg (1 lb)

Category	Specification
Dimensions (H x W x D)	30 x 9 x 9 cm (11.75” x 3.4” x 3.4”)
Maximum Power Consumption	12 W
Input Voltage	29 V
Security	
Encryption	56-bit DES
Certifications	
FCC ID	Z8H89FT0001
Industry Canada Cert	109W-0001

Wireless specifications

This section contains specifications of the PMP 450 wireless interface. These specifications include RF bands, channel bandwidth, spectrum settings, maximum power and link loss.

General wireless specifications

Table 39 lists the wireless specifications that apply to all PMP 450 variants.

Table 39 PMP 450 wireless specifications

Item	Specification
Channel selection	Manual selection (fixed frequency).
Manual power control	To avoid interference to other users of the band, maximum power can be set lower than the default power limit.
Duplex scheme	Adaptive TDD
Range	25 mi / 40 km
Over-the-air encryption	DES
Error Correction	FEC

Data network specifications

This section contains specifications of the PMP 450 Ethernet interface.

Ethernet interface

The PMP 450 Ethernet port conforms to the specifications listed below:

Table 40 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	IEEE 802.3 compatible
QoS	IEEE 802.1p, IEEE 802.1Q, IEEE 802.1ad, DSCP IPv4
Interface	10/100BaseT, half/full duplex, rate auto negotiated
Maximum Ethernet Frame Size	1522 Bytes

NOTE

Practical Ethernet rates will depend on network configuration, higher layer protocols and platforms used.

Over the air throughput is restricted to the rate of the Ethernet interface at the receiving end of the link.

Compliance with safety standards

This section lists the safety specifications against which the PMP 450 has been tested and certified. It also describes how to keep RF exposure within safe limits.

Electrical safety compliance

The PMP 450 hardware has been tested for compliance to the electrical safety specifications listed in Table 41.

Table 41 PMP 450 safety compliance specifications

Region	Specification
USA	UL 60950
Canada	CSA C22.2 No.60950
International	CB certified & certificate to IEC 60950

Electromagnetic compatibility (EMC) compliance

Table 42 lists the EMC specification type approvals that have been granted for PMP 450.

Table 42 EMC emissions compliance

Variant	Region	Specification (Type Approvals)
PMP 450	USA	FCC Part 15 Class B
	Canada	RSS Gen and RSS 210

Human exposure to radio frequency energy

Standards

Relevant standards (USA and EC) applicable when working with RF equipment are:

- ANSI IEEE C95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.
- Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC) and respective national regulations.

- *Directive 2004/40/EC of the European Parliament and of the Council of 29 April 2004* on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- 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 the Health Canada web site at http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites_e.html and Safety Code 6.
- EN 50383:2002 Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz - 40 GHz).
- BS EN 50385:2002 Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz – 40 GHz) – general public.
- 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.

Power density exposure limit

Install the radios for the PMP 450 family of PMP wireless solutions so as to provide and maintain the minimum separation distances from all persons.

The applicable power density exposure limit from the standards (see Human exposure to radio frequency energy on page 8-9) is:

10 W/m² for RF energy in the 5.8 GHz frequency bands.

Calculation of power density

NOTE

The following calculation is based on the ANSI IEEE C95.1-1991 method, as that provides a worst case analysis. Details of the assessment to EN50383:2002 can be provided, if required.

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

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

Where:	**Is:**
S	power density in W/m²
P	maximum average 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:

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

Calculated distances and power compliance margins

Table 43 shows calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination. These are conservative distances that include compliance margins. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

PMP 450 equipment adheres to all applicable EIRP limits for transmit power when operating in MIMO mode. Separation distances and compliance margins include compensation for both transmitters.

Explanation of terms used in Table 43:

Tx burst – maximum average transmit power in burst (Watt)

P – maximum average transmit power capability of the radio (Watt) (combined transmitters)

G – total transmit gain as a factor, converted from dB

S – power density (W/m^2)

d – minimum distance from point source (meters)

R – recommended distances (meters)

C – compliance factor

Table 43 Power compliance margins

Freq. Band	Antenna	Variable			*d* (calcu-lated)	Recom-mended Separation Distance	Power Compliance Margin
		P	G	S			
5.8 GHz OFDM	Integrated SM, 9 dBi patch	0.158 W (22 dBm)	7.9 (9 dB)	10 W/m^2 or 1 mW/cm^2	10 cm	20 cm (8 in)	40.27
	Integrated SM, 9 dBi patch with 5.5 dBi LENS	0.158 W (22 dBm)	28 (14.5 dB)	10 W/m^2 or 1 mW/cm^2	18.7 cm	50 cm (20 in)	71.01
	Integrated SM, 9 dBi patch with 14 dBi Reflector Dish	0.158 W (22 dBm)	199 (23 dB)	10 W/m^2 or 1 mW/cm^2	50 cm	100 cm (40 in)	40
	Connectorized AP, with 17 dBi Sector Antenna	0.158 W (22 dBm)	50 (17 dB)	10 W/m^2 or 1 mW/cm^2	25.1 cm	50 cm (20 in)	39.77

NOTE

Gain of antenna in dBi = 10*log(G).

The regulations require that the power used for the calculations is the maximum power in the transmit burst subject to allowance for source-based time-averaging.

At EU 5.8 GHz, the products are generally limited to a fixed EIRP which can be achieved with the Integrated Antenna. The calculations above assume that the maximum EIRP allowed by the regulations is being transmitted.

NOTE

If there are no EIRP limits in the country of deployment, use the distance calculations for FCC 5.8 GHz for all frequency bands.

Compliance with radio regulations

This section describes how the PMP 450 complies with the radio regulations that are enforced in various countries.

⚠ CAUTION

Changes or modifications not expressly approved by Cambium could void the user's authority to operate the system.

Type approvals

This system has achieved Type Approval in various countries around the world. This means that the system has been tested against various local technical regulations and found to comply. The frequency bands in which the system operates may be 'unlicensed' and, in these bands, the system can be used provided it does not cause interference. The system is not guaranteed protection against interference from other products and installations.

Table 42 lists the radio specification type approvals that have been granted for PMP 450 frequency variants.

Table 44 Radio certifications

Variant	Region	Specification (Type Approvals)
PMP 58450	USA	FCC Part 15 Class B
	CANADA	RSS Gen and RSS 210

FCC compliance testing

With GPS synchronization installed, the system has been tested for compliance to US (FCC) specifications. It has been shown to comply with the limits for emitted spurious radiation for a Class B digital device, pursuant to Part 15 of the FCC Rules in the USA. These limits have been designed to provide reasonable protection against harmful interference. However the equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to other radio communications. There is no guarantee that interference will not occur in a particular installation.

NOTE

A Class B Digital Device is a device that is marketed for use in a residential environment, notwithstanding use in commercial, business and industrial environments.

NOTE

Notwithstanding that Cambium has designed (and qualified) the PMP 450 products to generally meet the Class B requirement to minimize the potential for interference, the PMP 450 product range is not marketed for use in a residential environment.

Region Codes

Table 45 lists the region codes available on PMP 450 AP and SM units. Region code settings affect the radios in the following ways:

- Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain)

PMP 450 equipment shipped to the United States is locked down with a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.

Table 45 Region Code Information for PMP 450 AP

OFDM Radio Model	Channel Size	Region Code(s)	Band Edges (MHz)	Range of Center Frequencies Available (MHz)	Center Channel Spacing	# of Center Channels (based on PMP 450 available range)
PMP 450 Series AP, 5.8-GHz	20 MHz	United States, Canada, Australia, Brazil	5725 – 5850	5735 – 5840	5 MHz	22
		Ireland, Other	5725 - 5875	5735 – 5865	5 MHz	27
		India	5825 - 5875	5835 – 5865	5 MHz	7

Table 46 Region Code transmit power regulation

Radio/ Frequency	Channel Size	Region(s)	Combined TX Default Setting	Antenna Gain (18 dBi – 1dB cable loss)	Max EIRP (Tx + Antenna Gain)
PMP 450 AP 5.8 GHz OFDM	20 MHz	United States, Canada, Australia	19 dBm	17 dBi	36 dBm
		Brazil and India	13 dBm	17 dBi	30 dBm
		Ireland	16 dBm	17 dBi	33 dBm

NOTE: Transmit power is automatically limited to meet regional EIRP limits based on Region Code selection. No conducted EIRP/transmit power limit for Region Code "Other"

FCC and ICC IDs and certification numbers

Table 47 US FCC IDs and Industry Canada Certification Numbers and Covered Configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna (OFDM)	Maximum Combined Tx Output Power
Z8H89FT0002	109W-0002	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5780APC	17 dBi Connectorized	19 dBm
Z8H89FT0001	109W-0001	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated	19 dBm
Z8H89FT0001	109W-0001	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated with 14 dBi Reflector Dish	19 dBm
Z8H89FT0001	109W-0001	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated with 5.5 dBi LENS	19 dBm

Notifications

This section contains notifications of compliance with the radio regulations that are enforced in various regions.

PMP 450 regulatory compliance

The PMP 450 complies with the regulations that are enforced in the USA and Canada. The relevant notifications are specified in this section.

PMP 450 FCC and IC notification

U.S. Federal Communication Commission (FCC) and Industry Canada (IC) Notification.

This system has achieved Type Approval in various countries around the world. This means that the system has been tested against various local technical regulations and found to comply. The frequency band in which the system operates is 'license exempt' and the system is allowed to be used provided it does not cause interference. The licensing authority does not guarantee protection against interference from other products and installations.

This device complies with part 15 of the US FCC Rules and Regulations and with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. In Canada, users should be cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of the 5650 – 5850 MHz spectrum and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

For the connectorized version of the product and in order to reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Effective Isotropically Radiated Power (EIRP) is not more than that permitted for successful communication.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules and with RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply.

Appendix A: Glossary

Term	Definition
10Base-T	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.
169.254.0.0	Gateway IP address default in Cambium fixed wireless broadband IP network modules.
169.254.1.1	IP address default in Cambium fixed wireless broadband IP network modules.
255.255.0.0	Subnet mask default in Cambium 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 subscribers. Each Access Point Module covers a 60° or 90° 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° or 90° sector.
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.
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.
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 to subscriber modules.

Term	Definition
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module. 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.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
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.
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.

Term	Definition
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.
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.
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.
Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCError 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.
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.
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.

Term	Definition
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. Cambium 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.
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 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.
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.
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.
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.

Term	Definition
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.
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, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber, this LED flashes on and off to indicate that the module is not registered.
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.

Term	Definition
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.
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.

Term	Definition
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, 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).
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Cambium 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.
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.

Term	Definition
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.
Object	Network variable that is defined in the Management Information Base.
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.)
outerrrors 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.
PMP	See Point-to-Multipoint Protocol.

Term	Definition
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.
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.
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.
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.
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 frequency band range restrictions for the selected region. Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
Registrations MIB	Management Information Base file that defines registrations for global items such as product identities and product components. See also Management Information Base.
RetransLimitExp Field	This field displays how many times the retransmit limit has expired.

Term	Definition
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.
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.
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.
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.
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.
Standard Operating Margin	See Fade Margin.

Term	Definition
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/1	Second-from-right LED in the module. In the Access Point Module or in a registered Subscriber, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module, this LED flashes on and to indicate that the module is not registered.
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.
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.

Term	Definition
Textual Conventions MIB	Management Information Base file that defines system-specific textual conventions. See also Management Information Base.
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.