Cambium PMP 450 Operations Guide

System Release 13.2

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 is 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 are exposed to the outdoor environment.

RF exposure near the antenna

Radio frequency (RF) fields are 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 the *PMP 450 Planning Guide*.

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 Country 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 Country Codes that comply with FCC/IC rule.

Contents

List of Figures

List of Tables

About This Operations Guide

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

Users of this guide must 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
002v000	November 2012	Updated for System Release 12.0.1
003v000	January 2013	Updated for System Release 12.0.2
004v000	March 2013	Updated for System Release 12.0.3.1
005v000	June 2013	Updated for System Release 12.1
006v000	September 2013	Updated for System Release 12.1.2
007v000	March 2014	Updated for System Release 13.0
008v000	November 2014	Updated for System Release 13.2

Contacting Cambium Networks

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

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

Sales enquiries: sales@cambiumnetworks.com

Email support: support@cambiumnetworks.com

Telephone numbers:

For full list of Cambium support telephone numbers, see:
http://www.cambiumnetworks.com/support/contact-support

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.cambiumnetworks.com/support
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 products. For warranty assistance, contact the reseller or distributor.

⚠ CAUTION

Using non-Cambium parts for repair could damage the equipment and will 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

Key to successfully growing your network includes the following:

- Monitoring the RF environment.
- Considering configuration option for GPS synchronization
- 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 Using the Spectrum Analyzer tool on page 5-131 for details.

Considering configuration options for GPS synchronization

The configuration options available for synchronization on the PMP 450 Access Point are:

- **AutoSync**: The AP automatically receives sync from one of the following sources:
  - GPS Sync over Timing Port (UGPS, co-located AP GPS sync output, or “Remote AP” feed from a registered SM’s GPS sync output)
  - GPS Sync over Power Port (CMM)
  - On-board GPS (internal GPS)

  Upon AP power on, the AP does not transmit until a valid synchronization pulse is received from one of the sources above. When there are synchronization sources on both the timing port and the power port, the power port GPS source is chosen first.

  If there is a loss of GPS synchronization pulse, within two seconds the AP automatically attempts to source GPS signaling from another source. On-board GPS (internal GPS) is the last source checked for GPS signaling if there is no receipt of signaling from the timing port or from the power port (the on-board GPS module must not be used as the primary timing source). If no valid GPS signal is received, the AP ceases transmission and SM registration is lost until a valid GPS signal is received again on the AP.

- **AutoSync + Free Run**: This mode operates similarly to mode "AutoSync", but if a previously received synchronization signal is lost and no GPS signaling alternative is achieved (from the timing port, power port, or on-board GPS), the AP automatically changes to synchronization mode "Generate Sync". While SM registration is maintained, in this mode there is no synchronization of APs that can "hear" each other; the AP will only generate a sync signal for the local AP and its associated SMs. Once a valid GPS signal is obtained again, the AP automatically switches to receiving synchronization via the GPS source and SM registration is maintained.

> **NOTE**
>
> In mode AutoSync + Free Run, if a GPS signal is never achieved initially, the system will not switch to "Free Run" mode and SMs will not register to the AP. A valid GPS signal must be present initially for the AP to switch into "Free Run" mode (and to begin self-generating a synchronization pulse).
>
> Also, When an AP is operating in "Free Run" mode, over a short time it will no longer be synchronized with co-located or nearby APs (within radio range). Due to this lack of transmit and receive synchronization across APs or across systems, performance while in "Free Run" mode may be degraded until the APs operating in "Free Run" mode regain a external GPS synchronization source. Careful attention must be paid to ensure that all systems are properly receiving an external GPS synchronization pulse and please consider "Free Run" mode as an emergency option.

- **Generate Sync** (factory default): This option may be used when the AP is not receiving GPS synchronization pulses from either a CMM or UGPS module and there are no other APs active within the link range. Using this option will not synchronize transmission of APs that can "hear" each other; it will only generate a sync signal for the local AP and its associated SMs.

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://support.cambiumnetworks.com/pmp/software/index.php?tag=pmp450

Re-deploying Modules

Successfully redeploying a module may involve:

- Maintaining full and accurate records of modules being redeployed from warehouse stock.
- Exercising caution about the following:
  - 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.
  - 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 sync ports of the co-located modules using a sync cable with RJ-11 connectors
2. Set the **AP Type** of the co-located AP to “Remote AP”
3. Set the **Sync Input** of the co-located AP to “AutoSync”. This setting allows AP to automatically find the synchronization pulse received via the sync port
4. Set the **Frame Timing Pulse Gated** parameter on the co-located SM to “Enable”. This setting prevents interference in the event that the SM 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:

- Section Configuring quality of service on page 2-14 describes the Quality of Service (QoS) mechanisms implemented in the PMP 450 system.
- Section Configuring a RADIUS server on page 2-31 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 MIR parameters for bandwidth management:

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

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

Token Bucket Algorithm

The software uses a *token bucket* algorithm that has the following features:

- 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.

MIR 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

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

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

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

Figure 2 Uplink and downlink rate cap adjustment example

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

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

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

Committed Information Rate (CIR)

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum unless CIR is oversubscribed or RF conditions are degraded. CIR is oversubscribed when there is not enough available bandwidth to support CIR configuration for all subscribers. In this condition, SMs which are configured with a nonzero CIR will all operate at the maximum data rate supported by the link (subject to Maximum Information Rate and Burst Rate/Allocations). SMs which are configured with a CIR of 0 kbps will not transmit until CIR-configured SMs have completed transmission. CIR may be configured independently for high priority traffic and for low priority traffic. CIR parameters may be configured in the following ways:

- Web-based management GUI
- SNMP
- Authentication Server (RADIUS) - when a SM successfully registers and authenticates, CIR information is retrieved from the RADIUS server.

Active CIR configuration may be verified via the AP's **Home => Session Status** tab.

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 is 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.

The number of channels available on the AP is reduced by the number of SMs configured for the high-priority channel (each SM operating with high-priority enabled uses two channels (virtual circuits) instead of one).

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. 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	95 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	CIR high-priority CIR low-priority 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, CIR, VLAN and the high-priority channel as follows. The **Configuration Source** parameter affects the source of the following:

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

Table 3 Recommended combined settings for typical operations

Most operators who use…	This parameter must be set to…	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 a SM with authentication required

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

NOTE

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.

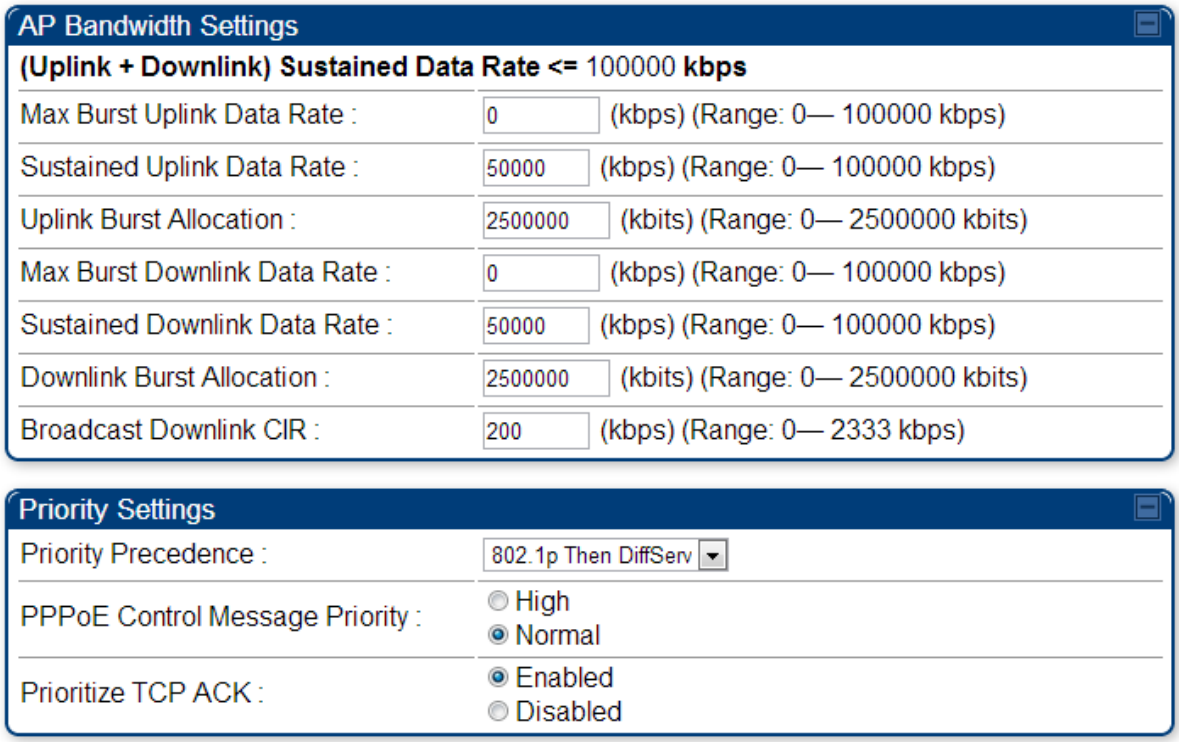
For any SM whose **Authentication Mode** parameter *is not* set to **Authentication Required**, the listed settings are derived as shown:

Table 5 Where feature values are obtained for a SM with authentication disabled

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

Quality of Service (QoS) tab of the AP

Figure 3 Quality of Service (QoS) tab of the AP



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

Table 6 AP QoS attributes

Attribute	Meaning
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the **Sustained Uplink Data Rate** with credits to transit more. When set to 0 (default), the burst rate is unlimited.
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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19
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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19
Max Burst Downlink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the **Sustained Downlink Data Rate** with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Sustained Downlink Data Rate	Specify the rate at which the AP must 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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19
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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19

Attribute	Meaning
Broadcast Downlink CIR	Broadcast Downlink CIR (Committed Information Rate, a minimum) supports system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default. Broadcast Downlink CIR is closely related to the Broadcast Repeat Count parameter, which is settable in the Radio tab of the Configuration page in the AP: when the Broadcast Repeat Count is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the Broadcast Repeat Count parameter.
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the 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.

IPv6 Prioritization

System Release 13.2 provides operators the ability to prioritize IPv6 traffic in addition to IPv4 traffic. IPv6 prioritization works similar to IPv4 prioritization where the user can select the Code Point and the corresponding priority from the GUI of the AP and the IPv6 packet is set up accordingly. There is no separate GUI option for IPv6 priority. Once the priority is set, it is set for IPv4 and IPv6 packets. Then depending upon which packet is received, the set priority is used. The default for IPv6 priority is none.

Configuring IPV6 Priority

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

IPv6 Filtering

In releases prior to System Release 13.2, the operator can filter (block) specified IPv4 protocols and ports from leaving the AP and SM and entering the network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other. In System Release 13.2, filtering capabilities have been added for IPv6 traffic. Unlike IPv6 Prioritization, IPv6 filtering is done independent of IPv4 filtering.

Configuring IPV6 Filtering

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

Figure 4 Protocol filtering tab on AP and SM (Packet Filter Configuration section)

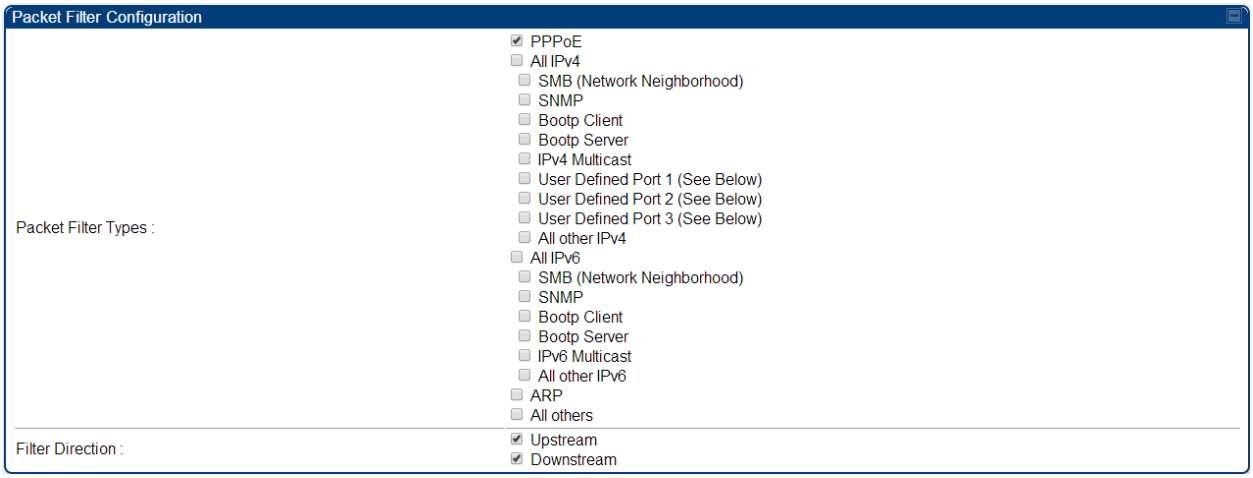


Table 7 Packet Filter Configuration attributes (IPv6 only)

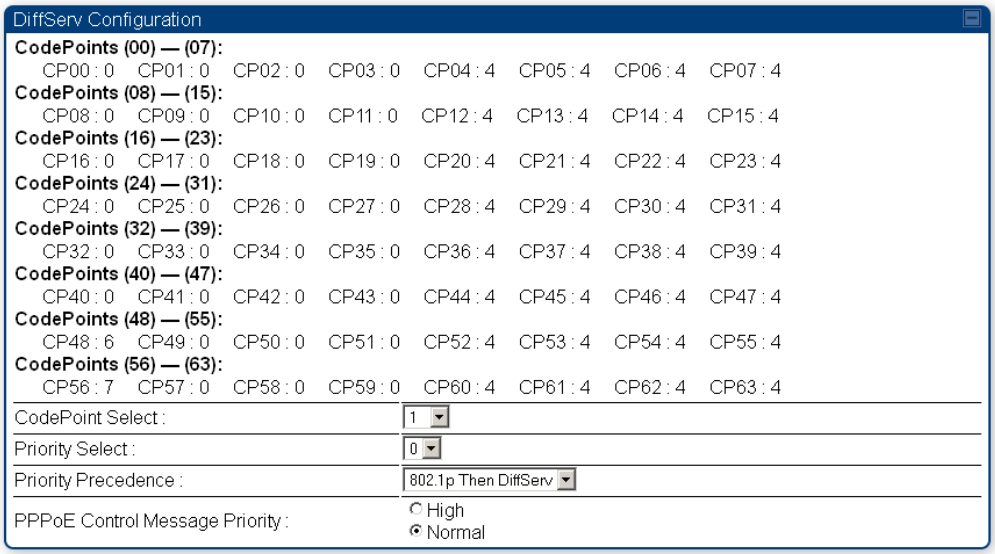
Attribute	Meaning
Packet Filter Types	For any box selected, the Protocol Filtering feature blocks the a ssociated protocol type. Port filtering on **User Defined Port**s is not available for IPv6 at this time.
Filter Direction	Operators may choose to filter upstream (uplink) RF packets or downstream (downlink) RF packets.

Table 8 IPV6 Filtering SNMP objects

Name	OID	MIB	Access	Syntax / Description
allipv6Filter	.1.3.6.1.4.1.161.19.3.3.9.160	WHISP-BOX- MIBV2-MIB	read-write	INTEGER
ipv6smbFilter	.1.3.6.1.4.1.161.19.3.3.9.161	WHISP-BOX- MIBV2-MIB	read-write	INTEGER
ipv6snmpFilter	.1.3.6.1.4.1.161.19.3.3.9.162	WHISP-BOX- MIBV2-MIB	read-write	INTEGER
ipv6bootpcFilter	.1.3.6.1.4.1.161.19.3.3.9.163	WHISP-BOX- MIBV2-MIB	read-write	INTEGER
ipv6bootpsFilter	.1.3.6.1.4.1.161.19.3.3.9.164	WHISP-BOX- MIBV2-MIB	read-write	INTEGER
ipv6MultFilter	.1.3.6.1.4.1.161.19.3.3.9.165	WHISP-BOX- MIBV2-MIB	read-write	INTEGER
allOtherIpv6Filter	.1.3.6.1.4.1.161.19.3.3.9.166	WHISP-BOX- MIBV2-MIB	read-write	INTEGER

DiffServ tab of the AP

Figure 5 Diffserv tab of the AP



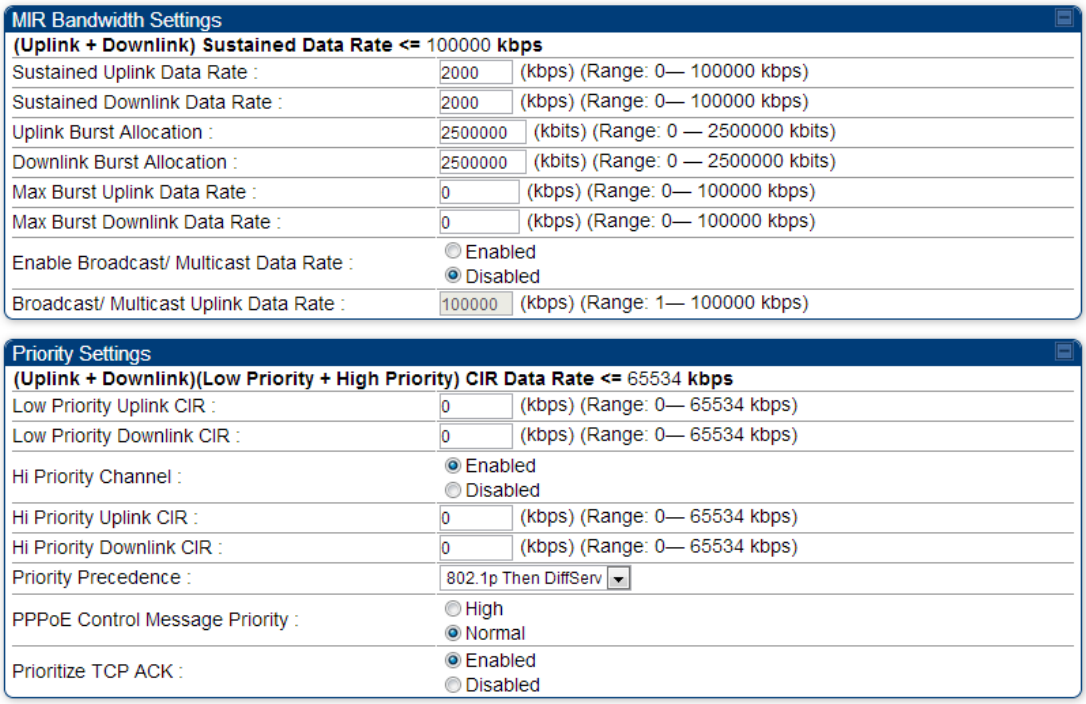
You may set the following **Diffserv** tab parameters.

Table 9 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 must 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.

Quality of Service (QoS) tab of the SM

Figure 6 Quality of Service (QoS) tab of the SM



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

Table 10 SM Quality of Service attributes

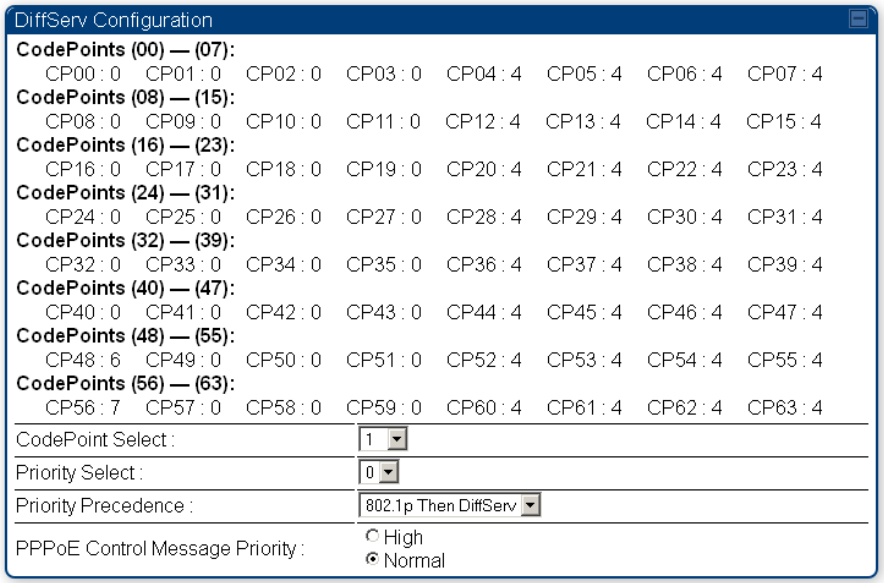
Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See • Maximum Information Rate (MIR) Parameters on page 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19
Sustained Downlink Data Rate	Specify the rate at which the AP must 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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19

Attribute	Meaning
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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19
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 2-14 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 2-16 • Setting the Configuration Source on page 2-19
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the **Sustained Uplink Data Rate** with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Max Burst Downlink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the **Sustained Downlink Data Rate** with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Enable Broadcast / Multicast Data Rate	This parameter allows the operator to specify if Broadcast and Multicast data is rate-limited.
Broadcast / Multicast Data Rate	This parameter allows the operator to specify a data rate at which Broadcast and Multicast traffic is sent via the radio link.
Low Priority Uplink CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 2-16 • Setting the Configuration Source on page 2-19
Low Priority Downlink CIR	This field indicates the minimum rate at which low priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 2-16 • Setting the Configuration Source on page 2-19
Hi Priority Channel	See • High-priority Bandwidth on page 2-16 • Setting the Configuration Source on page 2-19

Attribute	Meaning
Hi Priority Uplink CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 2-16 • Setting the Configuration Source on page 2-19
Hi Priority Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 2-16 • Setting the Configuration Source on page 2-19
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the 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. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to “Disabled”.

DiffServ tab of the SM

Figure 7 Diffserv tab of the SM



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

Table 11 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 must 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 of SM Configuration menu.

MIMO-A mode of operation for PMP 450

In releases prior to System Release 13.2, PMP 450 supports MIMO-B mode using the following modulation levels: QPSK, 16-QAM, 64-QAM and 256-QAM. System Release 13.2 introduces MIMO-A mode of operation using the same modulation levels as the MIMO-B mode. With MIMO-B, the PMP 450 radio sends different streams of data over the two antennas whereas with MIMO-A, the PMP 450 radio uses a scheme that tries to optimize coverage by transmitting the same data over both antennas. This redundancy improves the signal to noise ratio at the receiver making it more robust, at the cost of throughput.

In addition to introducing MIMO-A modes, improvements have been made to the existing rate adapt algorithm to switch between MIMO-A and MIMO-B seamlessly without any intervention or added configuration by the operator. The various modulation levels used by the PMP 450 are shown in Table 12.

Table 12 PMP 450 Modulation levels

Rate	MIMO-B	MIMO-A	SISO (for PMP 430 interoperability)
QPSK	2X MIMO-B	1X MIMO-A	1X SISO
16-QAM	4X MIMO-B	2X MIMO-A	2X SISO
64-QAM	6X MIMO-B	3X MIMO-A	3X SISO
265-QAM	8X MIMO-B	4X MIMO-A	

For System Performance details of all the PMP 450 products please refer the Link Capacity Planner v11 at: https://support.cambiumnetworks.com/files/pmp450.

Table 13 Co-channel Interference per (CCI) MCS, PMP/PTP 450

MCS of Victim	MCS of Interferer	Channel BW	CCI
1X (QPSK SISO)	6X (64-QAM MIMO-	5, 10 or 20 MHz	10 dB
2X (16-QAM SISO)	6X (64-QAM MIMO-	5, 10 or 20 MHz	17 dB
3X (64-QAM SISO)	6X (64-QAM MIMO-	5, 10 or 20 MHz	25 dB
1X (QPSK MIMO-A)	6X (64-QAM MIMO-	5, 10 or 20 MHz	7 dB
2X (16-QAM MIMO-	6X (64-QAM MIMO-	5, 10 or 20 MHz	14 dB
3X (64-QAM MIMO-	6X (64-QAM MIMO-	5, 10 or 20 MHz	22 dB
4X (256-QAM MIMO-	6X (64-QAM MIMO-	5, 10 or 20 MHz	30 dB
2X (QPSK MIMO-B)	6X (64-QAM MIMO-	5, 10 or 20 MHz	10 dB
4X (16-QAM MIMO-	6X (64-QAM MIMO-	5, 10 or 20 MHz	17 dB
6X (64-QAM MIMO-	6X (64-QAM MIMO-	5, 10 or 20 MHz	25 dB
8X (256-QAM MIMO-	6X (64-QAM MIMO-	5, 10 or 20 MHz	33 dB

Table 14 Adjacent Channel Interference (ACI) per MCS, PMP/PTP 450

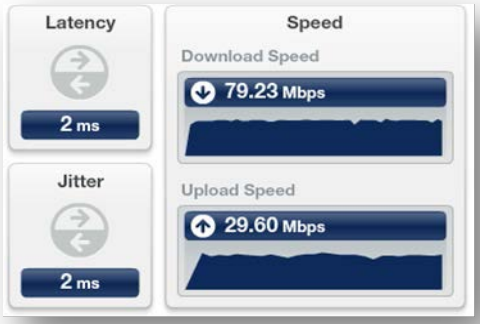
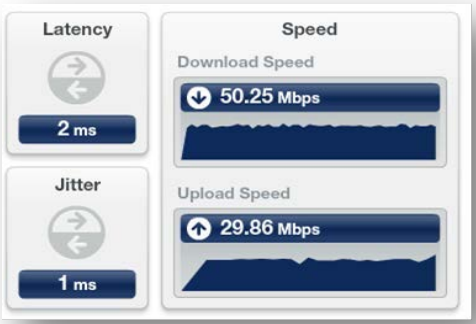
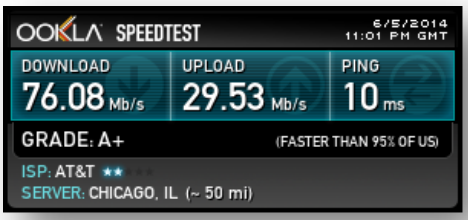
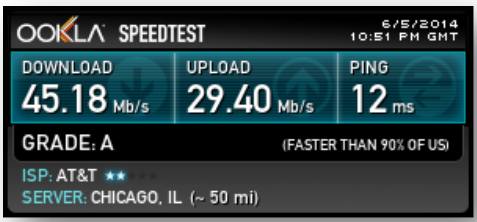
MCS of Victim	MCS of Interferer	Channel BW	ACI	Guard Band[1]
1X (QPSK SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
2X (16-QAM SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
3X (64-QAM SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz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

[1] No Guard Bands are needed for the 2.4 GHz, 5.4 GHz and 5.8 GHz bands. In the 3.5 / 3.6 GHz bands no guards are needed if the "Adjacent Channel Support" field is enabled under Configuration, Radio (this limits the SM Max Tx power to 23 dB combined). With 3.5/3.6 GHz SM transmitting at max power (Adjacent Channel Support disabled), the guard bands needed are: 5 MHz between two 20 MHz channels, 3 MHz between two 10 MHz channels and 2 MHz between two 5 MHz channels.

Improved PPS performance of PMP 450 SMs

System Release 13.2 provides improved packets per second (PPS) performance of the PMP 450 SMs. Through software enhancements and algorithm efficiencies, the PPS performance of the PMP 450 SM has been improved to 14000 packets/seconds, measured through a standard RFC2544 test using 64 bytes packets. With this enhancement, operators are able to provide higher bandwidth including better VoIP and video services to end customers using existing SM deployments.

Figure 8 Speedtest results example with 1 AP and 1 SM running System Release 13.2

Speedtest Server	Bridge Mode	NAT mode
Internal		
External		

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 a SM registers to an AP.
- **SM Accounting provides** support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection and bandwidth usage per session for each SM that connects to the AP.
- **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed IP** allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).

Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

- FreeRADIUS, Version 2.1.8
- Aradial RADIUS, Version 5.1.12

Note, Aradial 5.3 has a bug that prevents "remote device login", 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 a SM that itself has been configured to *require* RADIUS authentication by enabling Enforce Authentication as described below) is allowed to register to the AP.
- **Authentication Server:** Authentication Server in this instance refers to Wireless Manager in BAM-only mode. Authentication is required for a SM to register to the AP. Only SMs listed by MAC address in the Wireless Manager database is 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 is 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 or addresses configured here must match the IP address or addresses 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 9 Security tab of the AP

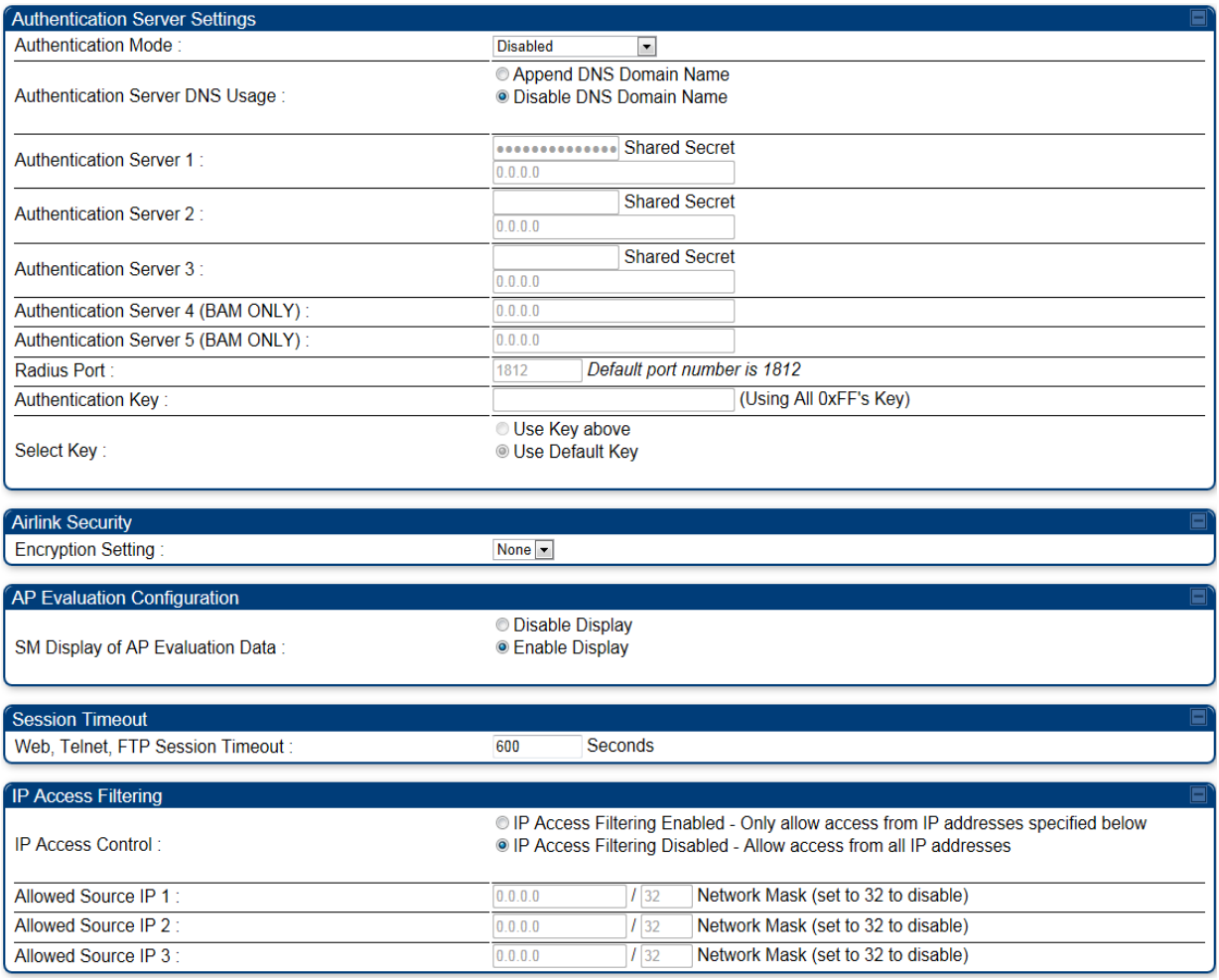


Table 15 AP Security tab attributes

Attribute	Meaning
Authentication Mode	Operators may use this field to select from among the following authentication modes: **Disabled**—the AP requires no SMs to authenticate. **Authentication Server** —the AP requires any SM that attempts registration to be authenticated in Wireless Manager before registration. **AP PreShared Key** - The AP acts as the authentication server to its SMs and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP and all SMs desired to register to that AP. There is also an option of leaving the AP and SMs at their default setting of using the "Default Key". Due to the nature of the authentication operation, if you want to set a specific authentication key, then you MUST configure the key on all of the SMs and reboot them BEFORE enabling the key and option on the AP. Otherwise, if you configure the AP first, none of the SMs are able to register. **RADIUS AAA** - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn't respond, Server 2 is tried and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network and does not progress trying the other servers.
Authentication Server DNS Usage	The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.
Authentication Server 1	Enter the IP address or server name of the authentication server (RADIUS or WM) and the Shared Secret configured in the authentication server. When **Authentication Mode RADIUS AAA** is selected, the default value of **Shared Secret** is "CanopySharedSecret". The **Shared Secret** may consist of up to 32 ASCII characters.
Authentication Server 2	
Authentication Server 3	
Authentication Server 4 (BAM Only)	
Authentication Server 5 (BAM Only)	
Radius Port	This field allows the operator to configure a custom port for RADIUS server communication. The default value is ***1812***.
Authentication Key	The authentication key is a 32-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.

Attribute	Meaning
Select Key	This option allows operators to choose which authentication key is used: **Use Key above** means that the key specified in **Authentication Key** is used for authentication **Use Default Key** means that a default key (based off of the SM's MAC address) is used for authentication.
Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. **None** provides no encryption on the air link. **DES** (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. **AES** (Advanced Encryption Standard)**:** An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
SM Display of AP Evaluation Data	You can use this field to suppress the display of data about this AP on the AP **Evaluation** tab of the **Tools** page in all SMs that register.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet or ftp access to the AP.
IP Access Control	You can permit access to the AP from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address.
Allowed Source IP 1	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read and access from all IP addresses is permitted.
Allowed Source IP 2	
Allowed Source IP 3	

SM Authentication Mode – Require RADIUS or Follow AP

If it is desired that a 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, a SM does not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected**.**

If it is desired that a SM use the authentication method configured on the AP it is registering to, set **Enforce Authentication** to **Disabled.** With **Enforce Authentication** disabled, a SM attempts 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 10 Security tab of the SM

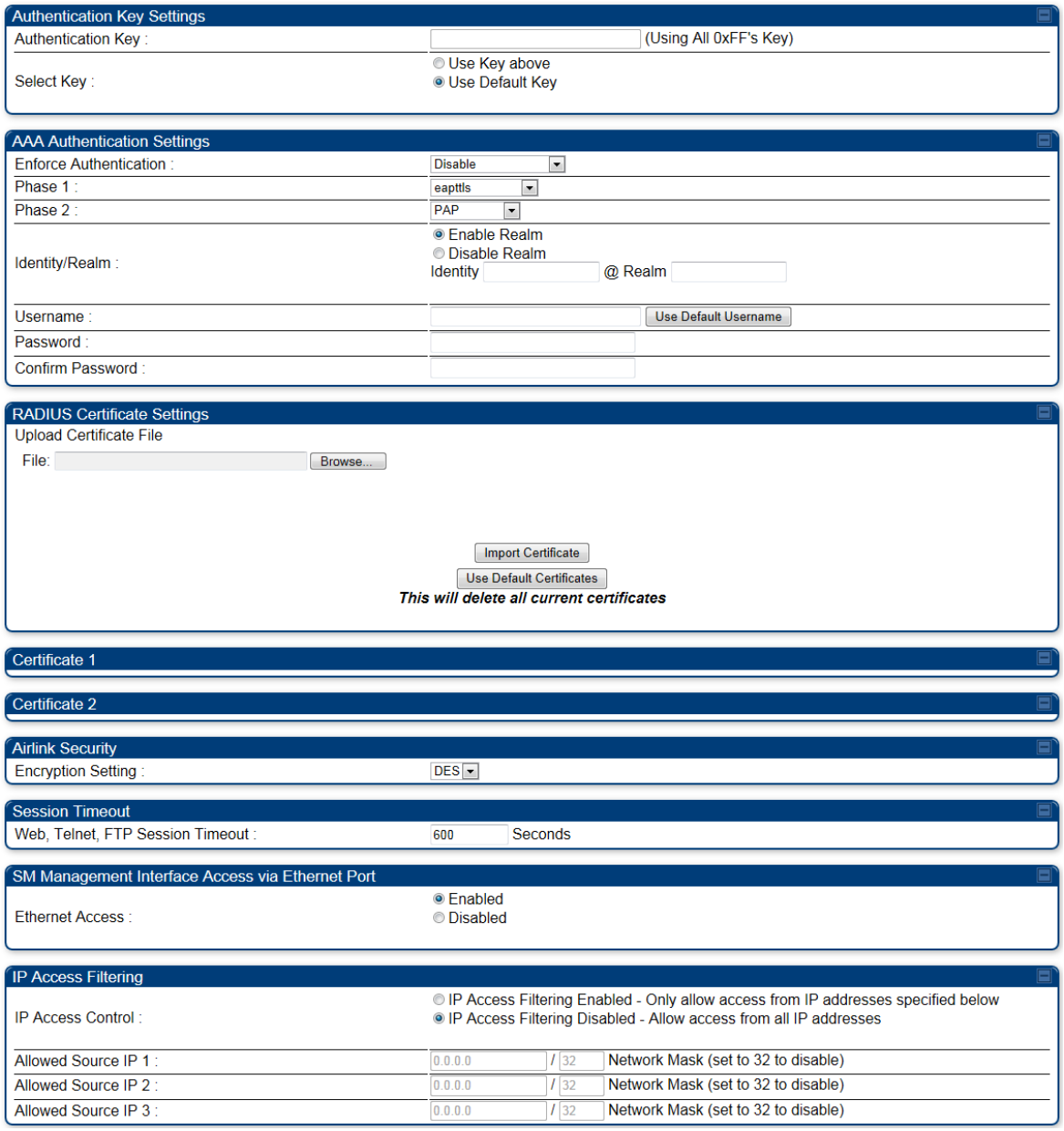


Table 16 SM Security tab attributes

Attribute	Meaning
Authentication Key	Only if the AP to which this SM will register requires authentication, specify the key that the SM will use when authenticating. For alpha characters in this hex key, use only upper case.
Select Key	The **Use Default Key** selection specifies the predetermined key for authentication in Wireless Manager The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the WM
Enforce Authentication	The SM may enforce authentication types of **AAA** and **AP Preshared Key**. The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM locks out the AP for 15 minutes).
Phase 1	The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).
Phase 2	Select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol) and **MSCHAP (**Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.
Identity/Realm	If Realms are being used, select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters. Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Username	Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password	Enter the desired password for the SM in the **Password** and **Confirm Password** fields**..** The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters

Attribute	Meaning
Upload Certificate File	To upload a certificate manually to a SM, first load it in a known place on your PC or network drive then click on the **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate and click the **Import Certificate** button and then reboot the radio to use the new certificate. When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used. The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system. Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the **Configuration => Security** tab. To restore the 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.
Encryption Setting	Specify the type of airlink security to apply to this SM. The encryption setting must match the encryption setting of the AP. **None** provides no encryption on the air link. **DES** (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system. **AES** (Advanced Encryption Standard)**:** An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet or FTP access to the SM.

Attribute	Meaning
Ethernet Access	If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select **Ethernet Access Disabled**. This selection disables access through this port to via HTTP (the GUI), SNMP, telnet, FTP and TFTP. With this selection, management access is available through only the RF interface via either an IP address (if **Network Accessibility** is set to **Public** on SM) or the Session Status or Remote Subscribers tab of the AP. **NOTE** This setting does not prevent a device connected to the Ethernet port from accessing the management interface of *other SMs* in the network. To prevent this, use the **IP Access Filtering Enabled** selection in the **IP Access Control** parameter of the SMs in the network. See **IP Access Control** below. If you want to allow management access through the Ethernet port, select **Ethernet Access Enabled**. This is the factory default setting for this parameter.
IP Access Control	You can permit access to the SM from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address
Allowed Source IP *1 to 3*	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the SM from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read and access from all IP addresses is permitted. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.

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, operators must create or procure their own certificates.

Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate’s description block on the **Configuration => Security** tab. To restore the 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

To upload a certificate manually to a SM, first load it in a known place on your PC or network drive and 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.

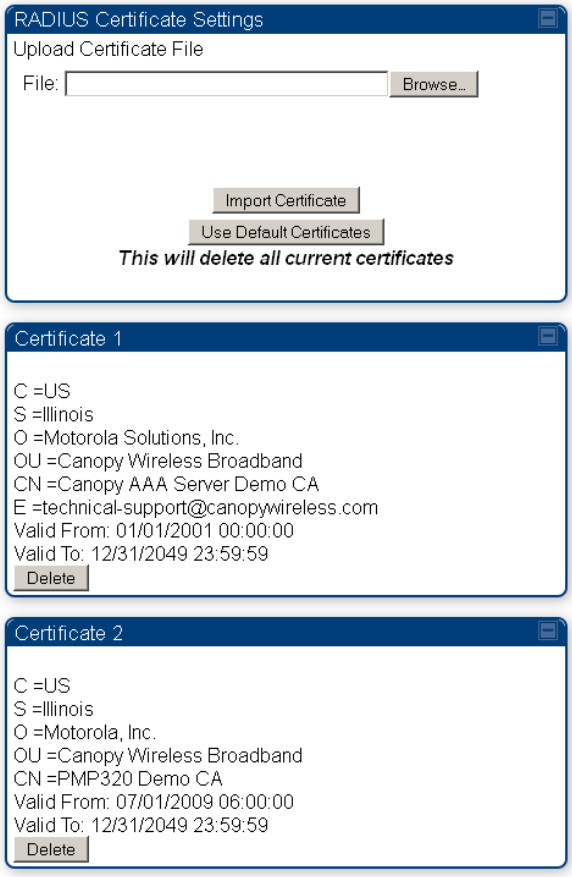
When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** appears in the description block of the certificate being used.

The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public or private key encryption system.

NOTE

Root certificates of more than one level (a certificate from someone who received their CA from Verisign, for example) fail. Certificates must be either root or self-signed.

Figure 11 SM Certificate Management



Configuring your RADIUS servers for SM authentication

Your RADIUS server must 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 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: http://support.cambiumnetworks.com/pmp/software/index.php?tag=pmp450 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 shows this string (listed as Authentication Response on the SM GUI) on the main Status page in the Subscriber Module Stats section.

Aradial AAA servers only support operator-configurable Authentication Accept responses, not Authentication Reject responses

Configuring your RADIUS server for SM configuration

The Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details are listed under Table 17. The associated SM GUI page, tab and parameter are listed to aid cross-referencing and understanding of the VSAs.

A RADIUS dictionary file is available from the software site:
http://support.cambiumnetworks.com/pmp/software/index.php?tag=pmp450

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.

NOTE

Beginning with System Release 12.0.2, two RADIUS dictionary files are available on the Cambium website – "RADIUS Dictionary file – Cambium" and "RADIUS Dictionary file – Motorola".

In addition to a renaming of attributes, the Cambium-branded dictionary file contains two new VSAs for controlling uplink and downlink Maximum Burst Data Rate (these VSAs are listed below in Table 17).

If you are transitioning from the Motorola-branded dictionary file to the Cambium-branded dictionary file, ensure that all RADIUS profiles containing Motorola-Canopy attribute references are updated to include Cambium-Canopy attribute references (for all applicable VSAs listed in Table 17). Also, ensure that all RADIUS configuration files reference the new dictionary file (as an alternative, operators may rename the Cambium-branded dictionary file to the filename currently in use by the RADIUS server). Once the profiles are updated and the new Cambium-branded dictionary file is installed on the RADIUS server, restart the RADIUS server to ensure that the new VSAs and attribute names are enabled.

Table 17 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Req'd	Value	
SM GUI Page > Tab > Parameter				Default	Size
MS-MPPE-Send-Key[2]	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key[3]	26.311.17	-	Y	-	
-				-	-
Cambium-Canopy-LPULCIR	26.161.1	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-LPDLCIR	26.161.2	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Downlink CIR				0 kbps	32 bits
Cambium-Canopy-HPULCIR	26.161.3	integer	N	0-65535 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-HPDLCIR	26.161.4	integer	N	0-65535 kbps	
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps	32 bits
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	0-100000 kbps	
Configuration > Quality of Service > Sustained Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-ULBL	26.161.7	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-DLBR	26.161.8	integer	N	0-100000 kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-DLBL	26.161.9	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-VLLEARNEN	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	

[2] Contains key for encrypting packets sent by the NAS to the remote host (for Microsoft Point-to-Point Encryption Protocol)

[3] Contains key for encrypting packets received by the NAS from the remote host (for Microsoft Point-to-Point Encryption Protocol)

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-VLSMMGPASS	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	0-100000 kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data Rate				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-ULBM	26.161.26	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Uplink Data Rate				0	32 bits
Cambium-Canopy-DLBM	26.161.27	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Downlink Data Rate				0	32 bits
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					

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 are 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 becomes 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 are 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.

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 is 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 or addresses 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 12 User Authentication tab of the AP

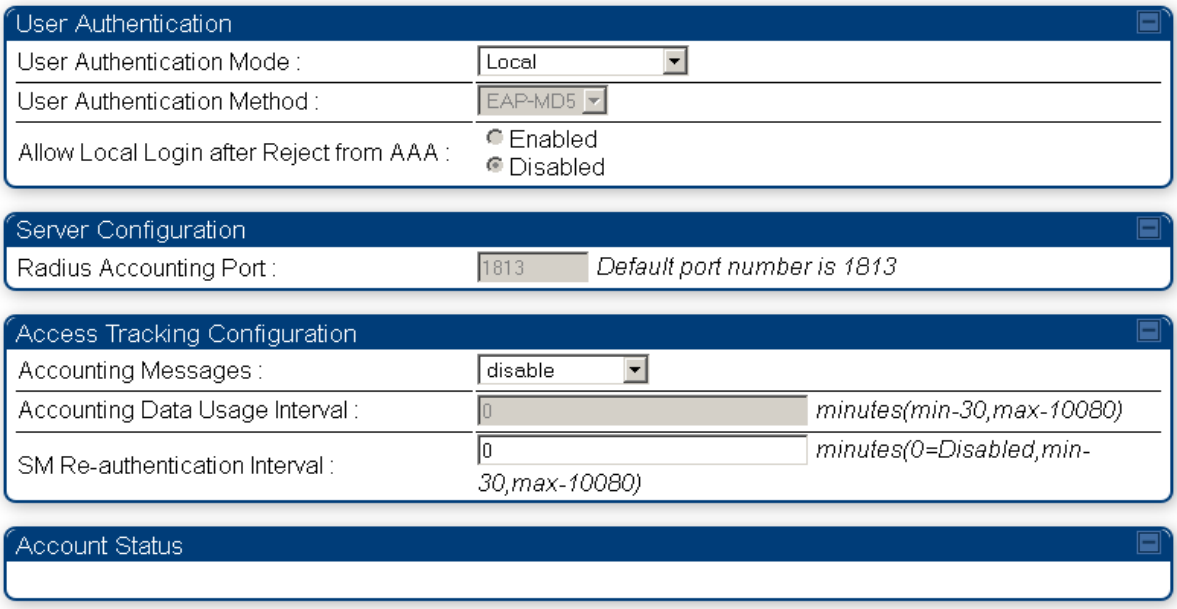


Table 18 User Authentication tab attributes

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 is 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 is allowed to login locally to the radio's management interface.
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 21). • dataUsage – accounting messages are sent to the RADIUS server regarding data usage (see Table 21).
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 re-authenticates to the RADIUS server.

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 is 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 is always used before and after registration, if the AP is not configured for RADIUS.

Figure 13 User Authentication and Access Tracking tab of the AP

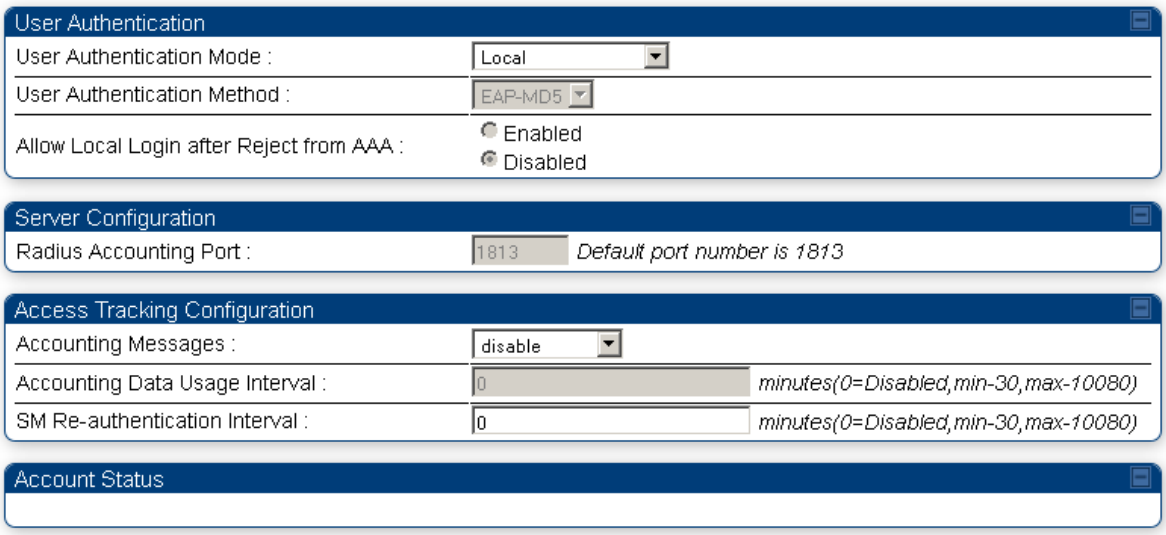


Table 19 AP User Authentication and Access Tracking attributes

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 is 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 is allowed to login locally to the radio's management interface.
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 21). • dataUsage – accounting messages are sent to the RADIUS server regarding data usage (see Table 21).
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 re-authenticates to the RADIUS server.

Figure 14 User Authentication tab of the SM

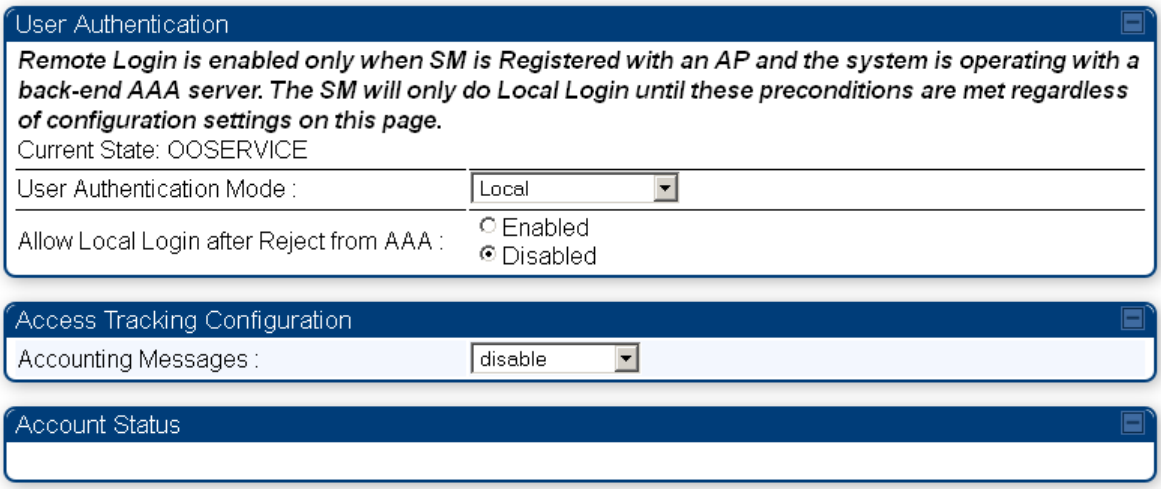


Table 20 SM User Authentication and Access Tracking attributes

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 is 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 is 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 21).

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 or either.

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 21 Device data accounting RADIUS attributes

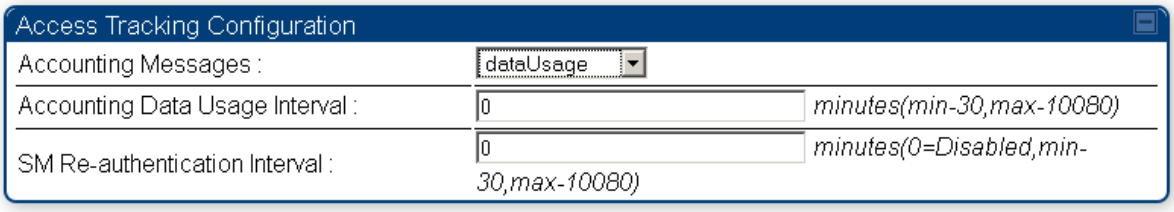
Sender	Message	Attribute	Value	Description
AP	Accounting -Request	Acct-Status-Type	1 - Start	This message is sent every time a SM registers with an AP and after the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC and increments after every start message sent of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

Sender	Message	Attribute	Value	Description
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	
		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).	

Sender	Message	Attribute	Value	Description
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Session-Time	Uptime of the SM session.	
		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 22 RADIUS accounting messages configuration



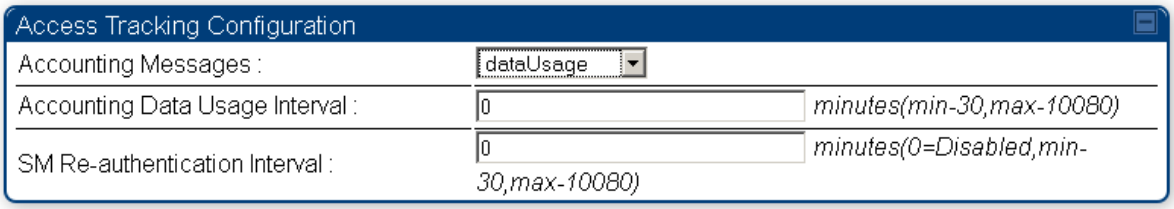
The data accounting message data is based on the SM statistics that the AP maintains and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify 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 is 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 are 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 23 Device re-authentication configuration



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 continues normal operation
- **Reject**: The SM de-registers and attempts network entry again after 1 minute and then if rejected will attempt re-entry every 15 minutes
- **Timeout or other error**: The SM remains in the session and attempt 5 times to re-authenticate with the RADIUS-REQUEST message. If these attempts fail, then the SM goes out of the session and proceeds 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 is 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-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 are 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 becomes 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 are ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) or 255.255.255.0 (NAT enabled) and Cambium-Canopy-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 as mentioned below:

- 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).

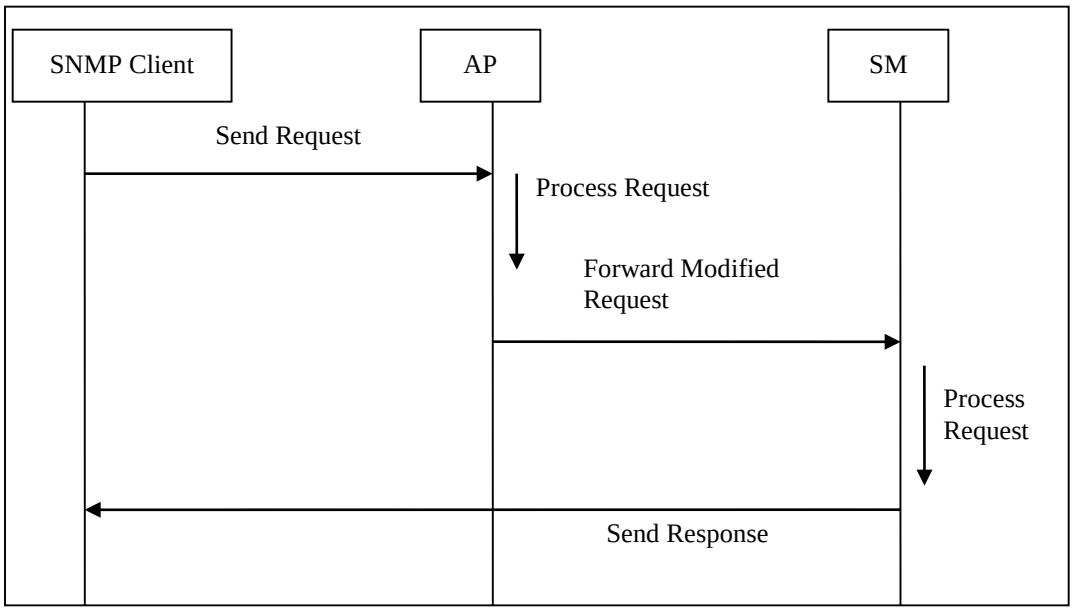
Traps from the Agent

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 a 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.)

Figure 15 SNMP Proxy flow



Configuration of Slave Devices

The Slave Devices (SMs) must be configured with a local IP address with the appropriate gateway setup.

The IP Configurations of the System must be such that the slave Ethernet interface and the SNMP Client are not on the same subnet. This scenario will cause all traffic from the slave devices to the SNMP Client to be sent out via its Ethernet interface, preventing routing back to the SNMP Client.

SNMP Proxy UDP Port

The SNMP Proxy is listening for SNMP requests to forward on UDP port 61002. It forwards the request to the slave device (SM) using UDP port 161.

Packet Format

The first OID sent in an SNMP request needs be modified to include the MAC address of the slave device Remaining OIDs continue to be the same as slave OIDs:

.SlaveOID. <MAC>

.SlaveOID

.SlaveOID

<MAC> = the MAC Address of the Registered Slave Device to which the request needs to be forwarded by the SNMP Proxy. Each byte of the MAC Address is encoded as a separate integer. Thus the MAC contains the information for 6 integers:

SlaveOID = the OID to query in the Slave device. This is the actual OID that is implemented within the MIB of the slave device.

SNMP Proxy Example - Get

SM MAC: 0a-00-3e-a0-00-a5; Converted to decimal: 10.0.62.160.0.165

AP IP: 10.120.153.6

Community String: Canopy

OID: whispSMConfig rFScanList .1.3.6.1.4.1.161.19.3.2.1.1.0

```
snmpget -p 61002 -v 2 -c Canopy 10.120.153.6
.1.3.6.1.4.1.161.19.3.2.1.1.0.10.0.62.160.0.165
```

This returns the following:

```
.1.3.6.1.4.1.161.19.3.2.1.1.0
Value (OctetString): 547500, 548000, 548500, 549000, 549500, 550000, 550500,
551000, 551500, 552000
```

SNMP Proxy Example - Get Multiple OIDs

This example uses the same AP and SM as above.

OIDs: whispSMStatus radioDbm .1.3.6.1.4.1.161.19.3.2.2.8.0

whispSMStatus registeredToAp .1.3.6.1.4.1.161.19.3.2.2.9.0

whispSMStatus adaptRate .1.3.6.1.4.1.161.19.3.2.2.20.0

```
snmpget -p 61002 -v 2 -c Canopy 10.120.153.6
.1.3.6.1.4.1.161.19.3.2.2.8.0.10.0.62.160.0.165 1.3.6.1.4.1.161.19.3.2.2.9.0
.1.3.6.1.4.1.161.19.3.2.2.20.0
Value (OctetString): -53.6

.1.3.6.1.4.1.161.19.3.2.2.9.0
Value (OctetString): 0a-00-3e-a0-07-7c

.1.3.6.1.4.1.161.19.3.2.2.20.0
Value (OctetString): VC  18 Rate 6X/4X    VC 255 Rate 6X/1X
```

SNMP Proxy Example - Set

Note: For SNMP writes to work, the SNMP Community String 1 Permissions must be set to Read / Write.

OID: whispSMConfig lanIpSm .1.3.6.1.4.1.161.19.3.2.1.3.0

```
snmpset -p 61002 -v 2 -c Canopy 10.120.153.6
.1.3.6.1.4.1.161.19.3.2.1.3.0.10.0.62.160.0.165 a 169.254.1.2
.1.3.6.1.4.1.161.19.3.2.1.3.0
Value (IpAddress): 169.254.1.2
```

SNMP Trap Notification for Slave Devices

The SNMP Proxy will not forward traps. The Slave devices must be configured to send traps directly to the SNMP Trap Receiver.

SNMP Proxy Errors - Other

If there is an error there will not be a response sent back to the SNMP agent. Possible errors include:

- Community String incorrect
- SM with that MAC address is not registered to that AP
- SNMP Read / Write is not enabled
- OID incorrect

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, refer *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 24.

Table 24 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://support.cambiumnetworks.com/pmp/software/index.php?tag=pmp450

   ⚠ 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 3-84.
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.

Box MIB Objects

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

Table 25 Box MIB Objects (common to AP and SM)

name	oid	valueType
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
calibrationStatusBool.0	.1.3.6.1.4.1.161.19.3.3.1.109.0	Integer
calibrationStatusBox.0	.1.3.6.1.4.1.161.19.3.3.1.110.0	OctetString
radioEngKeyed.0	.1.3.6.1.4.1.161.19.3.3.1.111.0	Integer
bridgeCbFecStatfloods.0	.1.3.6.1.4.1.161.19.3.3.1.112.0	Counter32
bridgeCbRFStatfloods.0	.1.3.6.1.4.1.161.19.3.3.1.113.0	Counter32
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
encryptionConfig.0	.1.3.6.1.4.1.161.19.3.3.2.148.0	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
region.0	.1.3.6.1.4.1.161.19.3.3.2.207.0	Integer
regionAsia.0	.1.3.6.1.4.1.161.19.3.3.2.208.0	Integer
regionEurope.0	.1.3.6.1.4.1.161.19.3.3.2.209.0	Integer
regionNorthAmerica.0	.1.3.6.1.4.1.161.19.3.3.2.210.0	Integer
regionOceania.0	.1.3.6.1.4.1.161.19.3.3.2.211.0	Integer
regionSouthAmerica.0	.1.3.6.1.4.1.161.19.3.3.2.212.0	Integer
regionOtherRegulatory.0	.1.3.6.1.4.1.161.19.3.3.2.213.0	Integer
receiveQualityDebug.0	.1.3.6.1.4.1.161.19.3.3.2.215.0	Integer
apType.0	.1.3.6.1.4.1.161.19.3.3.2.216.0	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
whispBridgeMacAddr.4	.1.3.6.1.4.1.161.19.3.3.4.1.1.4	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
whispBridgeDesLuid.4	.1.3.6.1.4.1.161.19.3.3.4.1.2.4	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
whispBridgeAge.4	.1.3.6.1.4.1.161.19.3.3.4.1.3.4	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
whispBridgeExt.4	.1.3.6.1.4.1.161.19.3.3.4.1.4.4	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
whispBridgeHash.4	.1.3.6.1.4.1.161.19.3.3.4.1.5.4	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.1.5472500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5472500	Integer
frequency.1.5475000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5475000	Integer
frequency.1.5477500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5477500	Integer
frequency.1.5480000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5480000	Integer
frequency.1.5482500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5482500	Integer
frequency.1.5485000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5485000	Integer
frequency.1.5487500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5487500	Integer
frequency.1.5490000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5490000	Integer
frequency.1.5492500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5492500	Integer
frequency.1.5495000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5495000	Integer
frequency.1.5497500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5497500	Integer
frequency.1.5500000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5500000	Integer
frequency.1.5502500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5502500	Integer
frequency.1.5505000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5505000	Integer
frequency.1.5507500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5507500	Integer
frequency.1.5510000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5510000	Integer
frequency.1.5512500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5512500	Integer
frequency.1.5515000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5515000	Integer
frequency.1.5517500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5517500	Integer
frequency.1.5520000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5520000	Integer
frequency.1.5522500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5522500	Integer
frequency.1.5525000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5525000	Integer
frequency.1.5527500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5527500	Integer
frequency.1.5530000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5530000	Integer
frequency.1.5532500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5532500	Integer
frequency.1.5535000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5535000	Integer

frequency.1.5537500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5537500	Integer
frequency.1.5540000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5540000	Integer
frequency.1.5542500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5542500	Integer
frequency.1.5545000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5545000	Integer
frequency.1.5547500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5547500	Integer
frequency.1.5550000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5550000	Integer
frequency.1.5552500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5552500	Integer
frequency.1.5555000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5555000	Integer
frequency.1.5557500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5557500	Integer
frequency.1.5560000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5560000	Integer
frequency.1.5562500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5562500	Integer
frequency.1.5565000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5565000	Integer
frequency.1.5567500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5567500	Integer
frequency.1.5570000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5570000	Integer
frequency.1.5572500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5572500	Integer
frequency.1.5575000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5575000	Integer
frequency.1.5577500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5577500	Integer
frequency.1.5580000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5580000	Integer
frequency.1.5582500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5582500	Integer
frequency.1.5585000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5585000	Integer
frequency.1.5587500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5587500	Integer
frequency.1.5590000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5590000	Integer
frequency.1.5592500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5592500	Integer
frequency.1.5595000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5595000	Integer
frequency.1.5597500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5597500	Integer
frequency.1.5652500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5652500	Integer
frequency.1.5655000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5655000	Integer
frequency.1.5657500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5657500	Integer
frequency.1.5660000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5660000	Integer
frequency.1.5662500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5662500	Integer

frequency.1.5665000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5665000	Integer
frequency.1.5667500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5667500	Integer
frequency.1.5670000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5670000	Integer
frequency.1.5672500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5672500	Integer
frequency.1.5675000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5675000	Integer
frequency.1.5677500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5677500	Integer
frequency.1.5680000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5680000	Integer
frequency.1.5682500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5682500	Integer
frequency.1.5685000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5685000	Integer
frequency.1.5687500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5687500	Integer
frequency.1.5690000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5690000	Integer
frequency.1.5692500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5692500	Integer
frequency.1.5695000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5695000	Integer
frequency.1.5697500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5697500	Integer
frequency.1.5700000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5700000	Integer
frequency.1.5702500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5702500	Integer
frequency.1.5705000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5705000	Integer
frequency.1.5707500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5707500	Integer
frequency.1.5710000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5710000	Integer
frequency.1.5712500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5712500	Integer
frequency.1.5715000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5715000	Integer
frequency.1.5717500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5717500	Integer
frequency.1.5720000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5720000	Integer
frequency.1.5722500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5722500	Integer
frequency.1.5730000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5730000	Integer
frequency.1.5732500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5732500	Integer
frequency.1.5735000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5735000	Integer
frequency.1.5737500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5737500	Integer
frequency.1.5740000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5740000	Integer
frequency.1.5742500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5742500	Integer

frequency.1.5745000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5745000	Integer
frequency.1.5747500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5747500	Integer
frequency.1.5750000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5750000	Integer
frequency.1.5752500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5752500	Integer
frequency.1.5755000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5755000	Integer
frequency.1.5757500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5757500	Integer
frequency.1.5760000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5760000	Integer
frequency.1.5762500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5762500	Integer
frequency.1.5765000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5765000	Integer
frequency.1.5767200	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5767200	Integer
frequency.1.5770000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5770000	Integer
frequency.1.5772500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5772500	Integer
frequency.1.5775000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5775000	Integer
frequency.1.5777500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5777500	Integer
frequency.1.5780000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5780000	Integer
frequency.1.5782500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5782500	Integer
frequency.1.5785000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5785000	Integer
frequency.1.5787500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5787500	Integer
frequency.1.5790000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5790000	Integer
frequency.1.5792500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5792500	Integer
frequency.1.5795000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5795000	Integer
frequency.1.5797500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5797500	Integer
frequency.1.5800000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5800000	Integer
frequency.1.5802500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5802500	Integer
frequency.1.5805000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5805000	Integer
frequency.1.5807000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5807000	Integer
frequency.1.5810000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5810000	Integer
frequency.1.5812500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5812500	Integer
frequency.1.5815000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5815000	Integer
frequency.1.5817500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5817500	Integer

frequency.1.5820000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5820000	Integer
frequency.1.5822500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5822500	Integer
frequency.1.5825000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5825000	Integer
frequency.1.5827500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5827500	Integer
frequency.1.5830000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5830000	Integer
frequency.1.5832500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5832500	Integer
frequency.1.5835000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5835000	Integer
frequency.1.5837500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5837500	Integer
frequency.1.5840000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5840000	Integer
frequency.1.5842500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5842500	Integer
frequency.1.5845000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5845000	Integer
radioConfigIndex.1	.1.3.6.1.4.1.161.19.3.3.16.1.1.1.1	Integer
radioFrequencyBand.1	.1.3.6.1.4.1.161.19.3.3.16.1.1.2.1	Integer

SM MIB Objects

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

Table 26 SM MIB Objects

name	oid	valueType
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
lowPriorityUplinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.56.0	Integer
lowPriorityDownlinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.57.0	Integer
hiPriorityChannel.0	.1.3.6.1.4.1.161.19.3.2.1.58.0	Integer
hiPriorityUplinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.59.0	Integer
hiPriorityDownlinkCIR.0	.1.3.6.1.4.1.161.19.3.2.1.60.0	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
upLnkMaxBurstDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.128.0	Integer
dwnLnkMaxBurstDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.129.0	Integer
cyclicPrefixScan.0	.1.3.6.1.4.1.161.19.3.2.1.130.0	OctetString
bandwidthScan.0	.1.3.6.1.4.1.161.19.3.2.1.131.0	OctetString
apSelection.0	.1.3.6.1.4.1.161.19.3.2.1.132.0	Integer
radioBandscanConfig.0	.1.3.6.1.4.1.161.19.3.2.1.133.0	Integer
allowedIPAccessNMLength1.0	.1.3.6.1.4.1.161.19.3.2.1.138.0	Integer
allowedIPAccessNMLength2.0	.1.3.6.1.4.1.161.19.3.2.1.139.0	Integer
allowedIPAccessNMLength3.0	.1.3.6.1.4.1.161.19.3.2.1.140.0	Integer
naptRemoteManage.0	.1.3.6.1.4.1.161.19.3.2.1.141.0	Integer
spectrumAnalysisScanBandwidth.0	.1.3.6.1.4.1.161.19.3.2.1.142.0	Integer
berDeModSelect.0	.1.3.6.1.4.1.161.19.3.2.1.143.0	Integer
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

calibrationStatus.0	.1.3.6.1.4.1.161.19.3.2.2.7.0	OctetString
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
fragmentsReceived1XVertical.0	.1.3.6.1.4.1.161.19.3.2.2.87.0	Counter32
fragmentsReceived2XVertical.0	.1.3.6.1.4.1.161.19.3.2.2.88.0	Counter32
fragmentsReceived3XVertical.0	.1.3.6.1.4.1.161.19.3.2.2.89.0	Counter32
fragmentsReceived4XVertical.0	.1.3.6.1.4.1.161.19.3.2.2.90.0	Counter32
signalToNoiseRatioSMVertical.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
signalToNoiseRatioSMHorizontal.0	.1.3.6.1.4.1.161.19.3.2.2.106.0	Integer
maxRadioDbmDeprecated.0	.1.3.6.1.4.1.161.19.3.2.2.107.0	Integer
signalStrengthRatio.0	.1.3.6.1.4.1.161.19.3.2.2.108.0	OctetString
fragmentsReceived1XHorizontal.0	.1.3.6.1.4.1.161.19.3.2.2.109.0	Counter32
fragmentsReceived2XHorizontal.0	.1.3.6.1.4.1.161.19.3.2.2.110.0	Counter32
fragmentsReceived3XHorizontal.0	.1.3.6.1.4.1.161.19.3.2.2.111.0	Counter32
fragmentsReceived4XHorizontal.0	.1.3.6.1.4.1.161.19.3.2.2.112.0	Counter32
radioDbmHorizontal.0	.1.3.6.1.4.1.161.19.3.2.2.117.0	OctetString
radioDbmVertical.0	.1.3.6.1.4.1.161.19.3.2.2.118.0	OctetString
bridgecbDownlinkMaxBurstBitRate.0	.1.3.6.1.4.1.161.19.3.2.2.119.0	Gauge
bridgecbUplinkMaxBurstBitRate.0	.1.3.6.1.4.1.161.19.3.2.2.120.0	Gauge
currentCyclicPrefix.0	.1.3.6.1.4.1.161.19.3.2.2.121.0	Integer
currentBandwidth.0	.1.3.6.1.4.1.161.19.3.2.2.122.0	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
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
clearLinkStats.0	.1.3.6.1.4.1.161.19.3.2.8.1.0	Integer
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
calibrationStatusBool.0	.1.3.6.1.4.1.161.19.3.3.1.109.0	Integer
calibrationStatusBox.0	.1.3.6.1.4.1.161.19.3.3.1.110.0	OctetString
radioEngKeyed.0	.1.3.6.1.4.1.161.19.3.3.1.111.0	Integer
bridgeCbFecStatfloods.0	.1.3.6.1.4.1.161.19.3.3.1.112.0	Counter32
bridgeCbRFStatfloods.0	.1.3.6.1.4.1.161.19.3.3.1.113.0	Counter32
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
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
encryptionConfig.0	.1.3.6.1.4.1.161.19.3.3.2.148.0	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
region.0	.1.3.6.1.4.1.161.19.3.3.2.207.0	Integer
regionAsia.0	.1.3.6.1.4.1.161.19.3.3.2.208.0	Integer
regionEurope.0	.1.3.6.1.4.1.161.19.3.3.2.209.0	Integer
regionNorthAmerica.0	.1.3.6.1.4.1.161.19.3.3.2.210.0	Integer
regionOceania.0	.1.3.6.1.4.1.161.19.3.3.2.211.0	Integer

regionSouthAmerica.0	.1.3.6.1.4.1.161.19.3.3.2.212.0	Integer
regionOtherRegulatory.0	.1.3.6.1.4.1.161.19.3.3.2.213.0	Integer
receiveQualityDebug.0	.1.3.6.1.4.1.161.19.3.3.2.215.0	Integer
apType.0	.1.3.6.1.4.1.161.19.3.3.2.216.0	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
whispVID.1	.1.3.6.1.4.1.161.19.3.3.8.1.1.1	Integer
whispVType.1	.1.3.6.1.4.1.161.19.3.3.8.1.2.1	OctetString
whispVAge.1	.1.3.6.1.4.1.161.19.3.3.8.1.3.1	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.1.5472500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5472500	Integer
frequency.1.5475000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5475000	Integer
frequency.1.5477500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5477500	Integer
frequency.1.5480000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5480000	Integer
frequency.1.5482500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5482500	Integer
frequency.1.5485000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5485000	Integer
frequency.1.5487500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5487500	Integer
frequency.1.5490000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5490000	Integer
frequency.1.5492500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5492500	Integer
frequency.1.5495000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5495000	Integer
frequency.1.5497500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5497500	Integer
frequency.1.5500000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5500000	Integer

frequency.1.5502500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5502500	Integer
frequency.1.5505000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5505000	Integer
frequency.1.5507500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5507500	Integer
frequency.1.5510000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5510000	Integer
frequency.1.5512500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5512500	Integer
frequency.1.5515000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5515000	Integer
frequency.1.5517500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5517500	Integer
frequency.1.5520000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5520000	Integer
frequency.1.5522500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5522500	Integer
frequency.1.5525000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5525000	Integer
frequency.1.5527500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5527500	Integer
frequency.1.5530000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5530000	Integer
frequency.1.5532500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5532500	Integer
frequency.1.5535000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5535000	Integer
frequency.1.5537500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5537500	Integer
frequency.1.5540000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5540000	Integer
frequency.1.5542500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5542500	Integer
frequency.1.5545000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5545000	Integer
frequency.1.5547500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5547500	Integer
frequency.1.5550000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5550000	Integer
frequency.1.5552500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5552500	Integer
frequency.1.5555000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5555000	Integer
frequency.1.5557500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5557500	Integer
frequency.1.5560000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5560000	Integer
frequency.1.5562500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5562500	Integer
frequency.1.5565000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5565000	Integer
frequency.1.5567500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5567500	Integer
frequency.1.5570000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5570000	Integer
frequency.1.5572500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5572500	Integer
frequency.1.5575000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5575000	Integer

frequency.1.5577500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5577500	Integer
frequency.1.5580000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5580000	Integer
frequency.1.5582500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5582500	Integer
frequency.1.5585000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5585000	Integer
frequency.1.5587500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5587500	Integer
frequency.1.5590000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5590000	Integer
frequency.1.5592500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5592500	Integer
frequency.1.5595000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5595000	Integer
frequency.1.5597500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5597500	Integer
frequency.1.5600000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5600000	Integer
frequency.1.5602500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5602500	Integer
frequency.1.5605000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5605000	Integer
frequency.1.5607500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5607500	Integer
frequency.1.5610000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5610000	Integer
frequency.1.5612500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5612500	Integer
frequency.1.5615000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5615000	Integer
frequency.1.5617500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5617500	Integer
frequency.1.5620000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5620000	Integer
frequency.1.5622500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5622500	Integer
frequency.1.5625000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5625000	Integer
frequency.1.5627500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5627500	Integer
frequency.1.5630000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5630000	Integer
frequency.1.5632500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5632500	Integer
frequency.1.5635000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5635000	Integer
frequency.1.5637500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5637500	Integer
frequency.1.5640000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5640000	Integer
frequency.1.5642500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5642500	Integer
frequency.1.5645000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5645000	Integer
frequency.1.5647500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5647500	Integer
frequency.1.5650000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5650000	Integer

frequency.1.5652500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5652500	Integer
frequency.1.5655000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5655000	Integer
frequency.1.5657500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5657500	Integer
frequency.1.5660000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5660000	Integer
frequency.1.5662500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5662500	Integer
frequency.1.5665000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5665000	Integer
frequency.1.5667500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5667500	Integer
frequency.1.5670000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5670000	Integer
frequency.1.5672500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5672500	Integer
frequency.1.5675000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5675000	Integer
frequency.1.5677500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5677500	Integer
frequency.1.5680000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5680000	Integer
frequency.1.5682500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5682500	Integer
frequency.1.5685000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5685000	Integer
frequency.1.5687500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5687500	Integer
frequency.1.5690000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5690000	Integer
frequency.1.5692500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5692500	Integer
frequency.1.5695000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5695000	Integer
frequency.1.5697500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5697500	Integer
frequency.1.5700000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5700000	Integer
frequency.1.5702500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5702500	Integer
frequency.1.5705000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5705000	Integer
frequency.1.5707500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5707500	Integer
frequency.1.5710000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5710000	Integer
frequency.1.5712500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5712500	Integer
frequency.1.5715000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5715000	Integer
frequency.1.5717500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5717500	Integer
frequency.1.5720000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5720000	Integer
frequency.1.5722500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5722500	Integer
frequency.1.5730000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5730000	Integer

frequency.1.5732500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5732500	Integer
frequency.1.5735000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5735000	Integer
frequency.1.5737500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5737500	Integer
frequency.1.5740000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5740000	Integer
frequency.1.5742500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5742500	Integer
frequency.1.5745000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5745000	Integer
frequency.1.5747500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5747500	Integer
frequency.1.5750000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5750000	Integer
frequency.1.5752500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5752500	Integer
frequency.1.5755000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5755000	Integer
frequency.1.5757500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5757500	Integer
frequency.1.5760000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5760000	Integer
frequency.1.5762500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5762500	Integer
frequency.1.5765000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5765000	Integer
frequency.1.5767200	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5767200	Integer
frequency.1.5770000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5770000	Integer
frequency.1.5772500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5772500	Integer
frequency.1.5775000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5775000	Integer
frequency.1.5777500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5777500	Integer
frequency.1.5780000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5780000	Integer
frequency.1.5782500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5782500	Integer
frequency.1.5785000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5785000	Integer
frequency.1.5787500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5787500	Integer
frequency.1.5790000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5790000	Integer
frequency.1.5792500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5792500	Integer
frequency.1.5795000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5795000	Integer
frequency.1.5797500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5797500	Integer
frequency.1.5800000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5800000	Integer
frequency.1.5802500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5802500	Integer
frequency.1.5805000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5805000	Integer

frequency.1.5807000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5807000	Integer
frequency.1.5810000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5810000	Integer
frequency.1.5812500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5812500	Integer
frequency.1.5815000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5815000	Integer
frequency.1.5817500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5817500	Integer
frequency.1.5820000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5820000	Integer
frequency.1.5822500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5822500	Integer
frequency.1.5825000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5825000	Integer
frequency.1.5827500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5827500	Integer
frequency.1.5830000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5830000	Integer
frequency.1.5832500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5832500	Integer
frequency.1.5835000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5835000	Integer
frequency.1.5837500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5837500	Integer
frequency.1.5840000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5840000	Integer
frequency.1.5842500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5842500	Integer
frequency.1.5845000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5845000	Integer
radioConfigIndex.1	.1.3.6.1.4.1.161.19.3.3.16.1.1.1.1	Integer
radioFrequencyBand.1	.1.3.6.1.4.1.161.19.3.3.16.1.1.2.1	Integer

AP MIB Objects

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

Table 27 AP MIB Objects

name	oid	valueType
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
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
gpsOutputEn.0	.1.3.6.1.4.1.161.19.3.1.1.107.0	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
upLnkMaxBurstDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.128.0	Integer
dwnLnkMaxBurstDataRate.0	.1.3.6.1.4.1.161.19.3.2.1.129.0	Integer
rfPPPoEPADIForwarding.0	.1.3.6.1.4.1.161.19.3.1.1.210.0	Integer
allowedIPAccessNMLength1.0	.1.3.6.1.4.1.161.19.3.2.1.138.0	Integer
allowedIPAccessNMLength2.0	.1.3.6.1.4.1.161.19.3.2.1.139.0	Integer
allowedIPAccessNMLength3.0	.1.3.6.1.4.1.161.19.3.2.1.140.0	Integer
bridgeFloodUnknownsEnable.0	.1.3.6.1.4.1.161.19.3.1.1.214.0	Integer
berModSelect.0	.1.3.6.1.4.1.161.19.3.1.1.215.0	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
signalToNoiseRatioDownLinkVertical.0	.1.3.6.1.4.1.161.19.3.1.2.2.33.0	Integer
signalToNoiseRatioUpLinkVertical.0	.1.3.6.1.4.1.161.19.3.1.2.2.34.0	Integer
signalToNoiseRatioDownLinkHorizontal.0	.1.3.6.1.4.1.161.19.3.1.2.2.51.0	Integer
signalToNoiseRatioUpLinkHorizontal.0	.1.3.6.1.4.1.161.19.3.1.2.2.52.0	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
gpsFreeRun.0	.1.3.6.1.4.1.161.19.3.1.3.17.0	Integer
intelligentGPSSyncStatus.0	.1.3.6.1.4.1.161.19.3.1.3.18.0	Integer
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
linkFragmentsReceived1XVertical.2	.1.3.6.1.4.1.161.19.3.1.4.1.70.2	Counter32
linkFragmentsReceived2XVertical.2	.1.3.6.1.4.1.161.19.3.1.4.1.71.2	Counter32
linkFragmentsReceived3XVertical.2	.1.3.6.1.4.1.161.19.3.1.4.1.72.2	Counter32

linkFragmentsReceived4XVertical.2	.1.3.6.1.4.1.161.19.3.1.4.1.73.2	Counter32
signalToNoiseRatioVertical.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
linkFragmentsReceived1XHorizontal.2	.1.3.6.1.4.1.161.19.3.1.4.1.80.2	Counter32
linkFragmentsReceived2XHorizontal.2	.1.3.6.1.4.1.161.19.3.1.4.1.81.2	Counter32
linkFragmentsReceived3XHorizontal.2	.1.3.6.1.4.1.161.19.3.1.4.1.82.2	Counter32
linkFragmentsReceived4XHorizontal.2	.1.3.6.1.4.1.161.19.3.1.4.1.83.2	Counter32
signalToNoiseRatioHorizontal.2	.1.3.6.1.4.1.161.19.3.1.4.1.84.2	Integer
linkSignalStrengthRatio.2	.1.3.6.1.4.1.161.19.3.1.4.1.86.2	OctetString
linkRadioDbmHorizontal.2	.1.3.6.1.4.1.161.19.3.1.4.1.87.2	OctetString
linkRadioDbmVertical.2	.1.3.6.1.4.1.161.19.3.1.4.1.88.2	OctetString
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
currentRadioFreqCarrier.0	.1.3.6.1.4.1.161.19.3.1.7.37.0	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
clearLinkTableStats.0	.1.3.6.1.4.1.161.19.3.1.11.1.0	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
calibrationStatusBool.0	.1.3.6.1.4.1.161.19.3.3.1.109.0	Integer
calibrationStatusBox.0	.1.3.6.1.4.1.161.19.3.3.1.110.0	OctetString
radioEngKeyed.0	.1.3.6.1.4.1.161.19.3.3.1.111.0	Integer
bridgeCbFecStatfloods.0	.1.3.6.1.4.1.161.19.3.3.1.112.0	Counter32
bridgeCbRFStatfloods.0	.1.3.6.1.4.1.161.19.3.3.1.113.0	Counter32
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
encryptionConfig.0	.1.3.6.1.4.1.161.19.3.3.2.148.0	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
region.0	.1.3.6.1.4.1.161.19.3.3.2.207.0	Integer
regionAsia.0	.1.3.6.1.4.1.161.19.3.3.2.208.0	Integer

regionEurope.0	.1.3.6.1.4.1.161.19.3.3.2.209.0	Integer
regionNorthAmerica.0	.1.3.6.1.4.1.161.19.3.3.2.210.0	Integer
regionOceania.0	.1.3.6.1.4.1.161.19.3.3.2.211.0	Integer
regionSouthAmerica.0	.1.3.6.1.4.1.161.19.3.3.2.212.0	Integer
regionOtherRegulatory.0	.1.3.6.1.4.1.161.19.3.3.2.213.0	Integer
receiveQualityDebug.0	.1.3.6.1.4.1.161.19.3.3.2.215.0	Integer
apType.0	.1.3.6.1.4.1.161.19.3.3.2.216.0	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
whispBridgeMacAddr.4	.1.3.6.1.4.1.161.19.3.3.4.1.1.4	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
whispBridgeDesLuid.4	.1.3.6.1.4.1.161.19.3.3.4.1.2.4	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
whispBridgeAge.4	.1.3.6.1.4.1.161.19.3.3.4.1.3.4	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
whispBridgeExt.4	.1.3.6.1.4.1.161.19.3.3.4.1.4.4	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
whispBridgeHash.4	.1.3.6.1.4.1.161.19.3.3.4.1.5.4	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.1.5472500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5472500	Integer
frequency.1.5475000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5475000	Integer

frequency.1.5477500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5477500	Integer
frequency.1.5480000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5480000	Integer
frequency.1.5482500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5482500	Integer
frequency.1.5485000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5485000	Integer
frequency.1.5487500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5487500	Integer
frequency.1.5490000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5490000	Integer
frequency.1.5492500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5492500	Integer
frequency.1.5495000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5495000	Integer
frequency.1.5497500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5497500	Integer
frequency.1.5500000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5500000	Integer
frequency.1.5502500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5502500	Integer
frequency.1.5505000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5505000	Integer
frequency.1.5507500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5507500	Integer
frequency.1.5510000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5510000	Integer
frequency.1.5512500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5512500	Integer
frequency.1.5515000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5515000	Integer
frequency.1.5517500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5517500	Integer
frequency.1.5520000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5520000	Integer
frequency.1.5522500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5522500	Integer
frequency.1.5525000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5525000	Integer
frequency.1.5527500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5527500	Integer
frequency.1.5530000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5530000	Integer
frequency.1.5532500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5532500	Integer
frequency.1.5535000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5535000	Integer
frequency.1.5537500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5537500	Integer
frequency.1.5540000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5540000	Integer
frequency.1.5542500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5542500	Integer
frequency.1.5545000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5545000	Integer
frequency.1.5547500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5547500	Integer
frequency.1.5550000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5550000	Integer

frequency.1.5552500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5552500	Integer
frequency.1.5555000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5555000	Integer
frequency.1.5557500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5557500	Integer
frequency.1.5560000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5560000	Integer
frequency.1.5562500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5562500	Integer
frequency.1.5565000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5565000	Integer
frequency.1.5567500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5567500	Integer
frequency.1.5570000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5570000	Integer
frequency.1.5572500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5572500	Integer
frequency.1.5575000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5575000	Integer
frequency.1.5577500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5577500	Integer
frequency.1.5580000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5580000	Integer
frequency.1.5582500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5582500	Integer
frequency.1.5585000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5585000	Integer
frequency.1.5587500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5587500	Integer
frequency.1.5590000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5590000	Integer
frequency.1.5592500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5592500	Integer
frequency.1.5595000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5595000	Integer
frequency.1.5597500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5597500	Integer
frequency.1.5652500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5652500	Integer
frequency.1.5655000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5655000	Integer
frequency.1.5657500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5657500	Integer
frequency.1.5660000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5660000	Integer
frequency.1.5662500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5662500	Integer
frequency.1.5665000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5665000	Integer
frequency.1.5667500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5667500	Integer
frequency.1.5670000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5670000	Integer
frequency.1.5672500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5672500	Integer
frequency.1.5675000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5675000	Integer
frequency.1.5677500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5677500	Integer

frequency.1.5680000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5680000	Integer
frequency.1.5682500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5682500	Integer
frequency.1.5685000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5685000	Integer
frequency.1.5687500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5687500	Integer
frequency.1.5690000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5690000	Integer
frequency.1.5692500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5692500	Integer
frequency.1.5695000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5695000	Integer
frequency.1.5697500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5697500	Integer
frequency.1.5700000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5700000	Integer
frequency.1.5702500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5702500	Integer
frequency.1.5705000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5705000	Integer
frequency.1.5707500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5707500	Integer
frequency.1.5710000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5710000	Integer
frequency.1.5712500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5712500	Integer
frequency.1.5715000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5715000	Integer
frequency.1.5717500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5717500	Integer
frequency.1.5720000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5720000	Integer
frequency.1.5722500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5722500	Integer
frequency.1.5730000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5730000	Integer
frequency.1.5732500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5732500	Integer
frequency.1.5735000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5735000	Integer
frequency.1.5737500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5737500	Integer
frequency.1.5740000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5740000	Integer
frequency.1.5742500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5742500	Integer
frequency.1.5745000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5745000	Integer
frequency.1.5747500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5747500	Integer
frequency.1.5750000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5750000	Integer
frequency.1.5752500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5752500	Integer
frequency.1.5755000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5755000	Integer
frequency.1.5757500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5757500	Integer

frequency.1.5760000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5760000	Integer
frequency.1.5762500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5762500	Integer
frequency.1.5765000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5765000	Integer
frequency.1.5767200	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5767200	Integer
frequency.1.5770000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5770000	Integer
frequency.1.5772500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5772500	Integer
frequency.1.5775000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5775000	Integer
frequency.1.5777500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5777500	Integer
frequency.1.5780000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5780000	Integer
frequency.1.5782500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5782500	Integer
frequency.1.5785000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5785000	Integer
frequency.1.5787500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5787500	Integer
frequency.1.5790000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5790000	Integer
frequency.1.5792500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5792500	Integer
frequency.1.5795000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5795000	Integer
frequency.1.5797500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5797500	Integer
frequency.1.5800000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5800000	Integer
frequency.1.5802500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5802500	Integer
frequency.1.5805000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5805000	Integer
frequency.1.5807000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5807000	Integer
frequency.1.5810000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5810000	Integer
frequency.1.5812500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5812500	Integer
frequency.1.5815000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5815000	Integer
frequency.1.5817500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5817500	Integer
frequency.1.5820000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5820000	Integer
frequency.1.5822500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5822500	Integer
frequency.1.5825000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5825000	Integer
frequency.1.5827500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5827500	Integer
frequency.1.5830000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5830000	Integer
frequency.1.5832500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5832500	Integer

frequency.1.5835000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5835000	Integer
frequency.1.5837500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5837500	Integer
frequency.1.5840000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5840000	Integer
frequency.1.5842500	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5842500	Integer
frequency.1.5845000	.1.3.6.1.4.1.161.19.3.3.15.3.1.1.1.5845000	Integer
radioConfigIndex.1	.1.3.6.1.4.1.161.19.3.3.16.1.1.1.1	Integer
radioFrequencyBand.1	.1.3.6.1.4.1.161.19.3.3.16.1.1.2.1	Integer

New OID to see the number of entries in the NAPT table

In System Release 13.2, we have provided the SNMP OID that returns the number of entries on NAT table.

Table 28 Link Capacity Test tab on AP and SM, new SNMP objects

Name	OID	MIB	Access	Syntax / Description
natTslTableEntries	.1.3.6.1.4.1.161.19.3.1.2.1.141	WHISP-SM-MIB	read-only	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 which allows managers to poll the agents.

Cambium modules can also be configured to send traps to the 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 shut down.
- 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 has the following functions:

- 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.

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/management-tools/cnut/

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 16 AP General Status page

Device Information	
Device Type :	3.6GHz MIMO OFDM - Access Point - 0a-00-3e-40-30-fc
Board Type :	P12 C200
Software Version :	CANOPY 13.2 (Build 32) AP-DES
Board MSN :	6069QA04AY
FPGA Version :	082614
PLD Version :	20
Uptime :	2d, 07:58:27
System Time :	09:20:56 01/03/2011 UTC
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	3600.00 MHz
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Color Code :	36
Max Range :	2 Miles
Transmit Power :	-10 dBm
Temperature :	35 °C / 96 °F

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

Frame Configuration Information	
Data Slots Down :	61
Data Slots Up :	20
Contention Slots :	3

Site Information	
Site Name :	3.65 AP in Temp
Site Contact :	Jonathan
Site Location :	RM Lab

Key Features Information	
Time Updated and Location Code :	10/03/2014 20:23:43 - INTL

The AP's **General Status** tab provides the following read-only fields.

Table 29 AP 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 and whether communications involving the module are secured by DES or AES encryption. If you request technical support, provide the information from this field.
Board Type	This field indicates the series of hardware.
Combo Radio Mode	This field indicates the mode of operation, currently only 'MIMO OFDM Only' is supported.
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 **Country Code** and radio frequency are compliant with respect to their compatibility. PMP 450 equipment shipped to the United States is locked to a Country Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Country Code to comply with local regulatory requirements.
Channel Center Frequency	This field indicates the current operating center frequency, in MHz.
Channel Bandwidth	This field indicates the current size of the channel band used for radio transmission.
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
Color Code	This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
Max Range	This field indicates the setting of the Max Range parameter, which contributes to the way the radio transmits. 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.
Transmitter Output Power	This field indicates the combined power level at which the AP is set to transmit, based on the Country Code and Antenna Gain settings.
Temperature	This field indicates the current operating temperature of the device board.
Registered SM Count	This field indicates how many SMs are registered to the AP.
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. • **No Sync Since Boot up / 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.
Sync Pulse Source	This field indicates the status of the synchronization source: • **Searching** indicates that the unit is searching for a GPS fix • **Timing Port/UGPS** indicates that the module is receiving sync via the timing RJ11 timing port • **Power Port** indicates that the module is receiving sync via the power port (Ethernet port). • **On-board GPS** indicates that the module is receiving sync via the unit's internal GPS module
Maximum Count of Registered SMs	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.

Attribute	Meaning
Data Slots Down	This field indicates the number of frame slots that are designated for use by data traffic 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) **Contention Slots** configured by the operator.
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) Contention Slots configured by the operator.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. The SM uses reserved Contention Slots and unused data slots for bandwidth requests.
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 a SM is displayed below.

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

Figure 17 General Status page of the SM

Device Information	
Device Type :	5.7GHz MIMO OFDM - Subscriber Module - 0a-00-3e-a0-2b-c8
Board Type :	P12 C200
Software Version :	CANOPY 13.2 (Build UARTDEBUG7) AP-DES
FPGA Version :	082614
PLD Version :	16
Uptime :	14:01:42
System Time :	01:38:49 10/03/2014 CDT
Ethernet Interface :	100Base-TX Full Duplex
Antenna Type :	External
Temperature :	46 °C / 114 °F

Subscriber Module Stats	
Session Status :	Ready
Session Uptime :	00:00:00
Registered AP :	n/a
Color Code :	None (None)
Channel Frequency :	None
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Air Delay :	0 ns, approximately 0.000 miles (0 feet)
Receive Power :	n/a
Signal Strength Ratio :	NA
Signal to Noise Ratio :	0 V / 0 H dB
Beacons :	0 %
Transmit Power :	16 dBm

Frame Configuration Information	
Data Slots Down :	61
Data Slots Up :	20
Contention Slots :	3

Region Specific Information	
Regional Code :	United States

Site Information	
Site Name :	5.7 in Temp .13
Site Contact :	No Site Contact
Site Location :	No Site Location

Key Features Information	
Maximum Throughput :	Unlimited
Time Updated and Location Code :	08/27/2014 20:17:50 - INTL

The SM's **General Status** tab provides the following read-only fields.

Table 30 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.
Board Type	This field indicates the series of hardware.
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.
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.
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 Ethernet interface to the SM.
Antenna Type	The current antenna type that has been selected.
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*.
Registered AP	Displays the MAC address and site name of the AP to which the SM is registered to. This parameter provides click-through proxy access to the AP's management interface.

Attribute	Meaning
Color Code	This field displays a value from 0 to 254 indicating the SM's configured color code. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
Channel Frequency	This field lists the current operating frequency of the radio.
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.
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.
Receive Power	This field lists the current combined receive power level, in dBm.
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power.
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.
Beacons	Displays a count of beacons received by the SM in percentage. This value must be typically between 99-100%. If lower than 99%, it indicates a problematic link. This statistic is updated every 16 seconds.
Transmit Power	This field lists the current combined transmit power level, in dBm.
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.

Attribute	Meaning
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. The SM uses reserved Contention Slots and unused data slots for bandwidth requests. If too few reserved Contention Slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced. In a typical cluster, each AP must be set to the same number of Contention Slots to assure proper timing in the send and receive cycles. However, where high incidence of small packets exists, as in a sector that serves several VoIP streams, additional Contention Slots may provide better results. For APs in a cluster of mismatched Contention Slots 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 Contention Slots may increase system performance, depending on traffic mix over time. Use care when changing the Contention slots configuration of only some APs, because changes affect the uplink/downlink ratio and can cause collocation issues. **NOTE** Change Contention slot configuration in an operating, stable system cautiously and with a back-out plan. After changing the Contention slot configuration, monitor the system closely for problems as well as improvements in system performance..
Regional 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 Country 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)

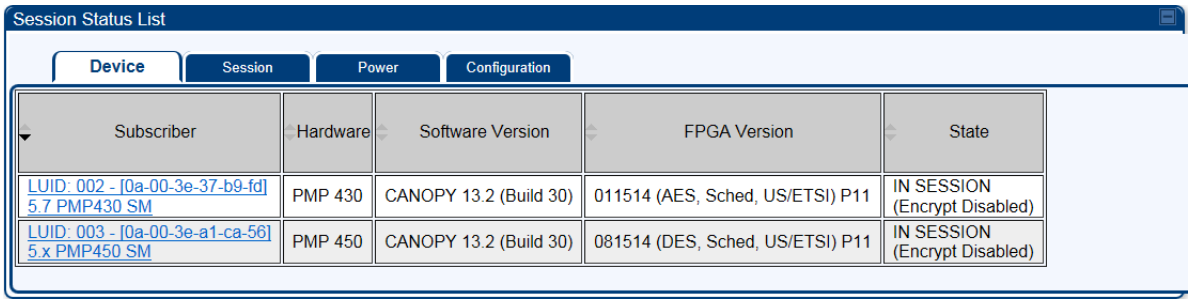
The **Session Status** tab in the Home page provides information about each SM that has registered to the AP. This information is useful for managing and troubleshooting a system. This tab also includes the current active values on each SM for MIR and VLAN, as well as the source of these values, representing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

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

Four tabs breakout SM's Session information: Device, Session, Power and Configuration.

Device tab

Figure 18 Device tab



The Device tab provides information on the Subscriber's LUID and MAC, Hardware, Software, FPGA versions and the state of the SM (Registered and/or encrypted).

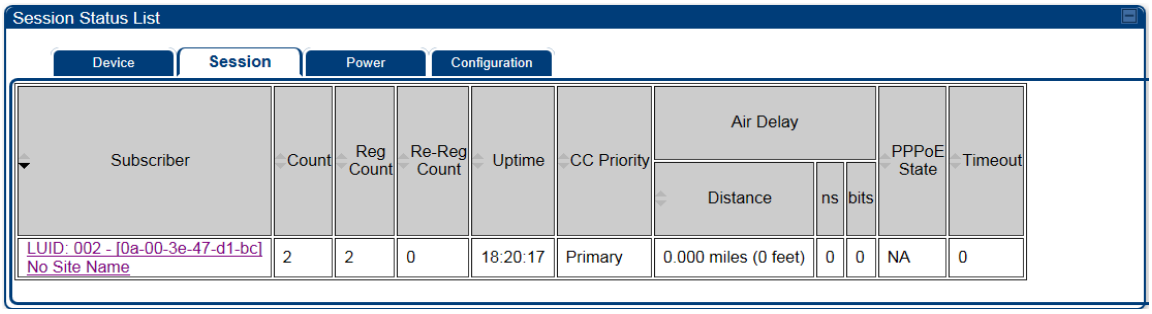
Table 31 Device tab attributes

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name 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 a 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. Site Name 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.
Hardware	This field displays the SMs hardware type.
Software Version	This field displays the software release that operates on the SM, the release date and time of the software.

Attribute	Meaning
FPGA Version	This field displays the version of FPGA that runs on the SM.
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.

Session tab

Figure 19 Session tab



The Session tab provides information on the SMs Session Count, Reg Count, Re-Reg Count, Uptime, Air delay, PPPoE State and Timeouts.

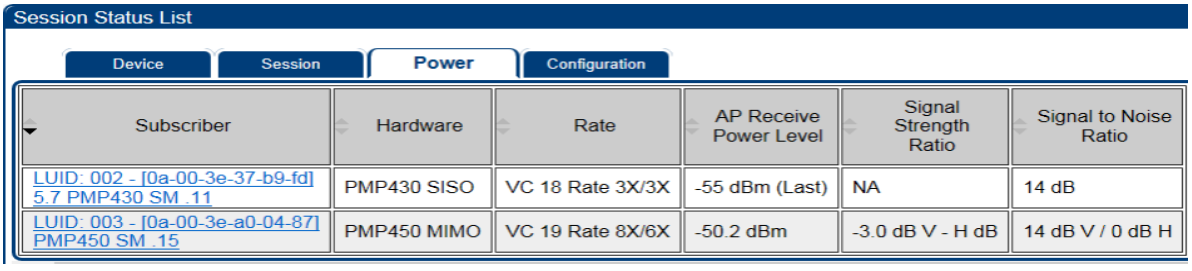
Table 32 Session tab attributes

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name 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 a 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. Site Name 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.
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.

Attribute	Meaning
Reg Count	When a 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).
Re-Reg Count	When a 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: • SM attempts to reregister for having lost communication with the AP. • 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).
Uptime	Once a SM successfully registers to an AP, this timer is started. If a session drops or is interrupted, this timer is reactivated once re-registration is complete.
AirDelay	This field displays the distance of the SM from the AP in meters, nanoseconds and bits. At close distances, the value in this field is unreliable.
PPPoE state	This field displays the current PPPoE state (whether configured) of the SM.
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.

Power tab

Figure 20 Power tab



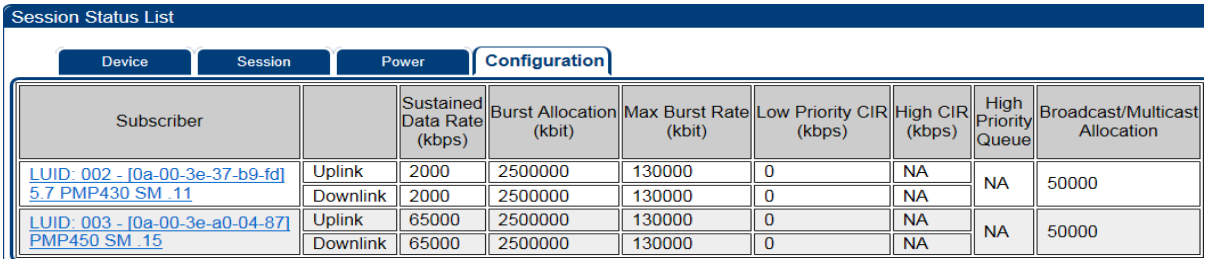
The Power tab provides information on the SMs Hardware State, Current Rate, AP Rx Power, Signal Strength Ratio and Signal to Noise ratio.

Table 33 Power tab attributes

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name 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 a 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. Site Name 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.
Hardware	This field displays the SMs hardware type.
Rate	This field displays whether the high-priority channel is enabled in the SM and the status of rate adapt. For example, if "8X/6X" is listed, the radio is capable of operating at 8X but is currently operating at 6X, due to RF conditions.
AP Receive Power Level	This field indicates the AP's combined receive power level for the listed SM.
Signal Strength Ratio	This field displays the ratio of the Vertical path received signal power to the Horizontal path received signal power. This ratio can be useful for determining multipathing conditions (high vertical to horizontal ratio).
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor.

Configuration tab

Figure 21 Configuration tab



The **Configuration** tab provides information on the SMs Uplink or Downlink (UL/DL) Sustained Data Rate, UL/DL Burst Allocation, UL/DL Burst Rate, UL/DL Low Priority CIR, UL/DL High CIR, UL/DL High Priority Queue Information and the UL/DL Broadcast or Multicast Allocation. This data is refreshed based on the Web Page Auto Update setting on the AP's General Configuration page.

Table 34 Configuration tab attributes

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name 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 a SM loses registration with the AP and then regains registration, the SM retains 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. Site Name 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.
Sustained Data Rate	This field displays the CIR value in kbps that is currently in effect for the SM in both the Uplink and Downlink direction. In the Uplink, this is the specified rate at which each SM registered to this AP is replenished with credits for transmission. In the Downlink, this is the specified rate at which the AP must be replenished with credits (tokens) for transmission to each of the SMs in its sector.
Burst Allocation	This field displays the Burst Allocation value that is currently in effect for the SM in both the Uplink and Downlink direction. In the Uplink, this is the specified maximum amount of data that each SM is allowed to transmit before being recharged at the **Sustained Data Rate (Uplink)** with credits to transmit more. In the Downlink, 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 Data Rate (Downlink)**.
Max Burst Rate	The data rate at which a SM is allowed to burst (until burst allocation limit is reached) before being recharged at the **Sustained Data Rate (Uplink and Downlink individually)** with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Low Priority CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink and downlink (unless CIR is oversubscribed or RF link quality is degraded).
High CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink and downlink (unless CIR is oversubscribed or RF link quality is degraded).
High Priority Queue	Not applicable for PMP 450 products.
Broadcast/Multicast Allocation	This field displays the data rate at which Broadcast and Multicast traffic is sent via the radio link.

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 22 Remote Subscribers tab of the AP

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 expand the window till all lines are shown beginning with time and date stamp.

Time and Date Stamp

The time and date stamp reflect one of the following:

- GPS time and date directly or indirectly received from the CMM.
- NTP time and date from a 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 must 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 23 Event log data

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 35 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.
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 24 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 25 Network Interface tab of the AP

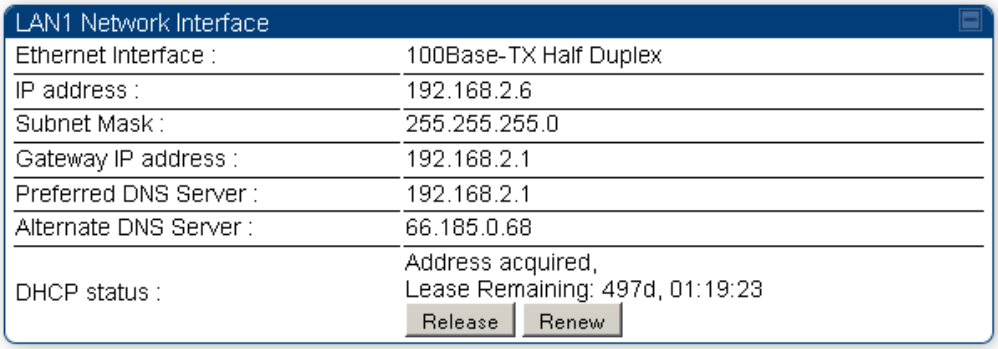
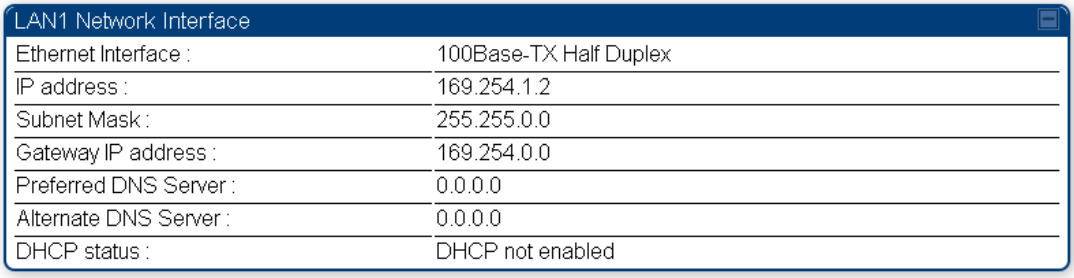


Figure 26 Network Interface tab of the SM



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 27 Layer 2 Neighbors tab

Viewing the Scheduler tab (AP and SM)

Statistics for the Scheduler are displayed as shown below:

Figure 28 Scheduler tab of AP

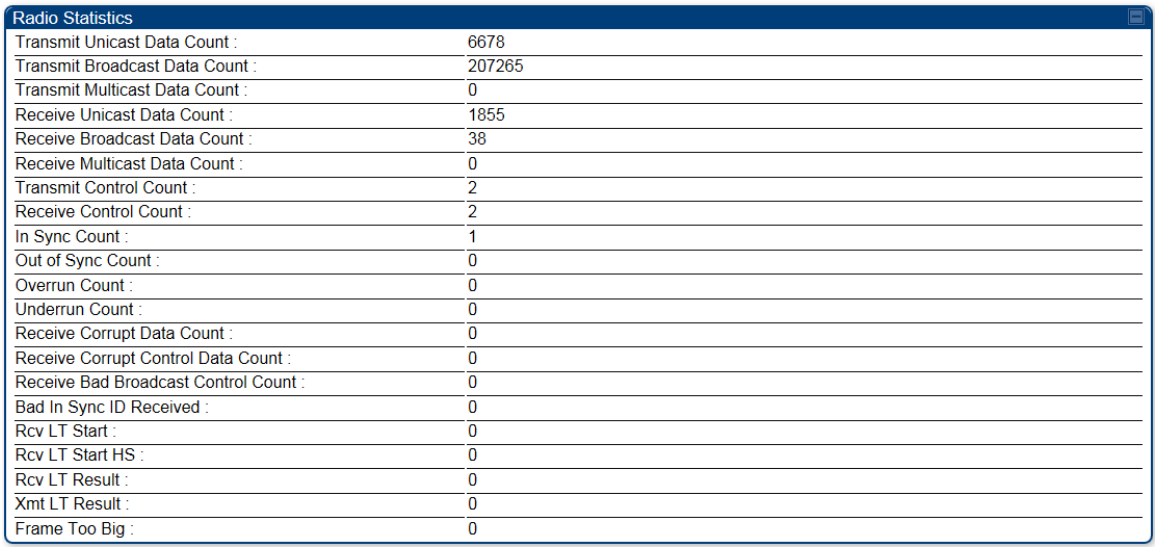


Table 36 Scheduler tab attributes

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
Transmit Multicast Data Count	The total amount of multicast packets transmitted by 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

Event Message	Meaning
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.).
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.
Frame Too Big	This statistics indicates the number of packets received and processed by the radios which were greater than 1529 bytes.

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 29 SM Registration Failures tab of the AP

Table 37 SM Registration Failures tab attributes

Attribute	Meaning
Status 17 Flag 0	No response was received from the AAA server and hence SM is trying to send a session request again.

There is a list of flags from 0 to 20 as shown in Table 38 and the “Flags” can be ignored.

Table 38 Flags status

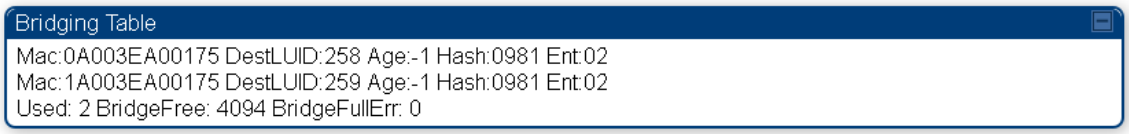
Flag	Meaning
0	Normal
1	Out of Range
2	No Luids
3	BH ReRange
4	Auth Fail
5	Encrypt Fail
6	Power Adjust
7	No VCs
8	Reserve VC Fail
9	Activate VC Fail
10	Hi VC Setup Fail
11	AP Lite Limit Reached
12	Only Ver 9.5+ Allowed
13	Temporary Data VC for AAA
14	AAA Authentication Failure
15	Registration Grant Reject
16	Blank
17	AAA Session Retry
18	AAA Reauth Failure
19	RegReq at zero power
20	RegReq no time ref

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 30 Bridging Table tab of the AP

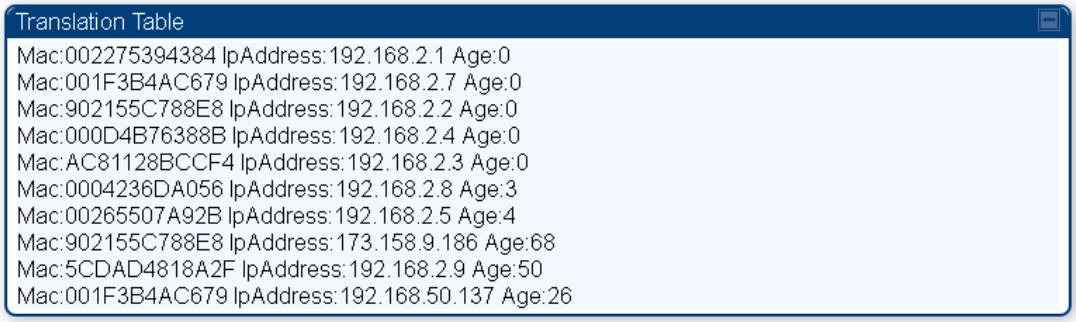


The Bridging Table supports up to 4096 entries.

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 is changed to that of the SM which bridged the packet in the uplink direction.)

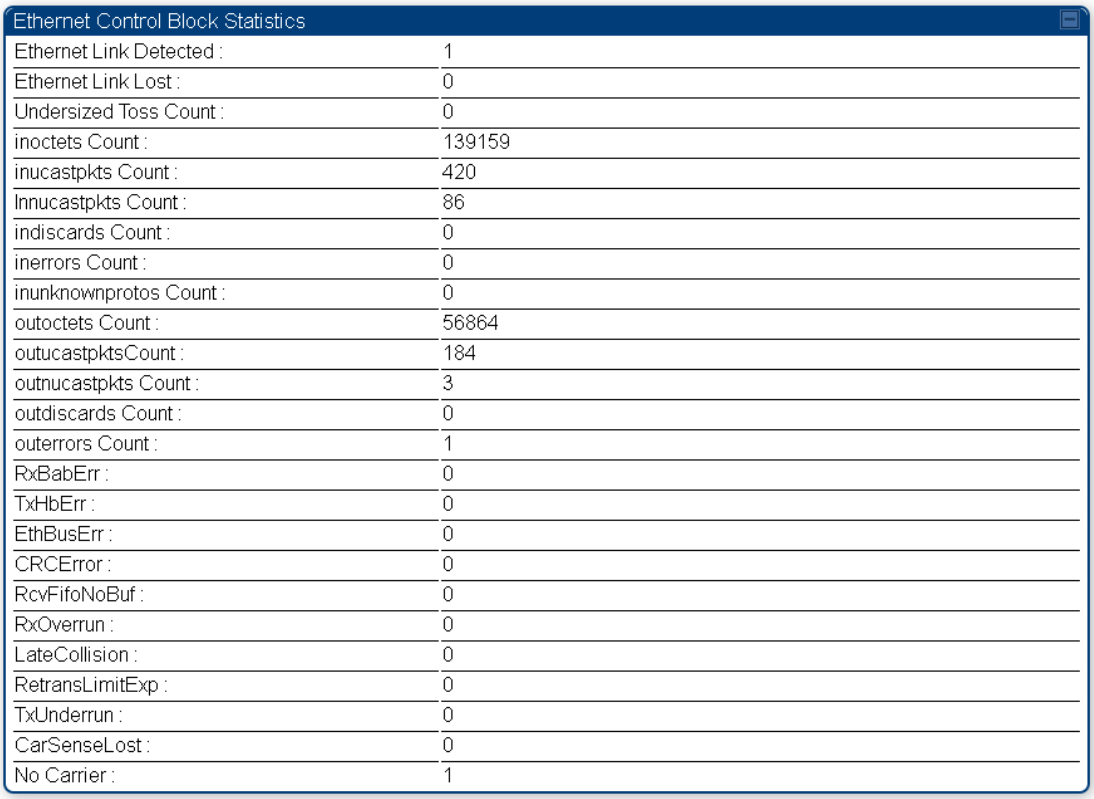
Figure 31 Translation Table tab of the SM



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 32 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 39 Ethernet tab attributes

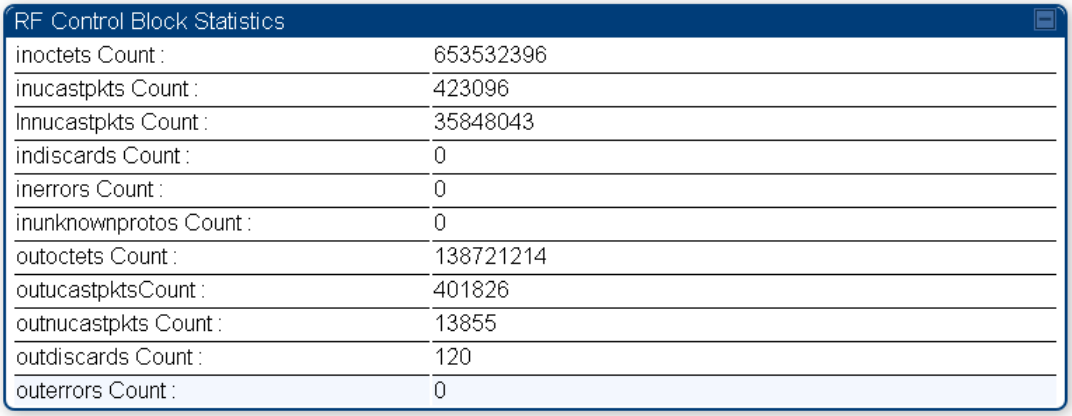
Attribute	Meaning
Ethernet Link Detected	1 indicates that an Ethernet link is established to the radio, 0 indicates that no Ethernet link is established
Ethernet Link Lost	This field indicates a count of how many times the Ethernet link was lost.
Undersized Toss Count	This field indicates the number 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.
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.

Attribute	Meaning
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 occurred.
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 33 Radio tab of the Statistics page, SM



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

Table 40 Radio (Statistics) tab attributes

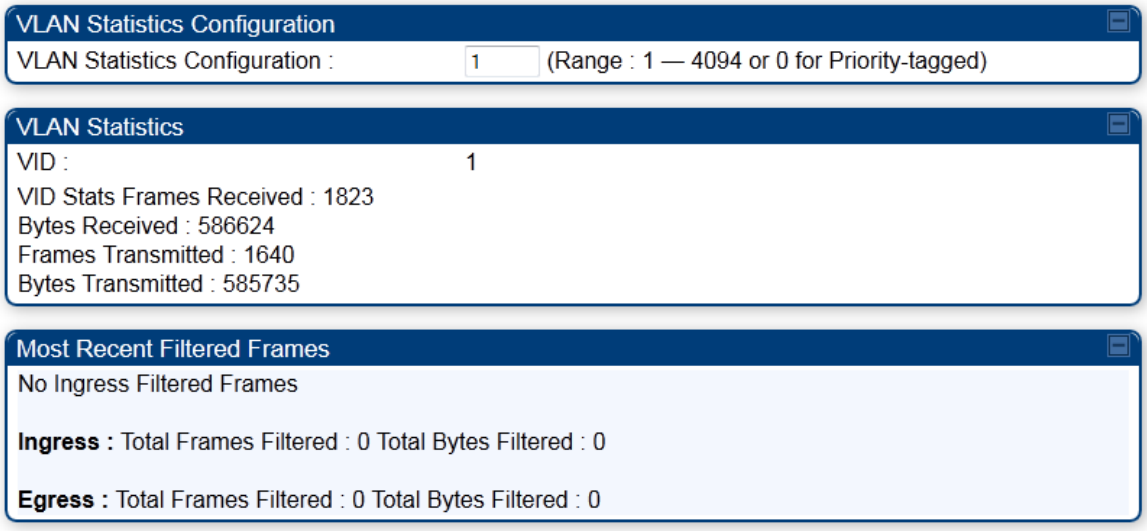
Attribute	Meaning
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Innucastpkts Count	This field 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. This stat is pegged whenever corrupt data is received by software or whenever the RF Software Bridge queue is full. Corrupt data is a very unusual event because all packets are CRC checked by hardware before being passed into software. The likely case for indiscards is if the RF bridge queue is full. If this is the case the radio is most likely PPS limited due to excessive small packet traffic or a problem at the Ethernet interface. If there is a problem at the Ethernet interface there is likely to be discards at the Ethernet as well.
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.)
outerrrors 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 34 VLAN tab of the AP



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

- **Unknown**— this must 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 must 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.

VLAN Remarking and Priority bits configuration

VLAN Remarking

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

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

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

VLAN ID Remarking

SM supports the ability to re-mark the VLAN ID on both upstream and downstream VLAN frames at the Ethernet interface. For instance, a configuration can be added to re-mark VLAN ID ‘x’ to VLAN ID ‘y’ as shown in Table 41. AP does not support VLAN ID remarking.

Table 41 VLAN Remarking Example

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

802.1P Remarking

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

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

VLAN Priority Bits configuration

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

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

Default Port VID

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

The priority bits used in the Q-tag/C-tag are configurable. The configuration can be:

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

MAC Address Mapped VID

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

Provider VID

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

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

Management VID

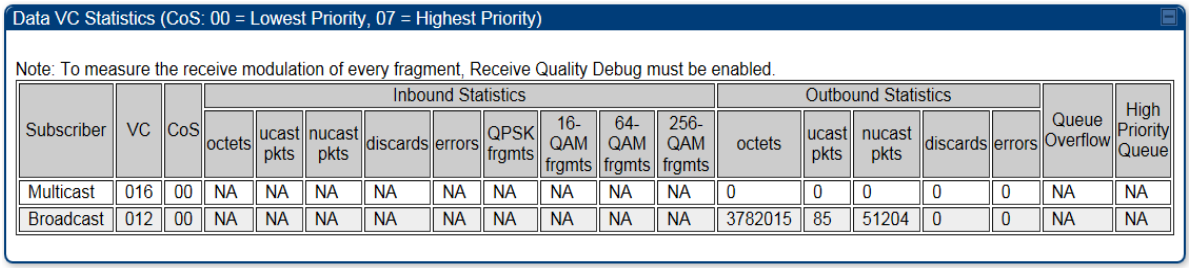
This VID is used to communicate with AP and SM for management purposes. The priority

bits used in the Q-tag are configurable similar to default port VID.

Viewing Data VC Statistics (All)

The **Data VC Statistics** tab displays information about Virtual Channel (VC) used in data communications.

Figure 35 Data VC tab of the AP



The **Data VC** tab displays the fields as explained in Table 42.

Table 42 Data VC tab attributes

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name 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 a SM loses registration with the AP and then regains registration, the SM retains the same LUID.
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.
Inbound Statistics, octets	This field displays how many octets were received on the interface, including those that deliver framing information.
Inbound Statistics, ucastpkts	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Inbound Statistics, nucastpkts	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
Inbound Statistics, discards	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. Inbound discard statistics are incremented similar to the indiscards stat on the RF control block stats page. The sum of all data VC indiscards must be close to the RF control block in discards. If indiscards are evenly distributed across SMs, then the radio is PPS limited due to either excessive small packet transmissions, or a problem at the Ethernet link. If indiscards are contained to one or a few SMs, then there is likely a problem at or underneath the SM which is incrementing the count.

Attribute	Meaning
Inbound Statistics, errors	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
Inbound Statistics, QPSK frgmts	This field displays how many inbound fragments were received via the QPSK modulation scheme.
Inbound Statistics, 16-QAM frgmts	This field displays how many inbound fragments were received via the 16-QAM modulation scheme.
Inbound Statistics, 64-QAM frgmts	This field displays how many inbound fragments were received via the 64-QAM modulation scheme.
Inbound Statistics, 256-QAM frgmts	This field displays how many inbound fragments were received via the 256-QAM modulation scheme.
Outbound Statistics, octets	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
Outbound Statistics, ucastpkts	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.
Outbound Statistics, nucastpkts	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.
Outbound Statistics, discards	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. Outbound discard statistics are incremented if a VC is not active when a packet is ready to send. This is a rare condition.
Outbound Statistics, errors	This field displays how many outbound packets contained errors that prevented their transmission.
Queue Overflow	This is a count of packets that were discarded because the queue for the VC was already full. If Queue Overflows are being seen across most or all SMs, then there is either an interferer local to the AP or the APs RF link is at capacity. If Queue Overflows are being seen at one or only a few SMs, then it is likely that there is a problem with those specific links whether it is insufficient signal strength, interferer, or a problem with the actual SM hardware.
High Priority Queue	Not applicable for PMP 450 products.

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 36 Overload tab of the AP

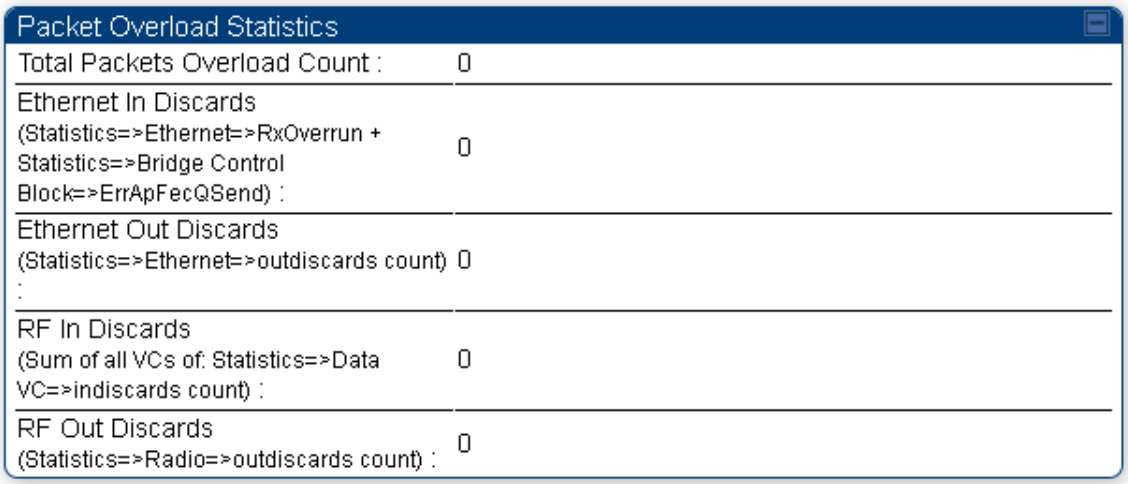


Table 43 Overload tab attributes

Attribute	Meaning
Total Packets Overload Count	This field represents the sum of all RF and Ethernet in/out discards.
Ethernet In Discards	This field represents the number of packets tossed due to the Ethernet queue being full. If a climb in this stat accompanies a climb in RF Out Discards stat, then most likely the board is at RF capacity either due to traffic exceeding the RF pipe, or interference temporarily limiting the RF throughput. If this stat climbs without the RF Out Discards stat climbing, then the radio is most likely PPS limited.
Ethernet Out Discards	This field represents the number of packets tossed due to an Ethernet out overload. This stat must not climb in normal operation because the Ethernet link is much higher capacity than the RF link. If this stat is incrementing, then either the Ethernet link is established at a low speed (i.e. 10Mbps – half duplex), or there is a problem with cabling/Ethernet hardware.
RF In Discards	This field indicates the number of packets tossed due to no resources available within the radio to process them. This stat also must not be increasing because the system is designed to shed packets on the RF Out interface. If this stat is incrementing the board, it is most likely congested due to high PPS rate in combination with an Ethernet Out problem, which limits packet flow off the device.
RF Out Discards	This field indicates the number of packets tossed due to RF link at capacity. This stat will increase whenever the RF link is at capacity. When the internal FPGA RF input queue overflows, this stat is incremented. If this stat is seen to be incrementing at the AP, then the sector is congested. If seen at the SM, the number of Contention Slots must be looked at to ensure that enough Contention Slots are allocated to allow for bandwidth requests to be seen at the AP.

Viewing the DHCP Relay tab (AP)

The DHCP Relay statistics tab displays requests and replies received, relayed and discarded when the AP is configured as a DHCP relay. Typically, in a working DHCP relay configuration a one-to-one ratio is established between requests and replies that are received and relayed.

Figure 37 DHCP Relay tab of the AP

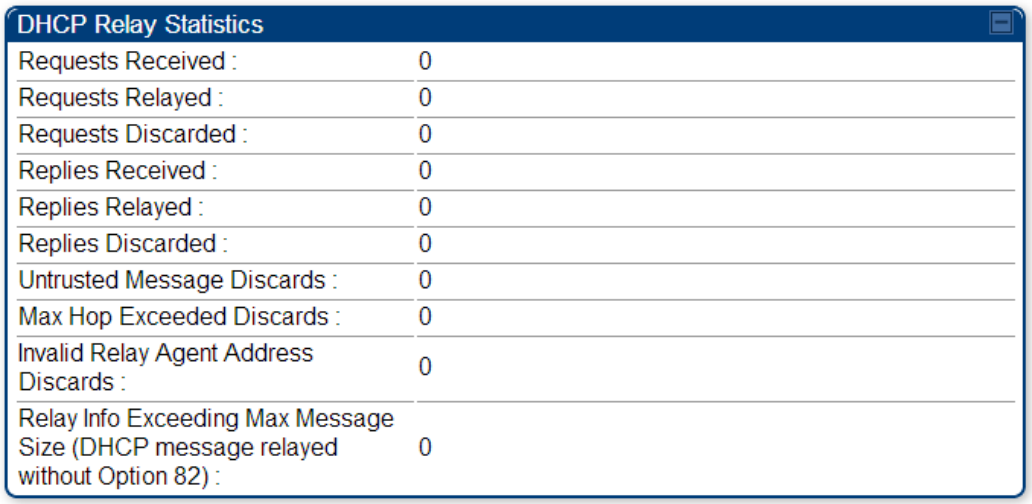


Table 44 DHCP Relay attributes

Attribute	Meaning
Requests Received	This field represents the number of DHCP relay requests received by the AP.
Requests Relayed	This field represents the number of DHCP relay requests relayed by the AP.
Requests Discarded	This field represents the number of DHCP relay requests discarded by the AP due to errors in the request.
Replies Received	This field represents the number of DHCP relay replies received by the AP.
Replies Relayed	This field represents the number of DHCP relay replies relayed by the AP.
Replies Discarded	This field represents the number of DHCP relay replies discarded by the AP due to errors in the reply.
Untrusted Message Discards	This field indicates messages that were discarded because the message already contained Option 82 information with no Relay Agent specified.
Max Hop Exceeded Discards	This field indicates messages that have been relayed too many times, exceeding the max hop count (16).
Invalid Relay Agent Address Discards	This field indicates messages that have been discarded because the message relay agent address is already in place (relay agent address does not equal address of the AP).
Relay Info Exceeding Max Message Size (DHCP message relayed without Option 82)	This field indicates DHCP messages too large to fit Option 82 data. These messages are sent on without Option 82 information.

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 38 Filter tab of the SM

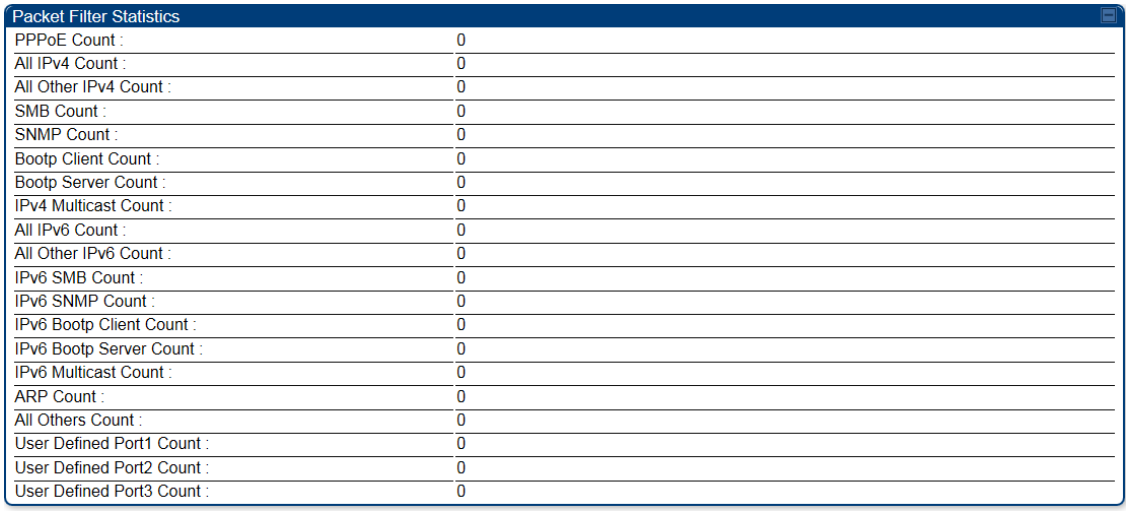


Table 45 Filter tab attributes

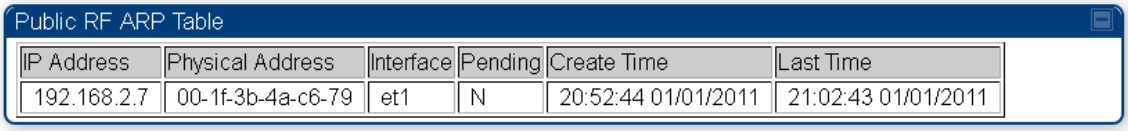
Attribute	Meaning
PPPoE Count	Number of PPoE packets filtered.
All IPv4 Count	Number of IPv4 packets filtered.
All Other IPv4 Count	Any IPv4 message that was not SMB, SNMP, Bootp, Multicast or one of the user defined filters, that was filtered out.
SMB Count	Number of IPv4 Server Message Block (file sharing) packets filtered.
SNMP Count	Number of IPv4 SNMP packets filtered.
Bootp Client Count	Total number of IPv4 DHCP requests filtered.
Bootp Server Count	Total number of IPv4 DHCP replies filtered.
IPv4 Multicast Count	Number of IPv4 Multicast messages filtered.
All IPv6 Count	Number of IPv6 messages filtered.
All Other IPv6 Count	Any IPv6 message that was not SMB, SNMP, Bootp, Multicast or one of the user defined filters, that was filtered out.
IPv6 SMB Count	Number of IPv6 Server Message Block (file sharing) packets filtered
IPv6 SNMP Count	Number of IPv6 SNMP messages filtred
IPv6 Bootp Client Count	Total number of IPv6 DHCP replies filtered
IPv6 Bootp Server Count	Total number of IPv6 DHCP replies filtered
IPv6 Multicast Count	Number of IPv6 Multicast messages filtered

Attribute	Meaning
ARP Count	Total number of ARP packets filtered.
All other Count	The count of any messages that did not fit above that were filtered out
User Defined Port1 Count	Number of packets defined by the user port1 that were filtered.
User Defined Port2 Count	Number of packets defined by the user port2 that were filtered.
User Defined Port3 Count	Number of packets defined by the user port3 that were filtered.

Viewing ARP Statistics (SM)

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

Figure 39 ARP tab of the SM



Viewing NAT Statistics (SM)

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

Figure 40 NAT Stats tab of the SM

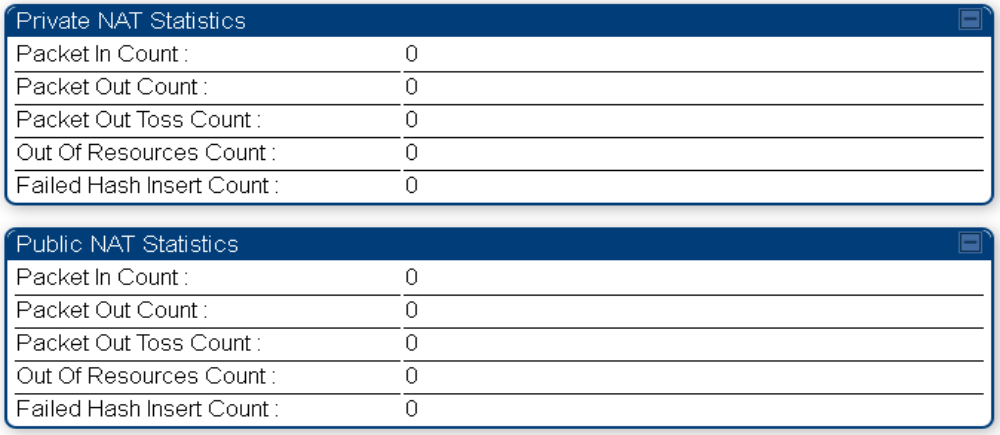


Table 46 NAT Stats attributes

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

Attribute	Meaning
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.
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 a 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 41 NAT DHCP Statistics of the SM

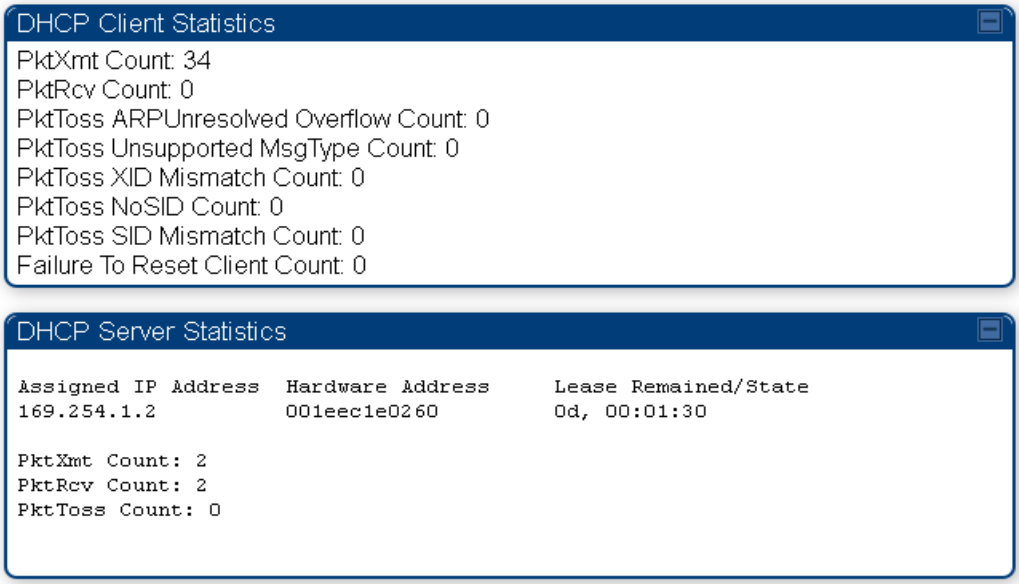


Table 47 NAT DHCP Statistics tab of the SM

Attribute	Meaning
PktXmt Count	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
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 SID Mismatch Count	Represents the number of packets 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 Sync Status Page (AP)

The **Sync Status** tab is only displayed when the Sync Input is set to AutoSync or AutoSync+Free Run.

Figure 42 AP Sync Status tab

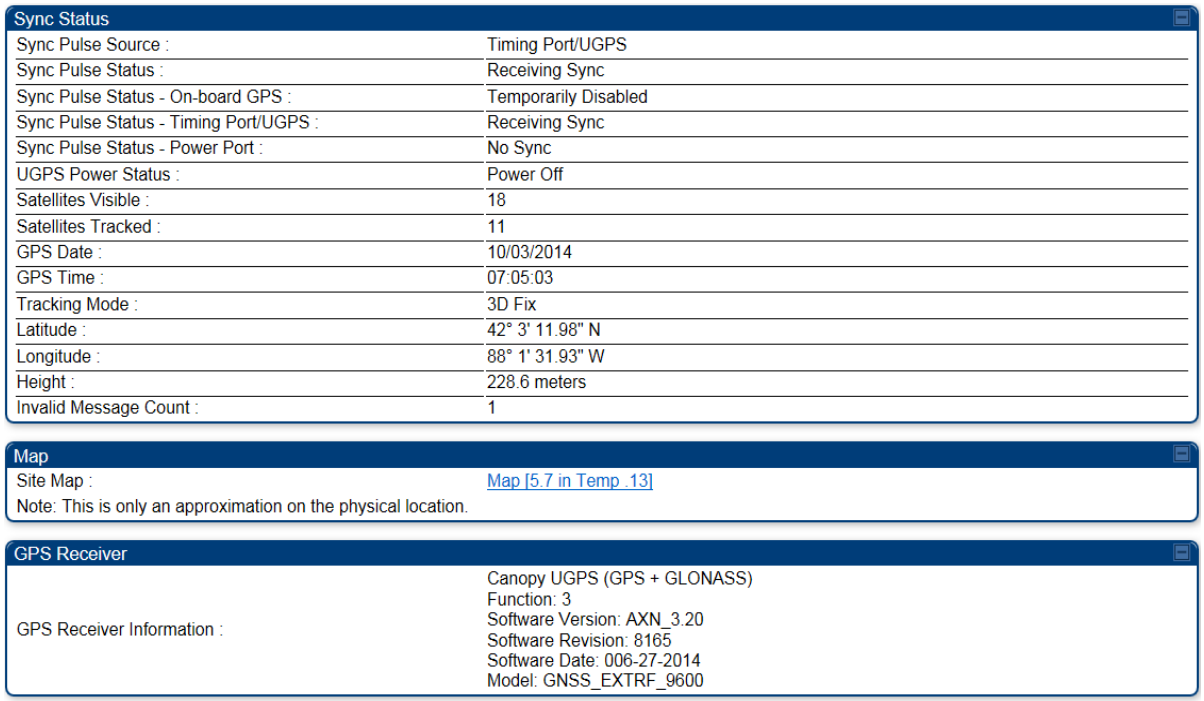


Table 48 AP Sync Status tab attributes

Attribute	Meaning
Sync Pulse Source	This field indicates the status of the synchronization source: • **Searching** indicates that the unit is searching for a GPS fix • **Timing Port/UGPS** indicates that the module is receiving sync via the timing RJ11 timing port • **Power Port** indicates that the module is receiving sync via the power port (Ethernet port). • **On-board GPS** indicates that the module is receiving sync via the unit's internal GPS module. The on-board GPS must not be used as the primary synchronization source.
Satellites Visible	This field indicates the number of satellites available for tracking.
Satellites Tracked	This field indicates the number of satellites tracked by the GPS module.
GPS Date	This field indicates the GPS date information provided by the GPS module.
GPS Time	This field indicates the GPS time information provided by the GPS module.
Tracking Mode	This field indicates the level of tracking fix use by the GPS module.
Latitude	This field indicates the GPS latitude data provided by the GPS module.
Longitude	This field indicates the GPS longitude data provided by the GPS module.
Height	This field indicates the GPS height data provided by the GPS module.
Invalid Message Count	This field indicates the number of messages received by the device from the GPS module which could not be decoded.
Site Map	The site map link, when clicked, redirects to a mapped representation of the modules location.
GPS Receiver Information	This section indicates general information about the GPS module used for synchronization.

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 is enabled on the SM, PPPoE statistics provide data about activities of the customer.

Figure 43 PPPoE tab of the SM

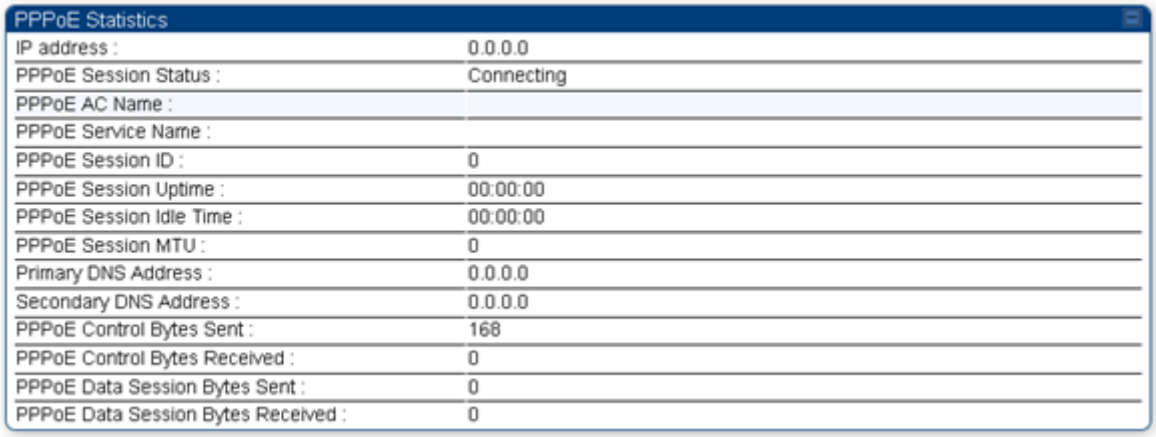


Table 49 PPPoE Statistics tab of the SM

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 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 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
PPPoE Control Bytes Sent	Displays the total number of PPPoE session control bytes sent from 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 44 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	
ErrNl1QSend :	0
ErrNl2QSend :	0
ErrBridgeFull :	0
ErrSendMsg :	0
ErrApFecQSend :	0
ErrApRfQSend :	0

Table 50 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
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.

Attribute	Meaning
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.
ErrBridgeFull	This field indicates the total number of times the bridging table was full and could not accept new entries.
ErrSendMsg	This field displays the error message from bridge core call back routine.
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 and 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 start the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. When choosing **Start Timed Spectrum Analysis**, the scan is run for the amount of time specified in the **Duration** configuration parameter. When choosing **Start Continuous Spectrum Analysis**, the scan is run continuously for 24 hours, or until stopped manually (using the **Stop Spectrum Analysis** button).

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

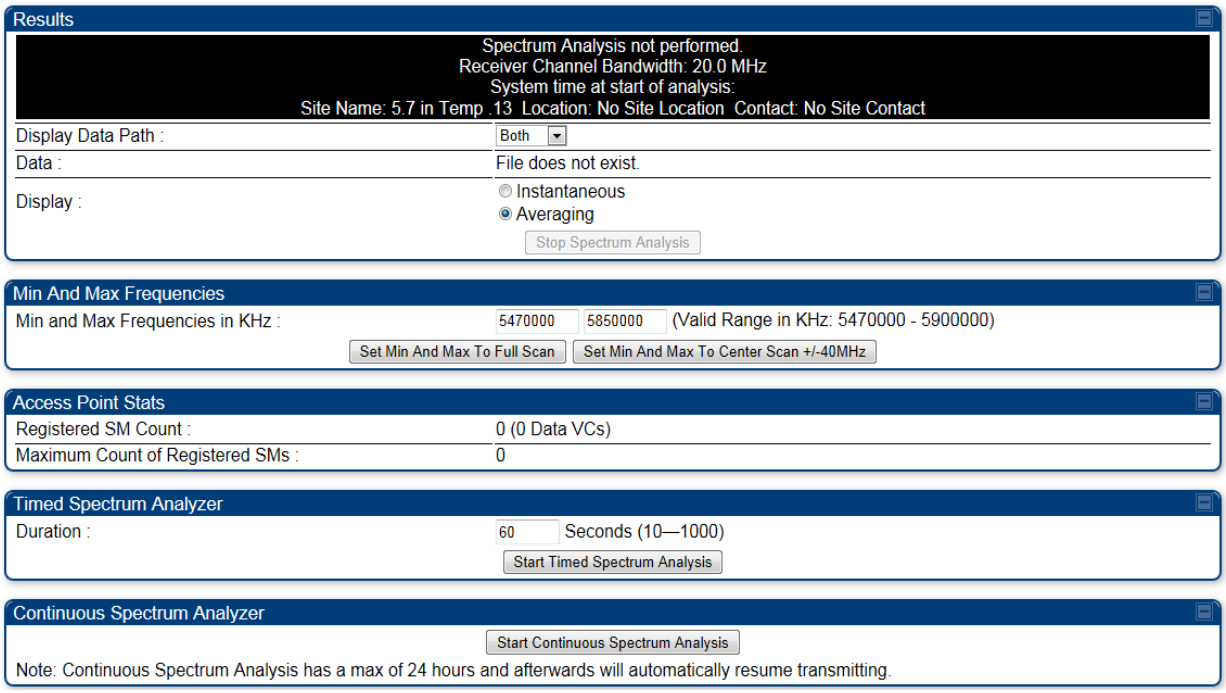
Vary the days and times when you analyze the spectrum in an area. The RF environment can change throughout the day or throughout the week.

Temporarily deploy a 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.

Graphical spectrum analyzer display

The SM and AP display the graphical spectrum analyzer. An example of the **Spectrum Analyzer** tab is shown in Figure 45.

Figure 45 Spectrum Analyzer display



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.

New navigation features include:

- Results may be panned left and right through the scanned spectrum by clicking and dragging the graph left and right
- Results may be zoomed in and out with the mouse wheel

  When the mouse is positioned over a bar, the receive power level, frequency, maximum and mean receive power levels are displayed above the graph

To keep the displayed data current, either set “Auto Refresh” on the module’s Configuration => General.

Table 51 Spectrum Analyzer attributes

Attribute	Meaning
Display Data Path	**Both** means that the vertical and horizontal paths are displayed or an individual path may be selected to display only a single-path reading.
Data	For ease of parsing data and to facilitate automation, the spectrum analyzer results may be saved as an XML file. To save the results in an XML formatted file, right-click the "SpectrumAnalysis.xml" link and save the file. If these results are viewed in a browser, they are displayed in the horizontal bar-graph fashion which was available prior to 12.1.
Display	**Instantaneous** means that each reading (vertical bar) is displayed with two horizontal lines above it representing the max power level received (top horizontal line) and the average power level received (lower horizontal line) at that frequency. **Averaging** means that each reading (vertical bar) is displayed with an associated horizontal line above it representing the max power level received at that frequency.
Registered SM Count	This field displays the MAC address and Site Name of the registered SM.
Maximum Count of Registered SMs	This field displays the maximum number of registered SMs.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Continuous Spectrum Analyzer	***Start Continuous Spectrum Analysis*** button ensures that when the SM is powered on, it automatically scans the spectrum for 10 seconds. These results may then be accessed via the **Tools => Spectrum Analyzer** GUI page.

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 the duration of 10 to 1000 seconds and select a SM from the drop-down list, then click the **Start Remote Spectrum Analysis** button to launch the analysis from that SM.

Figure 46 Remote Spectrum Analyzer tab of the AP

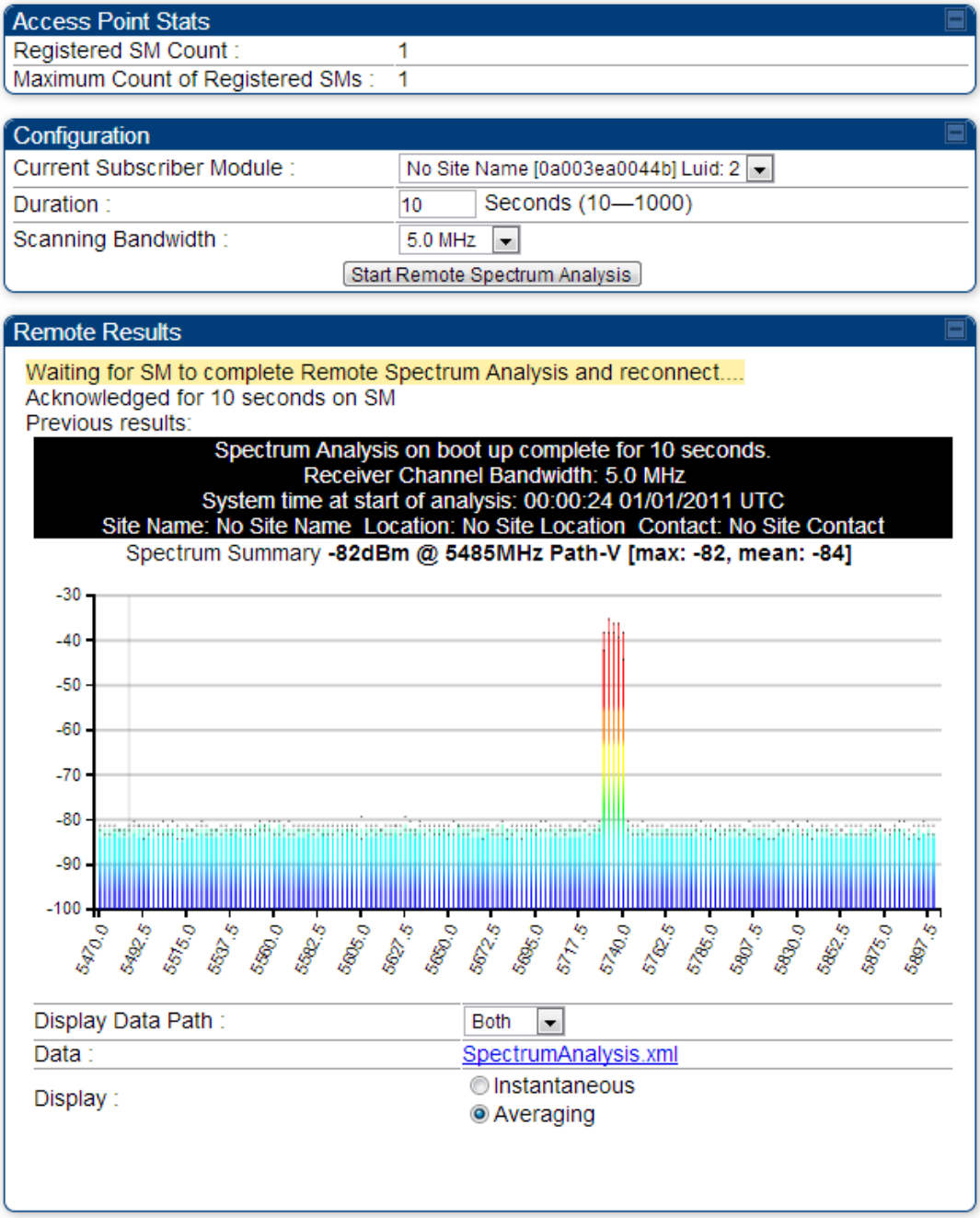


Table 52 Remote Spectrum Analyzer tab attributes

Attribute	Meaning
Registered SM Count	This field displays the number of SMs that were registered to the AP before the SA was started. This helps the user know all the SMs re-registered after performing a SA.
Maximum Count of Registered SMs	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.
Current Subscriber Module	The SM with which the Link Capacity Test is run.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Scanning Bandwidth	This parameter defines the size of the channel scanned when running the analyzer.

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, Signal Strength Ratio and Signal to Noise Ratio to ensure a stable link. The Tool provides color coded readings to facilitate in judging link quality.

NOTE

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

Figure 47 Alignment Tool tab of SM, good link example

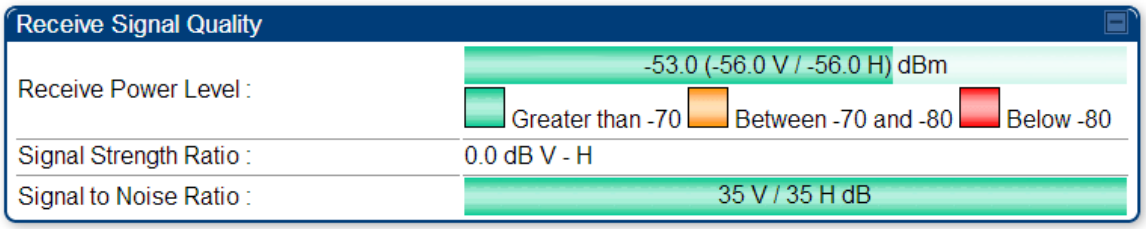


Figure 48 Alignment Tool tab of SM, acceptable link example

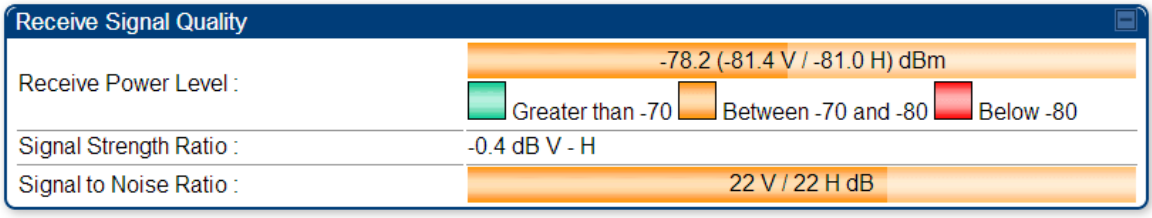
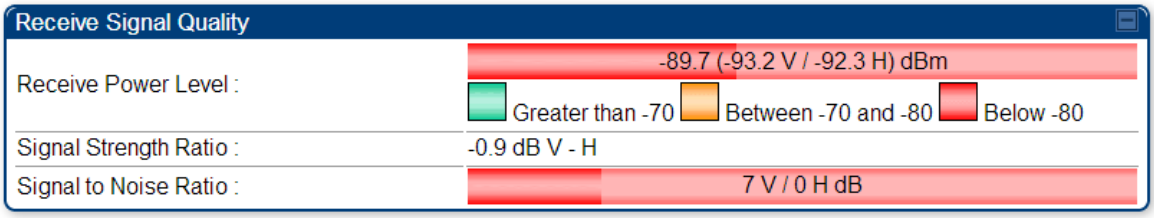


Figure 49 Alignment Tool tab of SM, poor RF environment



Using the Alignment tab (SM)

The SM's Aiming Tool (located in the SM GUI in **Tools**, **Alignment**) may be used to configure the SM's LED panel to indicate received signal strength and to display decoded beacon information/power levels. The SM LEDs provide different status based on the mode of the SM. A SM in "operating" mode will register and pass traffic normally. A SM in "aiming" mode will not register or pass traffic, but will display (via LED panel) the strength of received radio signals (based on radio channel selected via **Tools**, **Alignment**). To enter "aiming" mode, configure parameter **Scan Radio Frequency Only Mode** to "Enabled".

NOTE

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

Table 53 SM diagnostic LED descriptions

		Status information provided		
LED	**Color when active**	**SM in "Operating" Mode**	**SM in "Aiming" Mode**	**Notes**
LNK/5	green	Ethernet link	These five LEDs act as a bar graph to indicate the relative quality of alignment. As power level improves during alignment, more of these LEDs are lit.	Continuously lit when link is present.
ACT/4	yellow	Presence of data activity on the Ethernet link		Flashes during data transfer. Frequency of flash is not a diagnostic indication.
GPS/3	red	Interference		On - high interference. Blinking - medium interference. Off - low interference.
SES/2	green	Strong Receive Signal Power		Blinking from slow to full-on to indicate strong power, getting stronger.
SYN/1	yellow	Medium Receive Signal Power		Blinking from slow to full-on to indicate medium power, getting stronger.
PWR	red	Registration Indicator		Off when registered to AP. On when not registered to AP.

Figure 50 SM Alignment tab

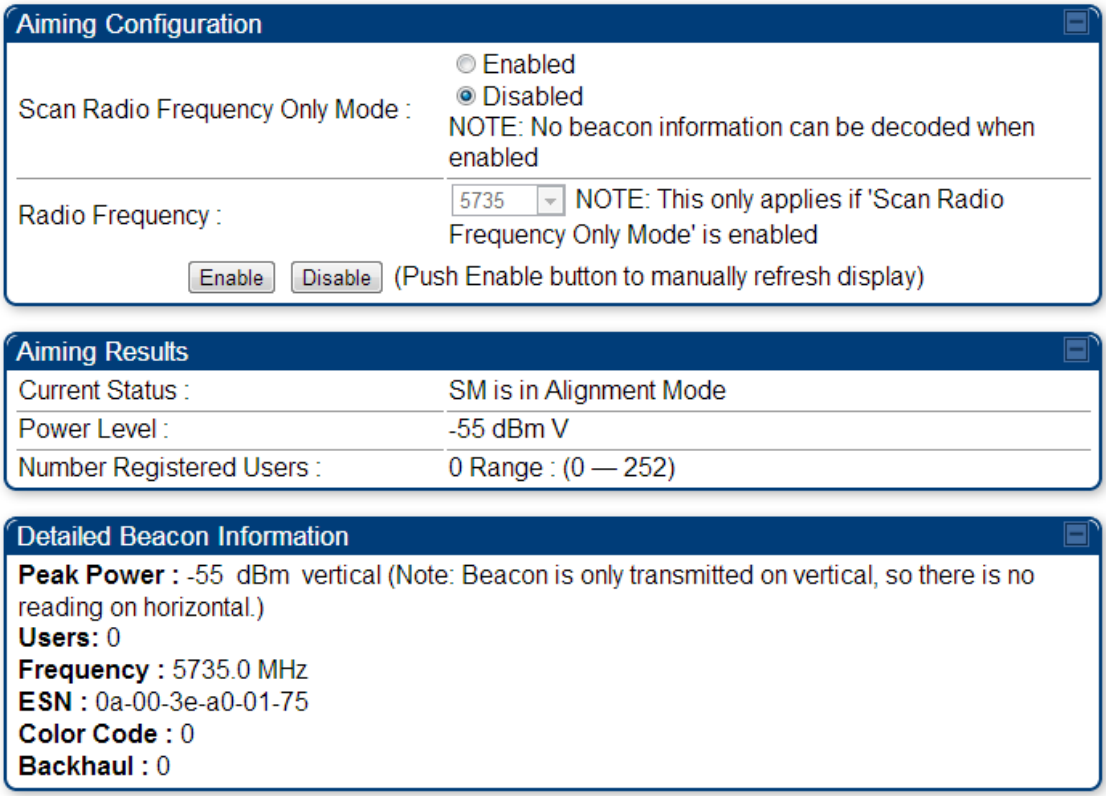


Table 54 Alignment tab attributes

Attribute	Meaning
Scan Radio Frequency Only Mode	**Enabled**: the radio is configured to "aiming" or "alignment" mode, wherein the SM's LED panel displays an indication of receive power level. See Table 30 on page 4-93. **Disabled:** the radio is configured to "operating" mode, wherein the SM registers and passes traffic normally.
Radio Frequency	This field indicates the center frequency for which results are displayed.
Current Status	This field indicates the current mode of the radio, "alignment" or "operating".
Power Level	This field indicates the current receive power level (vertical channel) for the frequency configured in parameter **Radio Frequency**.
Number Registered Users	When the radio is in "operating" mode, this field reports the number of registered SMs for the AP operating at the frequency defined in parameter **Radio Frequency**.
Peak Power	This field indicates the highest power level see by the SMs receiver.
Users	This field indicates the number of SMs currently registered to the AP which is transmitting the beacon information.

Attribute	Meaning
Frequency	This field indicates the frequency of the AP which is transmitting the beacon information.
ESN	This field indicates the MAC, or hardware address of the AP which is transmitting the beacon information.
Color Code	This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
Backhaul	**0** indicates that the beacon transmitter is an AP.

Using the Link Capacity Test tool (AP or SM)

The **Link Capacity Test** tab 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 51 Link Capacity Test tab of the AP

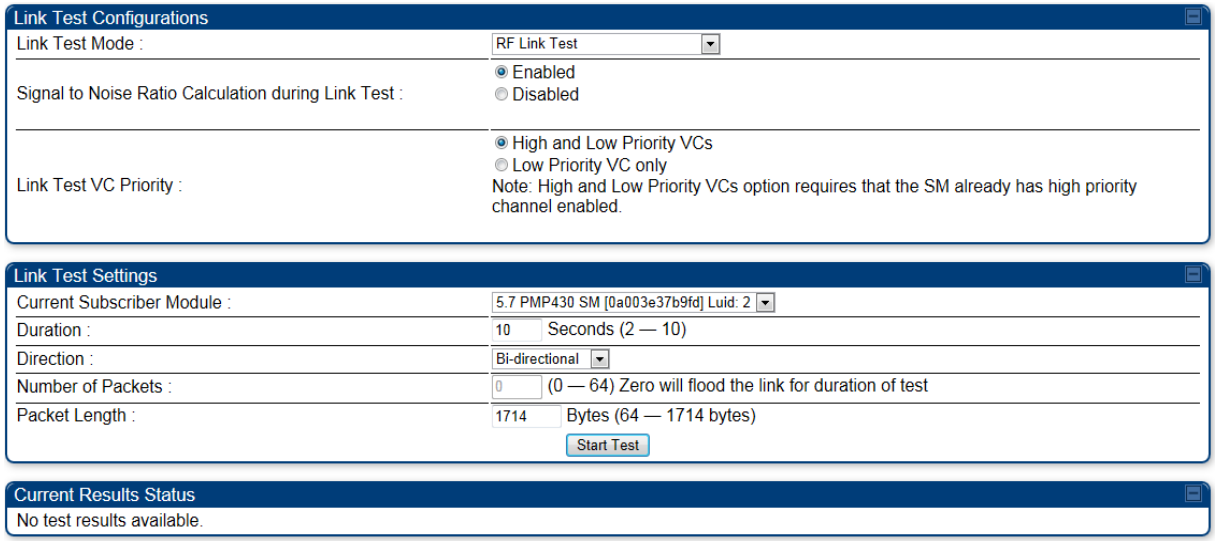
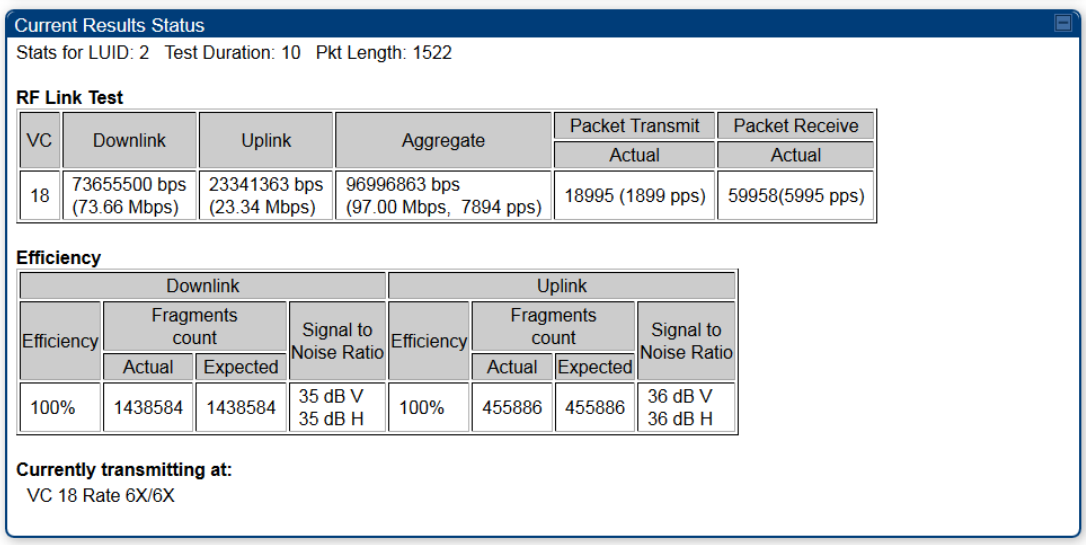


Table 55 Link Capacity Test tab attributes

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 the traffic during test and 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 is run.

Attribute	Meaning
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Direction	Configure the direction of the link test. Specify **Downlink** or **Uplink** to run the test only in the corresponding direction only. Specific **Bi-Directional** to run the test in both directions.
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 52 Link Capacity Test tab with 1522-byte packet length



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

Procedure 3 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 must 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 on **Tools** web page of the SM provides information about the AP that the SM sees.

NOTE

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

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 53 AP Evaluation tab of SM

The **AP Evaluation** tab has the following fields that can be used to manage and troubleshoot a system:

Table 56 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.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM.
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 prefixes mean that for every 16 bits of throughput data transmitted, an additional bit is used.
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 Country Code setting.
Power Level	This field displays the SM's combined 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	This field indicates the configured value for the AP's Max Range parameter.
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 a 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 a 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.
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.

Attribute	Meaning
Color Code	This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
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 slots in the frame for this AP.
NumDLHalfSlots	This is the number of downlink slots in the frame for this.
NumULContSlots	This field displays how many Contention Slots are being used in the uplink portion of the frame.
WhiteSched	Flag to display if schedule whitening is supported via FPGA
ICC	This field lists the SMs that have registered to the AP with their Installation Color Code (ICC), Primary CC, Secondary CC or Tertiary CC.
SM PPPoE	This filed provides information to the user whether the SM is supporting PPPoE or not.

Using the OFDM Frame Calculator tool

The first step to avoid interference in wireless systems is to set all APs to receive timing from a synchronization source (Cluster Management Module, or Universal Global Positioning System). 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) Contention 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 must use the Frame Calculator to identify compatible settings.

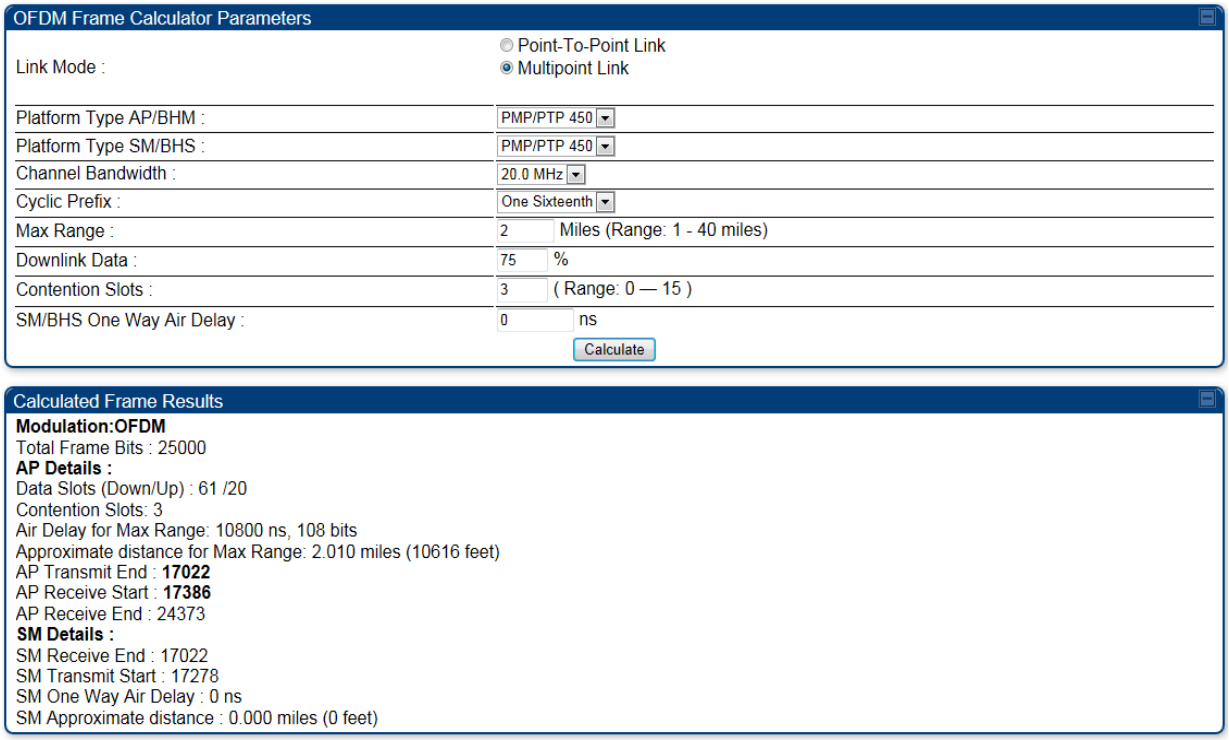
The frame calculator is available on the Frame Calculator tab of the Tools web page. To use the Frame Calculator, type various configurable parameter values into the calculator for each proximal AP and then record the resulting **AP Receive Start** value. Next vary the **Downlink Data** percentage in 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. In Cambium Point-to-Multipoint systems, 10 bit times = 1 μs.

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 co-location may work fine at low traffic levels, but encounter problems at higher traffic levels. The conservative practice is to tune for co-location before traffic ultimately increases. This prevents problems that occur as sectors are built.

Figure 54 OFDM Frame Calculator tab



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

Table 57 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).
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 4, 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.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. Set this parameter to the value of the **Contention Slot** parameter is set in the APs.
SM/BHS One Way Air Delay	This field displays the time in *ns* (nano seconds), that a BHS/SM is away from the BHM/AP.

The Calculated Frame Results display several items of interest:

Table 58 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)	This field is based on the **Downlink Data** setting. For example, a result within the typical range for a **Downlink Data** setting of 75% is 61/21, meaning 61 data slots down and 21 data slots up.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator.
Air Delay for Max Range	This is the roundtrip air delay in bit times for the **Max Range** value set in the calculator
Approximate distance for Max Range	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 starts the transmission.
SM One Way Air Delay	This filed displays the time in *ns*, that BHS/SM is away from the BHM/AP.
SM Approximate distance	This field displays an approximate distance in miles (feet) that the BHS/SM is away from the BHM/AP.

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 4 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.

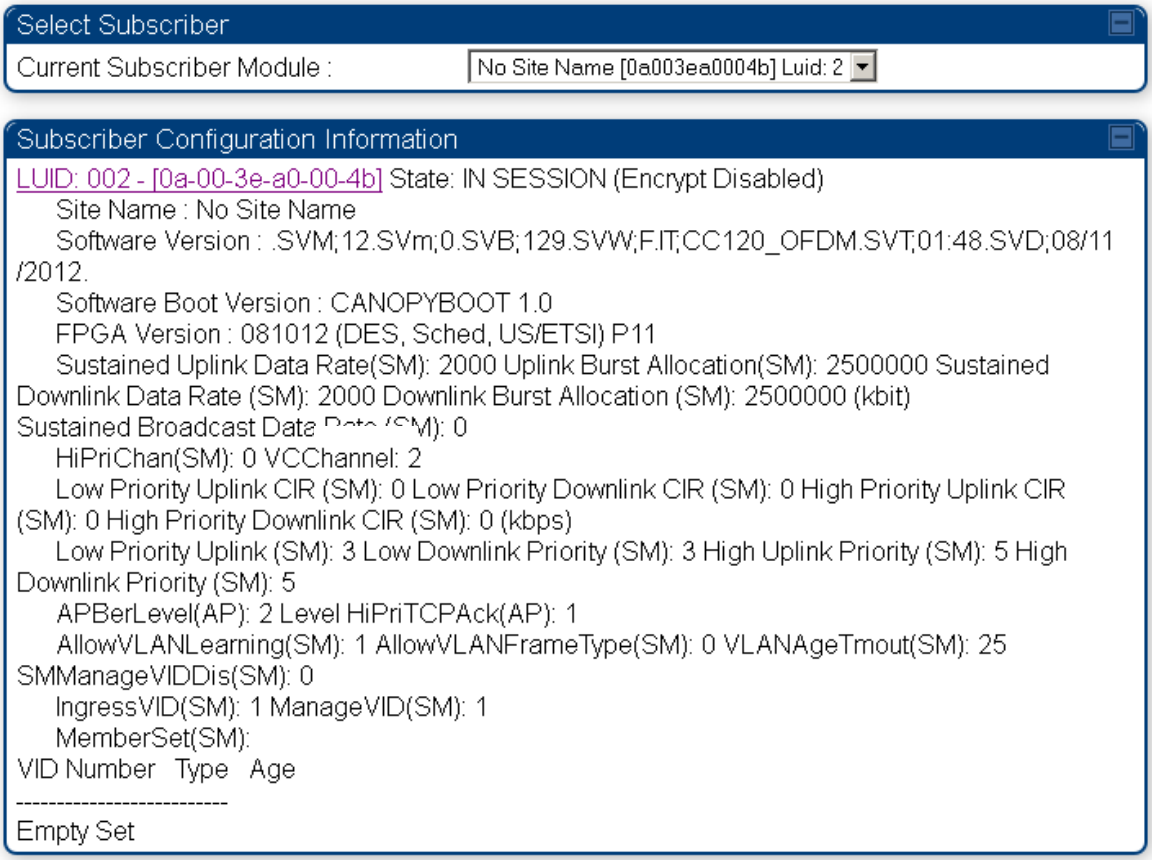
Using the SM Configuration tool (AP)

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 55 SM Configuration tab of AP



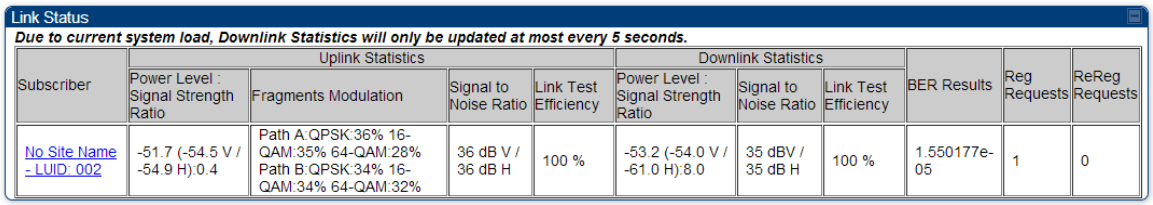
The AP displays one of the following for the configuration source:

- (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 or SM)

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 56 Link Status tab of AP



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

Table 59 OFDM Calculated Frame Results attributes

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name 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 a 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. Site Name 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.
Uplink Statistics - Power Level: Signal Strength Ratio	This field represents the combined received power level at the AP as well as the ratio of horizontal path signal strength to vertical path signal strength.
Uplink Statistics – Fragments Modulation	This field represents the percentage of fragments received at each modulation state, per path (polarization).
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) expressed for both the horizontal and vertical channels.
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: Signal Strength Ratio	This field represents the received power level at the SM as well as the ratio of horizontal path signal strength to vertical path signal strength 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) expressed for both the horizontal and vertical channels.
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 (1×10^{-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 a 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 includes the received power level, signal to noise ratio and link tests.

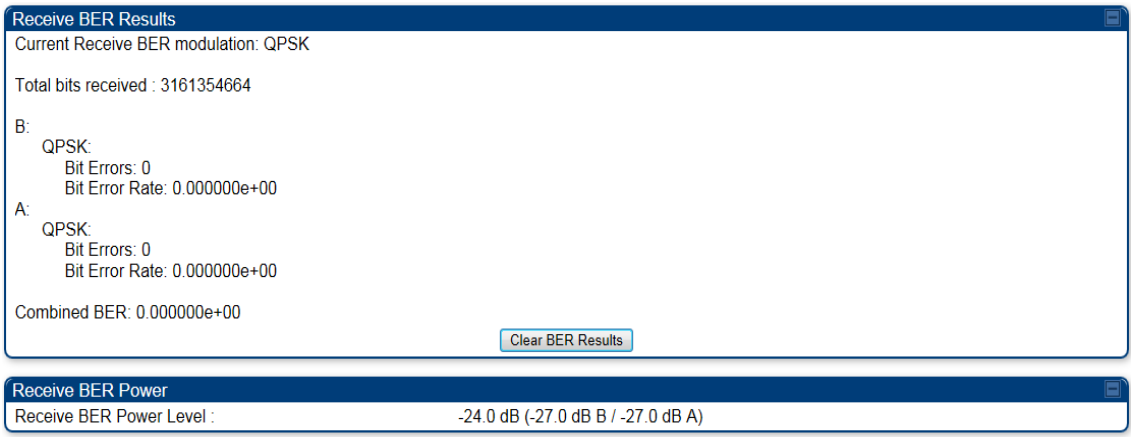
BER is only instrumented on the downlink and is displayed on the BER Results tab of the Tools page in any SM. Each time the tab is clicked, the current results are read and counters are reset to zero.

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.

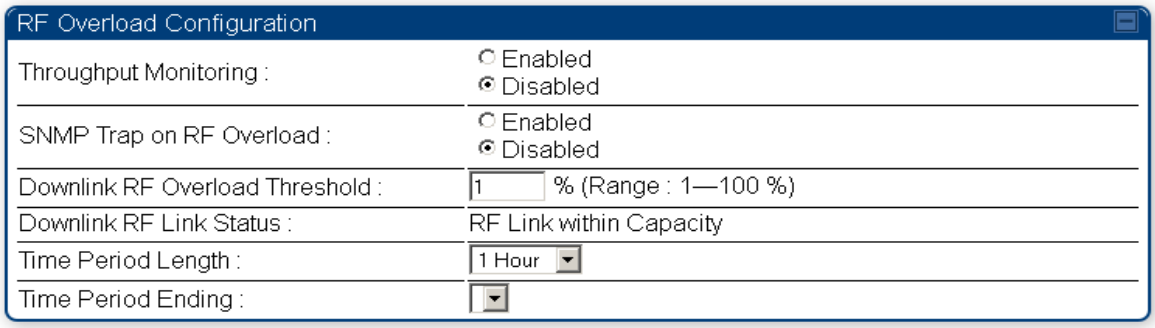
Figure 57 BER Results tab of the SM



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 58 Throughput tab of the AP



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

Table 60 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

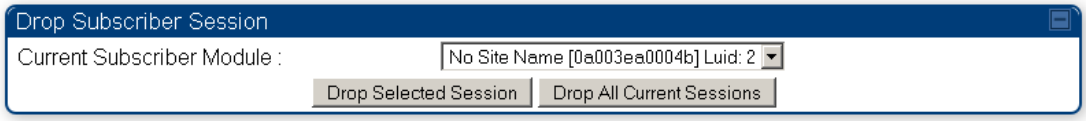
This table contains a row that corresponds to each active LUID served by the AP. Note that an LUID may be assigned 1 or 2 VCs. If the LUID is assigned 2 VCs, then the data in the table is the sum of the activity for both VCs. This table may be used to determine which LUIDs are experiencing overload so 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 a SM re-registration. This operation is useful to force QoS changes for SMs without losing AP logs or statistics. This operation may take 5 minutes to regain all SM registrations.

Figure 59 Sessions tab of the AP



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

Typical Contents of Release Notes

Cambium supports each release with software release notes, which include the following:

- Description of features that are introduced in the new release.
- Issues fixed on the new release.
- 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 5 Typical upgrade process

1. Visit https://support.cambiumnetworks.com/files/pmp450.
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). To replace them individually, use one of the following two procedures.

Procedure 6 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 7 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 8 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.

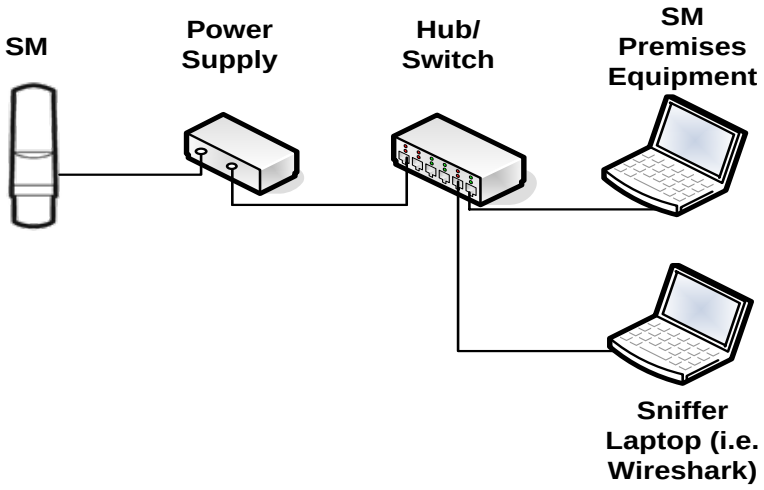
- 1 laptop computer with protocol analyzer software installed
- 2 straight-through Ethernet cables
- 1 power converter

Analyzing Traffic at a 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 a SM is shown below:

Figure 60 Protocol Analysis at the SM

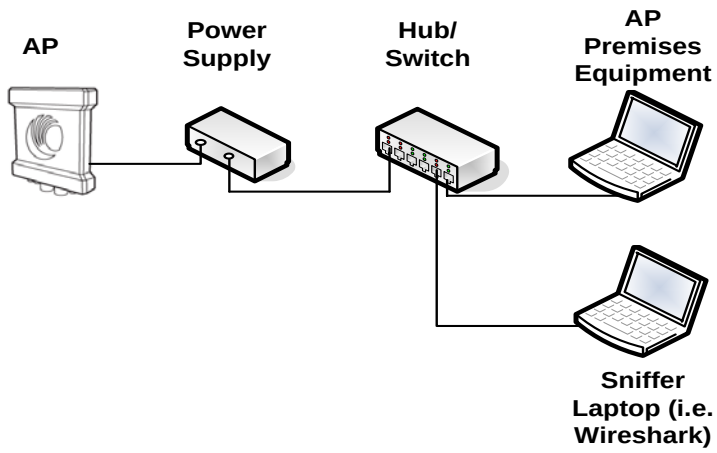


Analyzing traffic at an AP with no CMM

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 61 Protocol analyzer at AP not connected to a CMM

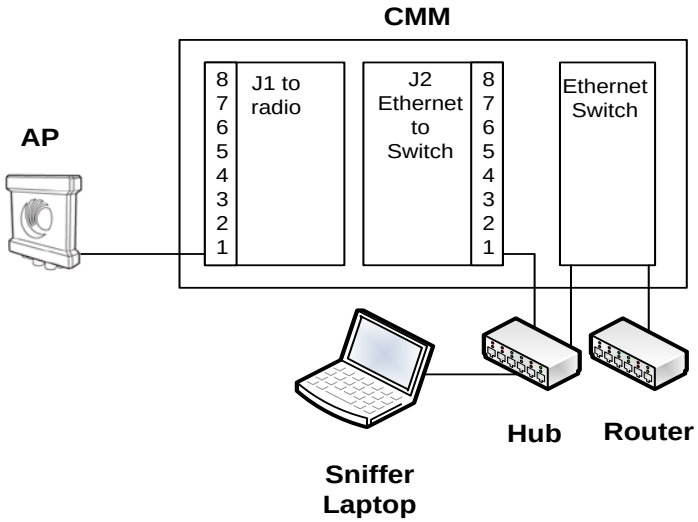


Analyzing Traffic at an AP with a CMM

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 62 Protocol analysis at AP connected to a CMM



Example of a protocol analyzer setup for a SM

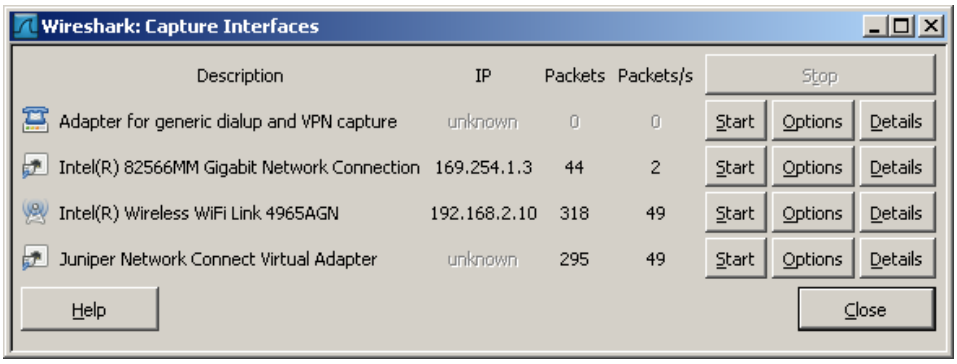
The following is an example of a network protocol analyzer setup using Wireshark software to capture traffic at the SM level. This example is based on the following assumptions:

- 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.

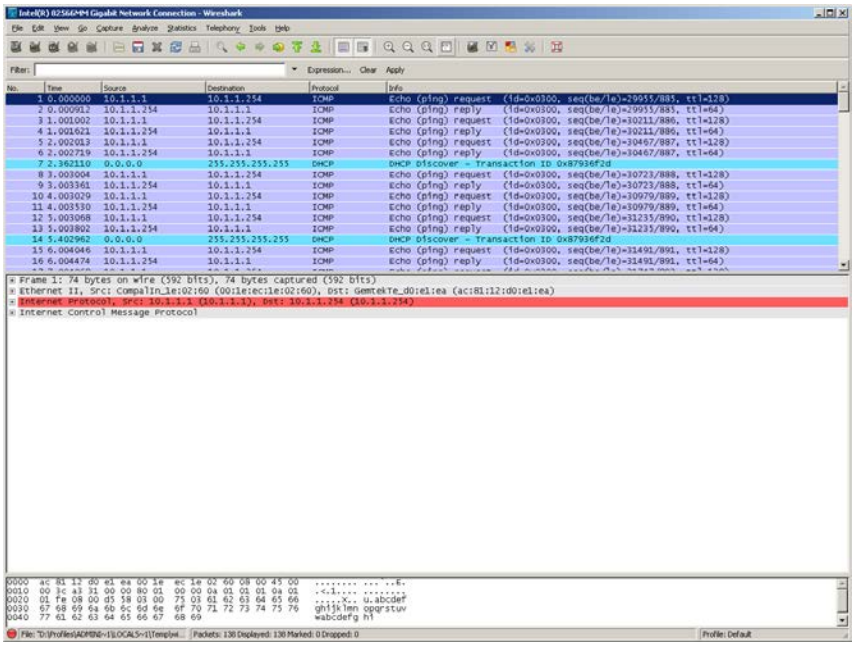
Although these procedures involve the SM, the only difference in the procedure for analyzing traffic on an AP is the hub insertion point.

Procedure 9 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



5. The captured packets are displayed in the main window:



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 the following:

- 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
  - Backhaul
  - Backhaul to CMM
  - Power
- Researching Event Logs of the involved equipment
- Interpreting messages in the Event Log
- Answering the questions listed in the following sections.
- 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, 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 is completed through the above steps, follow these:

- Check the Canopy knowledge base (https://support.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 7-167
  - NAT/DHCP-configured SM has lost or does not establish connectivity on page 7-169
  - SM Does Not Register to an AP on page 7-170
  - Module has lost or does not gain sync on page 7-171
  - Module does not establish Ethernet connectivity on page 7-172
  - Module on page 7-173
  - Power supply does not produce power on page 7-173
  - CMM does not pass proper GPS sync to connected modules on page 7-174

Procedures for Troubleshooting

Module has lost or does not establish connectivity

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

Procedure 10 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 a SM configured for NAT/DHCP, perform the following steps.

Procedure 11 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 a SM failing to register to an AP, perform the following steps.

Procedure 12 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 must 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 Pre-shared 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 13 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 must not take longer than 5 minutes from unit startup.
6. If these indicators are present in the second AP, then:
   - 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 14 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 must light up 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 15 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 then check:
   - if the known good module fails to power up, request a 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 16 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 17 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 must not take 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 18 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 19 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.

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.
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.

Term	Definition
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 a 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.
CIR	Committed Information Rate. For a SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum (unless oversubscribed). In the Cambium implementation, this is controlled by the Low Priority Uplink CIR, Low Priority Downlink CIR, High Priority Uplink CIR and High Priority Downlink CIR parameters.
CLIP	Cassegrain Lens for Improved Performance
Cluster Management Module	Module that provides power, GPS timing and networking connections for an AP cluster. Also known as CMM.

Term	Definition
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 valid values is 0 to 255.
Community String Field	Control string that allows a network management station to access MIB information about the module.
Country Code	A parameter that offers multiple fixed selections, each of which automatically implements frequency band range restrictions for the selected country. Units shipped to countries other than the United States must be configured with the corresponding Region Code and Country Code to comply with local regulatory requirements.
CRCError Field	This field displays how many CRC errors occurred on the Ethernet controller.
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.
DFS	See Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses and allows modules to be moved to a different network within the system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.
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.

Term	Definition
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 Frequency Selection	A requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems and to avoid co-channel operation with these systems.
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.
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 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.

Term	Definition
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.
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.

Term	Definition
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.
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.
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 a 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.

Term	Definition
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.
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.

Term	Definition
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.
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.
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.
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, this LED is unused. In the operating mode for a Subscriber Module, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module, this LED is part of a bar graph that indicates the quality of the RF link.
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. 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.
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.

Term	Definition
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.
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.

Term	Definition
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.