Cambium PMP 450 Installation Guide

System Release 12.0

Cambium Networks

Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

Safety and regulatory information

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

Important safety information

⚠ WARNING

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

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

Grounding and protective earth

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

Powering down before servicing

Always power down and unplug the equipment before servicing.

Primary disconnect device

The AP or SM unit's power supply is the primary disconnect device.

External cables

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

RF exposure near the antenna

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

Minimum separation distances

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

The minimum separation distances for each frequency variant are specified in **Calculated distances and power compliance margins** on page 2-37.

Important regulatory information

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

Radar avoidance

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

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

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

Contact the Cambium helpdesk if more guidance is required.

USA and Canada specific information

The USA Federal Communications Commission (FCC) has asked manufacturers to implement special features to prevent interference to radar systems that operate in the 5250-5350 and 5470-5725 MHz bands. These features must be implemented in all products able to operate outdoors in the UNII band. The use of the 5600 – 5650 MHz band is prohibited, even with detect-and-avoid functionality implemented.

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

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

Contents

List of Figures

List of Tables

About This Installation Guide

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

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

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

The guide consists of the following chapters:

- Installation planning
- Reference information
- Preparing for installation
- Installing Components

General information

Version information

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

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

Contacting Cambium Networks

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

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

Sales enquiries: solutions@cambiumnetworks.com

Email support: support@cambiumnetworks.com

Telephone numbers:

North America: +1 866-961-9288

Latin/Central America: +420 533 336 946

Europe, Middle East or Africa: +44 203 0277499

Asia/Pacific: +420 533 336 946

For full list of Cambium support telephone numbers, see:

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

Address:

Cambium Networks Limited,
1299 E Algonquin Road

Schaumburg, IL 60196

Purpose

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

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

Cross references

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

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

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to email support (see 'Contacting Cambium Networks').

Problems and warranty

Reporting problems

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

1. Search this document and the software release notes of supported releases.
2. Visit the support website.
3. Ask for assistance from the Cambium product supplier.
4. Gather information from affected units such as:
   - The IP addresses and MAC addresses.
   - The software releases.
   - The configuration of software features.
   - Any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

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

Repair and service

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

Warranty

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

To register PMP products or activate warranties, visit the support website.

For warranty assistance, contact the reseller or distributor.

⚠ CAUTION

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

⚠ CAUTION

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

Security advice

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

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

Warnings, cautions, and notes

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

Warnings

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

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

Cautions

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

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

Notes

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

> **NOTE**
>
> Note text.

Caring for the environment

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

In EU countries

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

Disposal of Cambium equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

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

Disposal of surplus packaging

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

In non-EU countries

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

Chapter 1: Installation planning

This chapter provides information to help the user to plan a PMP 450 network.

The following topics are described in this chapter:

- Regulatory planning on page 1-10 describes how to plan PMP 450 links to conform to the regulatory restrictions that apply in the country of operation.
- Site planning on page 1-11 describes factors to be considered when choosing sites for the AP, SM and accessories.
- Grounding and lightning protection on page 1-14 describes how to plan for proper grounding and lightning protection including cabling requirements and installation suggestions
- Ordering components on page 1-23 details part numbers and descriptions of PMP 450 equipment

Regulatory planning

This section describes how to plan PMP 450 links to conform to the regulatory restrictions that apply in the country of operation.

CAUTION

It is the responsibility of the user to ensure that the PMP product is operated in accordance with local regulatory limits.

NOTE

Contact the applicable radio regulator to find out whether or not registration of the PMP network is required.

Obeying Regulatory limits

The local regulator may restrict frequency usage and channel width, and may limit the amount of conducted or radiated transmitter power.

Many countries impose EIRP limits (Allowed EIRP) on products operating in the bands used by the PMP 450 Series. For example, in the 5.8 GHz band, these limits are calculated as follows:

- In the 5.8 GHz band (5725 MHz to 5875 MHz), the EIRP must not exceed the lesser of 36 dBm or (23 + 10 x Log Channel width in MHz) dBm.

Some countries (for example the USA) impose conducted power limits on products operating in the 5.8 GHz band.

Conforming to the limits

Ensure the system is configured to conform to local regulatory requirements by setting the appropriate Region Code setting on the APs and SMs in the network. When using connectorized APs with external antennas, the regulations may require the maximum transmit power to be reduced. To ensure that regulatory requirements are met for connectorized installations, refer to Compliance with radio regulations on page 2-41.

PMP 450 devices do not operate in the 2.4 GHz or UNII (5150-5250, 5250-5350, 5470-5725 MHz) bands.

Site planning

This section describes factors to be taken into account when choosing sites for the AP or SM, power supplies, CMM4 (if applicable) and GPS antenna (if applicable).

AP or SM site selection

When selecting a site for the AP or SM, consider the following factors:

- Height and location to ensure that people are kept away from the antenna; see Minimum separation distances on page II.
- Height and location to achieve the best radio path.
- Ability to meet the requirements specified in Grounding and lightning protection on page 1-14.
- Aesthetics and planning permission issues.
- Cable lengths; see Maximum cable lengths on page 1-11.
- The effect of strong winds on the installation; see Wind loading on page 1-12.

Power supply site selection

When selecting a site for the AP or SM power supply, consider the following factors:

- Indoor location with no possibility of condensation.
- Availability of a mains electricity supply.
- Accessibility for viewing status indicator and connecting Ethernet cables.
- Cable lengths; see Maximum cable lengths on page 1-11.

Maximum cable lengths

When installing PMP 450 Series APs or SMs, the maximum permitted length of the copper Ethernet interface cable is 100 m (330 ft) from AP/SM to their associated power supplies or CMM4.

Wind loading

Ensure that the site will not be prone to excessive wind loading.

Antennas and equipment mounted on towers or buildings will subject the mounting structure to significant lateral forces when there is appreciable wind. Antennas are normally specified by the amount of force (in pounds) for specific wind strengths. The magnitude of the force depends on both the wind strength and size of the antenna.

Calculation of lateral force (metric)

The magnitude of the lateral force can be estimated from:

Force (in kilogrammes) = $0.1045aV^2$

Where:	Is:
a	surface area in square meters
V	wind speed in meters per second

The lateral force produced by a single PMP 450 at different wind speeds is shown in Table 1 Lateral force - metric and Table 2 Lateral force - US.

Table 1 Lateral force - metric

Largest surface area (square meters)	Lateral force (Kg) at wind speed (meters per second)				
	30	40	50	60	70
.066 (AP)	6	11	17	25	34
.0027 (SM)	0.25	0.45	0.7	1	1.4

Calculation of lateral force (US)

The magnitude of the lateral force can be estimated from:

Force (in pounds) = $0.0042Av^2$

Where:	Is:
A	surface area in square feet
v	wind speed in miles per hour

The lateral force produced by a single PMP 450 unit at different wind speeds is shown in Table 2.

Table 2 Lateral force - US

Largest surface area (square feet)	Lateral force (lb) at wind speed (miles per hour)				
	80	100	120	140	150
0.71 (AP)	19	30	43	58	67
0.29 (SM)	7.8	12	18	23	27

Capabilities of the PMP 450 Series

The structure and mounting brackets of the AP are capable of withstanding wind speeds up to 190 kph (118 mph). Ensure that the structure to which the AP is fixed to is also capable of withstanding the prevalent wind speeds and loads.

The structure and mounting brackets of the SM are capable of withstanding wind speeds up to 190 kph (118 mph). Ensure that the structure to which the SM is fixed to is also capable of withstanding the prevalent wind speeds and loads.

Wind speed statistics

Contact the national meteorological office for the country concerned to identify the likely wind speeds prevalent at the proposed location. Use this data to estimate the total wind loading on the support structures. Sources of information:

- US National Weather Service, http://www.nws.noaa.gov/
- UK Meteorological Office, www.meto.gov.uk

Grounding and lightning protection

This section describes the grounding and lightning protection requirements of a PMP 450 installation.

WARNING

Electro-magnetic discharge (lightning) damage is not covered under warranty. The recommendations in this guide, when followed correctly, give the user the best protection from the harmful effects of EMD. However 100% protection is neither implied nor possible.

The need for power surge protection

Structures, equipment and people must be protected against power surges (typically caused by lightning) by conducting the surge current to ground via a separate preferential solid path. The actual degree of protection required depends on local conditions and applicable local regulations. Cambium recommends that PMP 450 installation is contracted to a professional installer.

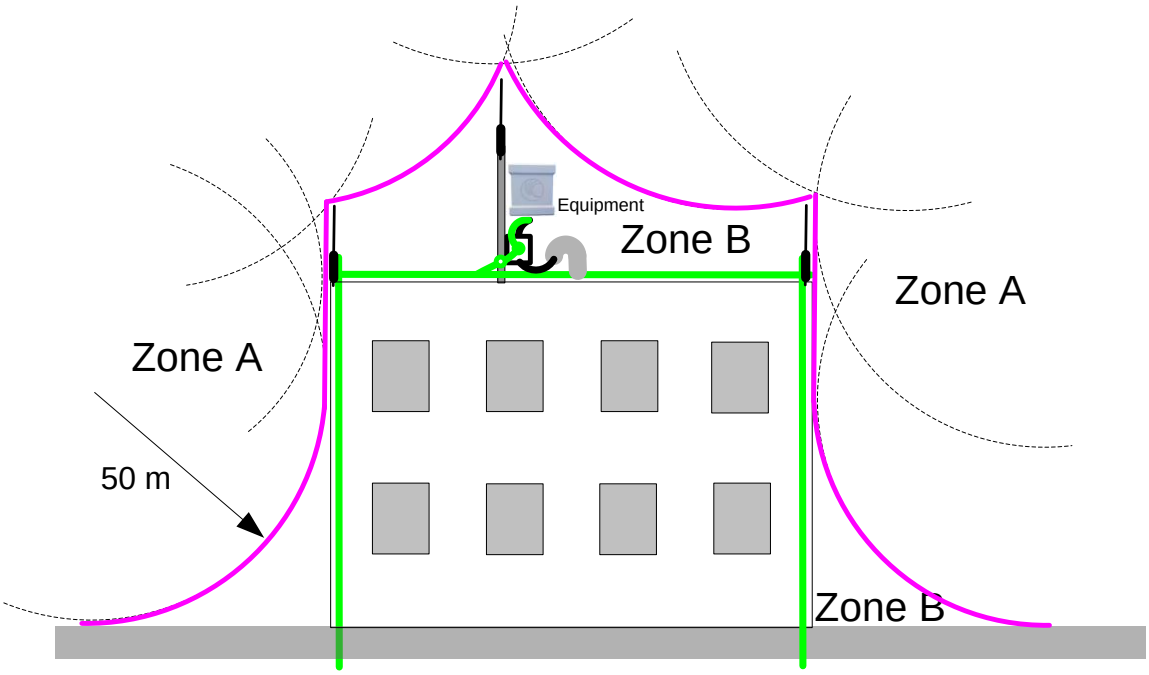
Standards

Full details of lightning protection methods and requirements can be found in the international standards IEC 61024-1 and IEC 61312-1, the U.S. National Electric Code ANSI/NFPA No. 70-1984 or section 54 of the Canadian Electric Code.

Lightning protection zones

The 'rolling sphere method' (Figure 1) is used to determine where it is safe to mount equipment. An imaginary sphere, typically 50 meters in radius, is rolled over the structure. Where the sphere rests against the ground and a strike termination device (such as a finial or ground bar), all the space under the sphere is considered to be in the zone of protection (Zone B). Similarly, where the sphere rests on two finials, the space under the sphere is considered to be in the zone of protection.

Figure 1 Rolling sphere method to determine the lightning protection zones



Assess locations on masts, towers and buildings to determine if the location is in Zone A or Zone B:

- Zone A: In this zone a direct lightning strike is possible. Do not mount equipment in this zone.
- Zone B: In this zone, direct EMD (lightning) effects are still possible, but mounting in this zone significantly reduces the possibility of a direct strike. Mount equipment in this zone.

⚠ WARNING

Never mount equipment in Zone A. Mounting in Zone A may put equipment, structures and life at risk.

General protection requirements

To adequately protect a PMP 450 installation, both ground bonding and transient voltage surge suppression are required.

Basic requirements

The following basic protection requirements must be implemented:

- The equipment (AP, SM or GPS receiver) must be in 'Zone B' (see Lightning protection zones on page 1-15).
- The AP must be grounded to the supporting structure.
- A surge suppression unit (600SSD) must be installed close to the SM.
- The distance between the SM and 600SSD should be kept to a minimum.
- The drop cable length between the SM and 600SSD must be less than 600 mm.
- An surge suppression unit (200SS) must be installed within 600 mm (24 in) of the point at which the drop cable enters the building or equipment room.
- The drop cable must be bonded to the supporting structure in order to prevent lightning creating a potential between the structure and cable, which could cause arcing, resulting in fire risk and damage to equipment.
- The drop cable must be grounded at the building entry point.
- The drop cable must not be laid alongside a lightning air terminal.
- All grounding cables must be a minimum size of 10 mm^2 csa (8AWG), preferably 16 mm^2 csa (6AWG), or 25 mm^2 csa (4AWG).

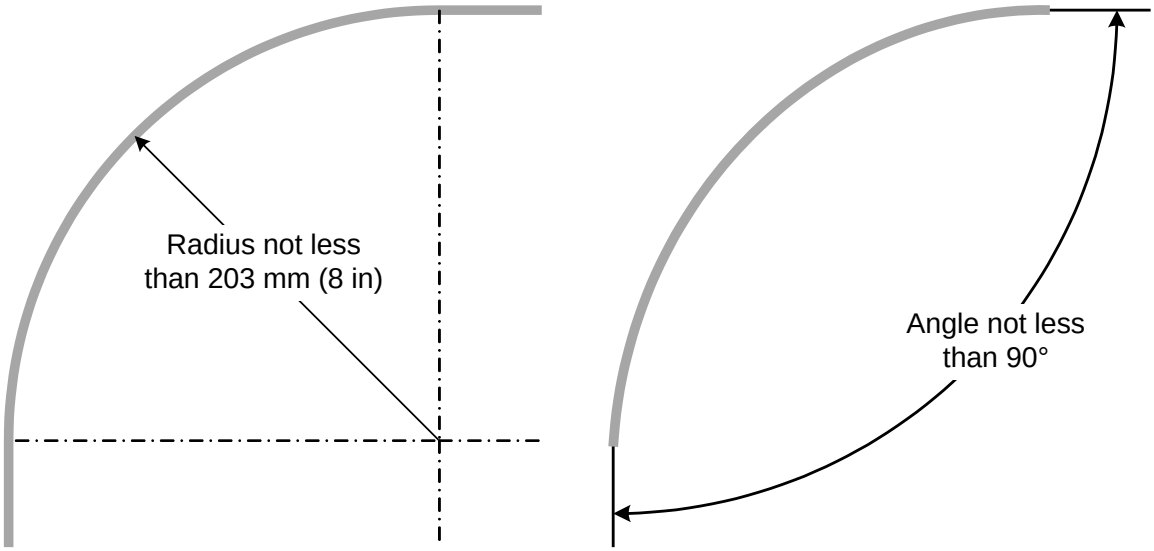
Grounding cable requirements

When routing, fastening and connecting grounding cables, the following requirements must be implemented:

- Grounding conductors must be run as short, straight, and smoothly as possible, with the fewest possible number of bends and curves.
- Grounding cables must not be installed with drip loops.
- All bends must have a minimum radius of 203 mm (8 in) and a minimum angle of 90° (Figure 2). A diagonal run is preferable to a bend, even though it does not follow the contour or run parallel to the supporting structure.
- All bends, curves and connections must be routed towards the grounding electrode system, ground rod, or ground bar.
- Grounding conductors must be securely fastened.

- Braided grounding conductors must not be used.
- Approved bonding techniques must be used for the connection of dissimilar metals.

Figure 2 Grounding cable minimum bend radius and angle



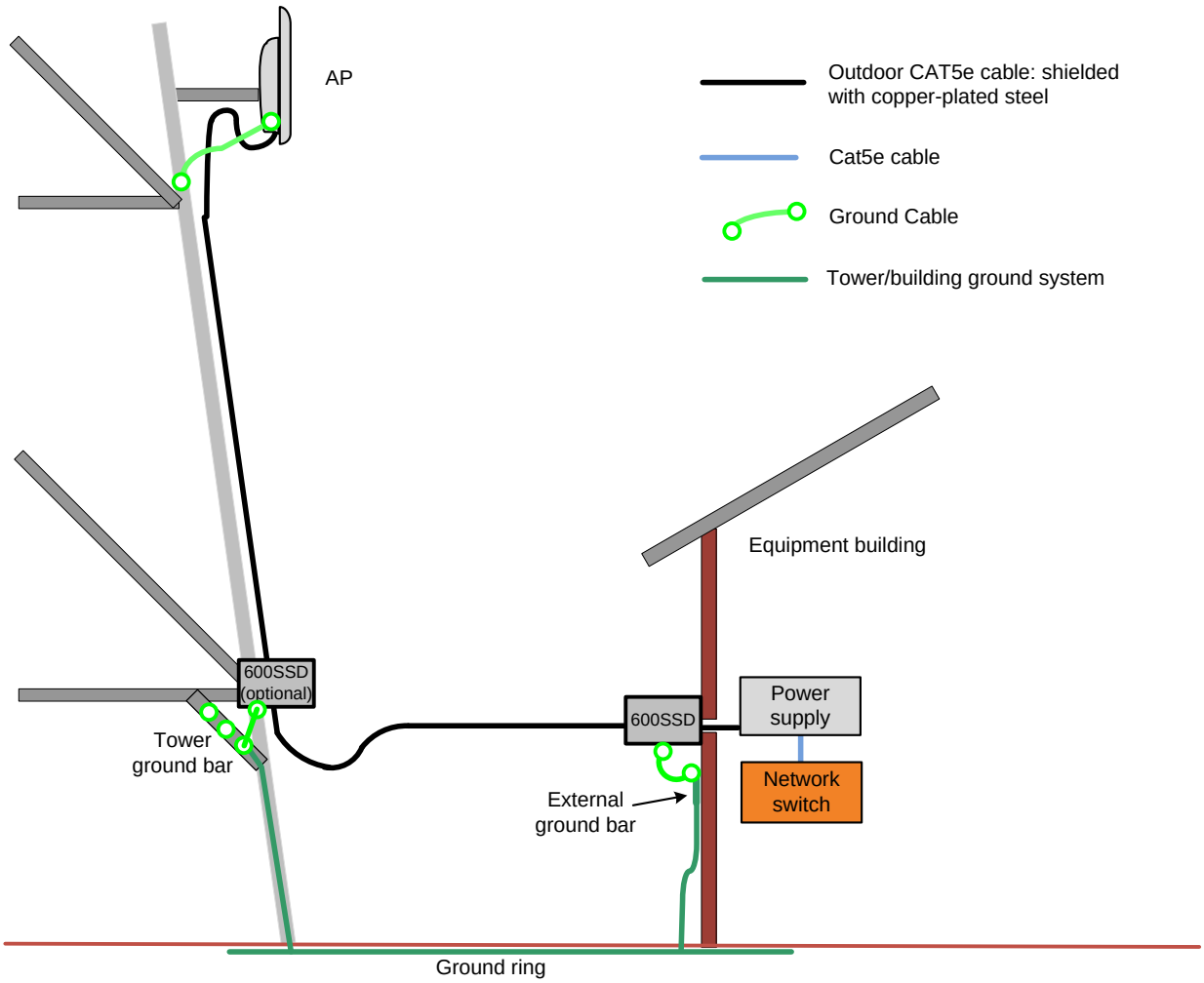
Protection requirements for a mast or tower installation

If the AP or SM is to be mounted on a metal tower or mast, then in addition to the general protection requirements (above), the following requirements must be observed:

- The equipment must be lower than the top of the tower or its lightning air terminal.
- The metal tower or mast must be correctly grounded.
- A grounding kit must be installed at the first point of contact between the drop cable and the tower, near the top.
- If the tower is greater than 61 m (200 ft) in height, an additional grounding kit must be installed at the tower midpoint. Additional ground kits must be installed as necessary to reduce the distance between ground kits to 61 m (200 ft) or less.
- In high lightning prone geographical areas, additional ground kits should be installed at spacing between 15 to 22 m (50 to 75 ft). This is especially important on towers taller than 45 m (150 ft).

Schematic examples of mast or tower installations are shown in Figure 3.

Figure 3 Grounding and lightning protection on mast or tower



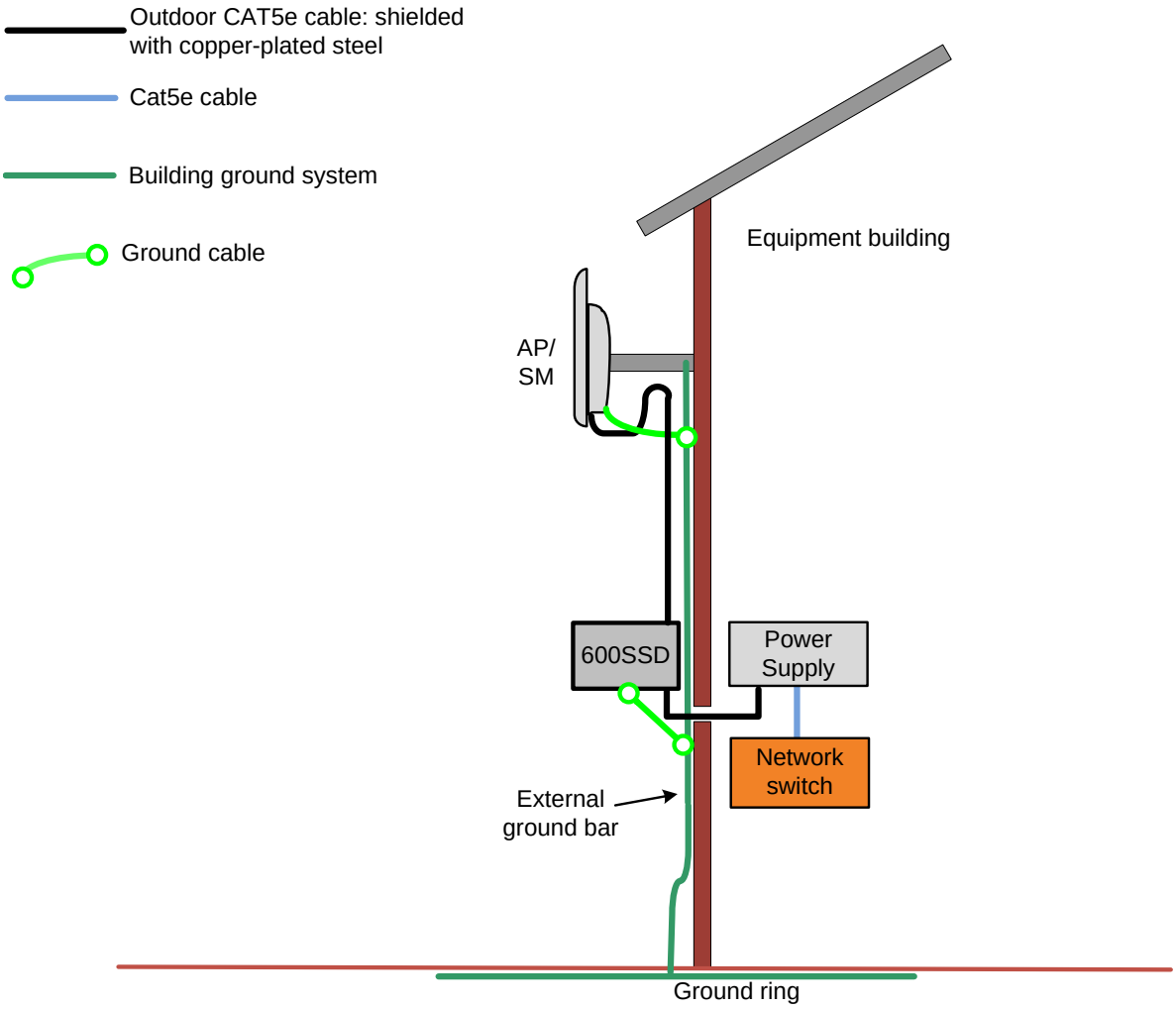
Protection requirements for a wall installation

If the AP or SM is to be mounted on the wall of a building, then in addition to the general protection requirements (above), the following requirements must be observed:

- The equipment must be lower than the top of the building or its lightning air terminal.
- The building must be correctly grounded.

Schematic examples of wall installations are shown in Figure 4.

Figure 4 Grounding and lightning protection on wall

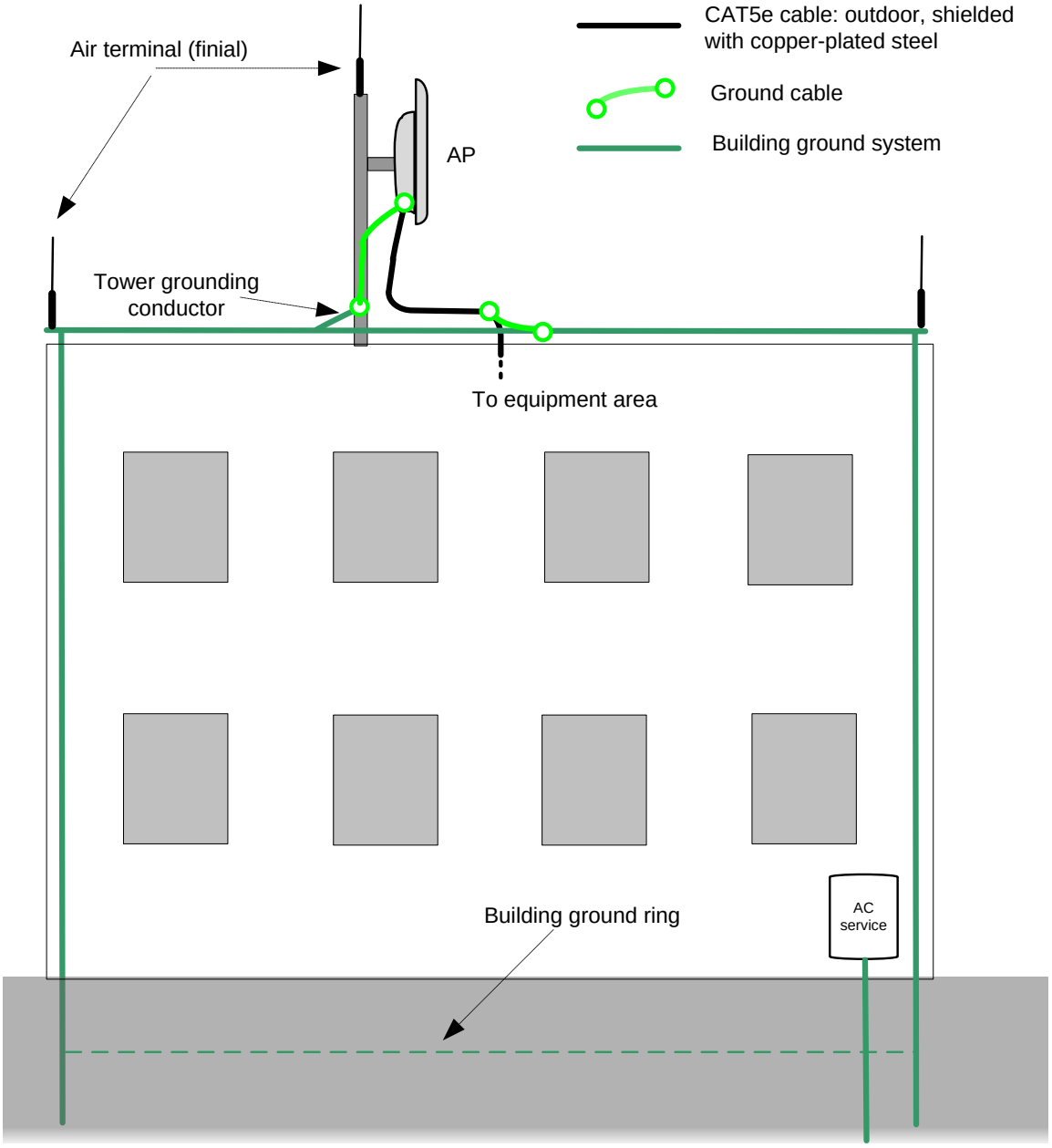


Protection requirements on a high rise building

If the AP is to be mounted on a high rise building, it is likely that cable entry is at roof level (Figure 5) and the equipment room is several floors below (Figure 6). The following additional requirements must be observed:

- The AP must be below the lightning terminals and finials.
- A grounding conductor must be installed around the roof perimeter, to form the main roof perimeter lightning protection ring.
- Air terminals are typically installed along the length of the main roof perimeter lightning protection ring typically every 6.1m (20ft).
- The main roof perimeter lightning protection ring must contain at least two down conductors connected to the grounding electrode system. The down conductors should be physically separated from one another, as far as practical.

Figure 5 Grounding and lightning protection on building

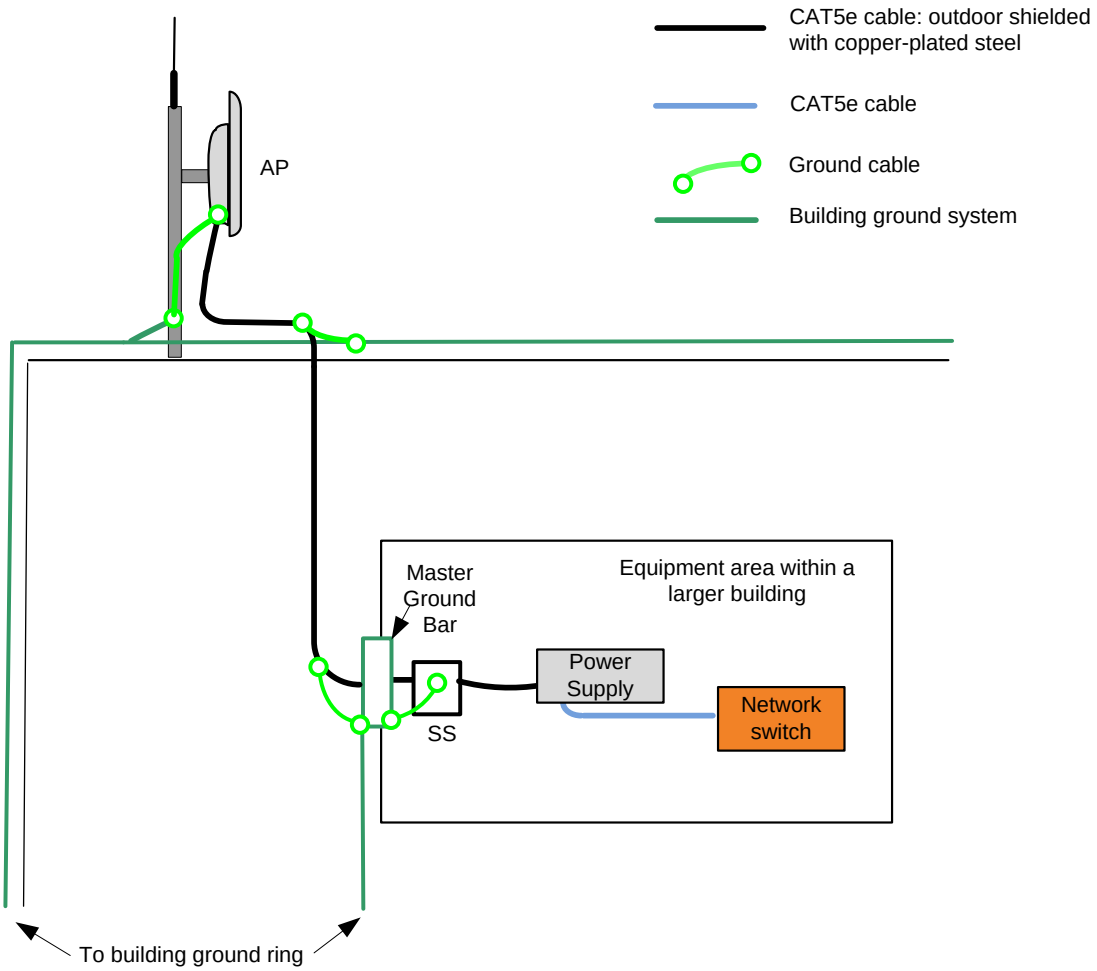


Protection inside a high rise building

The following protection requirements must be observed inside multi-story or high rise buildings (Figure 6):

- The drop cable shield must be bonded to the building grounding system at the entry point to the building.
- The drop cable shield must be bonded to the building grounding system at the entry point to the equipment area.

Figure 6 Grounding and lightning protection inside high building



Ordering components

This section describes how to select components for PMP 450 greenfield network or PMP 450 network migration. It specifies Cambium part numbers for PMP 450 components.

Radio module part numbers

Table 3 lists PMP 450 components.

Table 3 PMP 450 components

Part Number	Product Description	Notes
C054045A001A	PMP 450 Connectorized Access Point	
C054045A002A	PMP 450 Connectorized Access Point, US only	
C054045C001A	PMP 450 Subscriber Module, 4 Mbps	
C054045C002A	PMP 450 Subscriber Module, 10 Mbps	
C054045C003A	PMP 450 Subscriber Module, 20 Mbps	
C054045C004A	PMP 450 Subscriber Module, Uncapped	
AP Antenna Options		
85009324001	90 Degree Sector Antenna (H+V OFDM inputs)	
85009325001	60 Degree Sector Antenna (H+V OFDM, FSK input)	
85009326001	120 Degree Sector Antenna (H+V OFDM inputs)	
30009406002	N-type to N-type cable (16 inch length)	
	N-type cap for AP when using 90 degree or 120 degree sector antenna	
AP Optional Equipment		
ACPSSW-20A	POWER SUPPLY,20W, 29.5V, 100-240VAC/50-60HZ	
ACPSSW-21A	POWER SUPPLY,20W,29.5V,100-	

	240VAC/50-60HZ +C8 AC	
ACPS120WA	POWER SUPPLY,120W 30VDC AT 60C 100-240VAC EL5	
600SSD	SURGE PROTECTOR	
SMMB2A	UNIVERSAL MOUNTING BRACKET	
1070CKDB	CMM MICRO (OUTDOOR ENCLOSURE)	
1090CKBA	CMM4 W/RUGGEDIZED SWITCH AND GPS	
1091AA	CMM4 NO SWITCH	
1092AA	CMM4 RACK MOUNT ASSEMBLY	
1096A	UNIVERSAL GPS MODULE	
SM Optional Equipment		
ACPSSW-09B	POWER SUPPLY,13.6W, 29.5V, 100-240VAC/50-60HZ	
ACPSSW-10B	POWER SUPPLY,13.6W,29.5V,100-240VAC/50-60HZ+ARG	
ACPSSW-11B	POWER SUPPLY, 13.6W,29.5V,100-240VAC/50-60HZ+AUS	
ACPSSW-12C	POWER SUPPLY,ASSY,P/S,29.5V90-240VAC/50-60HZ PS	
ACPSSW-13B	POWER SUPPLY,13.6W,29.5V,100-240/50-60+FIXED US	
ACPSSW-14A	POWER SUPPLY,13.6W,29.5V,100-240VAC/50-60HZ+BRAZ	
C050000D001A	5 GHz CASSEGRAIN LENS (CLIP)	
HK2022A	53CM OFFSET, REFLECTOR DISH KIT,4PK	
SMMB1A	UNIVERSAL MOUNTING KIT	
600SSD	SURGE PROTECTOR	
200SS	SURGE PROTECTOR	
	Default Plug	
	Alignment tone headset	

License Keys		
C000045K001A	PMP 100 Compatibility License Key (Combo Key)	
Upgrade Keys		
C000045K002A	PMP 450 4 TO 10 MBPS UPGRADE KEY	
C000045K003A	PMP 450 4 TO 20 MBPS UPGRADE KEY	
C000045K004A	PMP 450 4 TO Uncapped UPGRADE KEY	
C000045K005A	PMP 450 10 TO 20 MBPS UPGRADE KEY	
C000045K006A	PMP 450 10 TO Uncapped MBPS UPGRADE KEY	
C000045K007A	PMP 450 20 TO Uncapped MBPS UPGRADE KEY	
Extended Warranty		
SG00TS4009A	PMP450 AP Extended Warranty, 1 Additional Year	
SG00TS4017A	PMP450 AP Extended Warranty, 2 Additional Years	
SG00TS4025A	PMP450 AP Extended Warranty, 4 Additional Years	
SG00TS4010A	PMP450 SM Extended Warranty, 1 Additional Year	
SG00TS4018A	PMP450 SM Extended Warranty, 2 Additional Years	
SG00TS4026A	PMP450 SM Extended Warranty, 4 Additional Years	

Chapter 2: Reference information

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

The following topics are described in this chapter:

- Equipment specifications on page 2-27 contains specifications of the AP, SM and other equipment required for PMP 450 installations.
- Wireless specifications on page 2-32 contains specifications of the PMP 450 wireless interface, including RF bands, channel width and link loss.
- Data network specifications on page 2-34 contains specifications of the PMP 450 Ethernet interface.
- Compliance with safety standards on page 2-35 lists the safety specifications against which the PMP 450 has been tested and certified. It also describes how to keep RF exposure within safe limits.
- Compliance with radio regulations on page 2-41 describes how the PMP 450 complies with the radio regulations that are in force in various countries.
- Notifications on page 2-45 contains notifications made to regulatory bodies for the PMP 450.
- Data throughput tables on page 2-49 contains tables and graphs to support calculation of the data rate capacity that can be provided by PMP 450 configurations.

Equipment specifications

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

AP specifications

The PMP 450 AP conforms to the specifications listed in Table 4. These specifications apply to all PMP 450 product variants.

Table 4 Connectorized AP physical specifications

Category	Specification
Product	
Model Number	C054045A001A, C054045A002A
Spectrum	
Channel Spacing	Configurable on 5 MHz increments
Frequency Range	5470 – 5875 MHz
Channel Width	20 MHz
Interface	
MAC (Media Access Control) Layer	Cambium Proprietary
Physical Layer	2x2 MIMO OFDM
Ethernet Interface	10/100BaseT, half/full duplex, rate auto negotiated (802.3 compliant)
Protocols Used	IPv4, UDP, TCP, IP, ICMP, Telnet, SNMP, HTTP, FTP
Network Management	HTTP, Telnet, FTP, SNMP v2c
VLAN	802.1ad (DVLAN Q-inQ), 802.1Q with 802.1p priority, dynamic port VID
Performance	
Nominal Receive Sensitivity (w/ FEC) @ 20 MHz Channel	OFDM: 1x = -87 dBm, 2x = -80 dBm, 3x = -73 dBm

Category	Specification
Maximum Deployment Range	Up to 40 km (25 mi)
Subscribers Per Sector	Up to 200
ARQ	Yes
Cyclic Prefix	1/16
Modulation Levels (Adaptive)	OFDM: QPSK, 16-QAM, 64-QAM (MIMO-B)
Latency	3 – 5 ms
GPS Synchronization	Yes, via CMM3, CMM4, or UGPS
Quality of Service	Diffserv QoS
Link Budget	
Antenna Beam Width	60º sectors
Transmit Power	-30 to +19 dBm (to EIRP limit by region) in 1 dB-configurable intervals
Antenna Gain	17 dBi Horizontal and Vertical
Maximum Transmit Power	22 dBm combined OFDM
Physical	
Wind Loading	190 km/hour (118 mi/hour)
Antenna Connection	50 ohm, N-type
Environmental	IP67
Temperature	-40ºC to +55ºC (-40ºF to +131ºF)
Weight	5.9 kg (13 lbs) with antenna 2.5 kg (5.5 lbs) without antenna
Wind Survival	90 lb (173 N)
Dimensions (H x W x D)	Radio: 27 x 21 x 7 cm (10.6” x 8.3” x 2.8”) Antenna: 51 x 13 x 7.3 cm (20.2” x 5.1” x 2.9”)

Category	Specification
Maximum Power Consumption	18 W
Input Voltage	24 to 30 V
Security	
Encryption	56-bit DES
Certifications	
FCC ID	TBD
Industry Canada Cert	TBD
CE	TBD

SM specifications

The PMP 450 SM conforms to the specifications listed in Table 4 and **Error! Reference source not found.**. These specifications apply to all PMP 450 product variants.

Figure 7 SM specifications

Category	Specification
Product	
Model Number	C054045C001A, C054045C002A, C054045C003A, C054045C004A
Spectrum	
Channel Spacing	Configurable on 5 MHz increments
Frequency Range	5470 – 5875 MHz
Channel Width	20 MHz
Interface	
MAC (Media Access Control) Layer	Cambium Proprietary
Physical Layer	2x2 MIMO OFDM
Ethernet Interface	10/100BaseT, half/full duplex, rate auto negotiated (802.3 compliant)

Category	Specification
Protocols Used	IPv4, UDP, TCP, IP, ICMP, Telnet, SNMP, HTTP, FTP
Network Management	HTTP, Telnet, FTP, SNMP v2c
VLAN	802.1ad (DVLAN Q-in-Q), 802.1Q with 802.1p priority, dynamic port VID
Performance	
Nominal Receive Sensitivity (w/ FEC) @ 20 MHz Channel	OFDM: 1x = -87 dBm, 2x = -84 dBm, 4x = -77 dBm, 6x = -70 dBm
Maximum Deployment Range	Up to 40 km (25 mi)
ARQ	Yes
Cyclic Prefix	1/16
Modulation Levels (Adaptive)	OFDM: 1x = QPSK, 2x = QPSK-MIMO-B, 4x = 16-QAM-MIMO-B, 6x = 64-QAM-MIMO-B)
Latency	5 - 7 ms
Packets Per Second	TBD
GPS Synchronization	Yes
Quality of Service	Diffserv QoS
Link Budget	
Antenna Beam Width	55° azimuth, 55° elevation (both horizontal and vertical)
Transmit Power	-30 to +19 dBm (to EIRP limit by region) in 1 dB-configurable intervals
Antenna Gain	8 dBi H+V, integrated patch
Maximum Transmit Power	19 dBm combined
Reflector Gain	+15 dBi
LENS Gain	+8 dBi
Physical	

Category	Specification
Wind Loading	190 km/hour (118 mi/hour)
Environmental	IP55
Temperature	-40°C to +55°C (-40°F to +131°F)
Weight	0.45 kg (1 lb)
Wind Survival	90 lb (173 N)
Dimensions (H x W x D)	30 x 9 x 9 cm (11.75" x 3.4" x 3.4")
Maximum Power Consumption	12 W
Input Voltage	24 to 30 V
Security	
Encryption	56-bit DES
Certifications	
FCC ID	TBD
Industry Canada Cert	TBD
CE	TBD

Wireless specifications

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

General wireless specifications

Table 5 lists the wireless specifications that apply to all PMP 450 variants.

Table 5 PMP 450 wireless specifications

Item	Specification
Channel selection	Manual selection (fixed frequency). Dynamic frequency selection (DFS) is available in radar avoidance regions.
Manual power control	To avoid interference to other users of the band, maximum power can be set lower than the default power limit.
Duplex scheme	Adaptive TDD
Range	TBD
Over-the-air encryption	DES
Error Correction	FEC

Available spectrum settings

This section shows how the spectrum available for PMP 450 usage is divided into radio channels. This division is based on configured parameters such as region code and channel bandwidth.

5.7-GHz Single AP Available Channels

A single 5.7-GHz AP enabled for frequencies can operate in the following channels, which are separated by 5-MHz increments.

Table 6 5.7 GHz available channels

(All Frequencies in GHz)

5.735	5.765	5.795	5.825	5.855
5.740	5.770	5.800	5.830	5.860
5.745	5.775	5.805	5.835	5.865
5.750	5.780	5.810	5.840	
5.755	5.785	5.815	5.845	
5.760	5.790	5.820	5.850	

The channels of *adjacent* APs should be separated by at least 20 MHz. However, 25 MHz of separation is advised.

5.7-GHz AP Cluster Recommended Channels

Six non-overlapping channels are recommended for use in 5.7-GHz AP clusters:

(All Frequencies in GHz)

5.735	5.775	5.815
5.755	5.795	5.835

The fully populated cluster requires only three channels, each reused by the module that is mounted 180° offset. The six channels above are also used for backhaul point-to-point links.

As noted above, a 5.7-GHz AP can operate on a frequency as high as 5.840 GHz. Where engineering plans allow, this frequency can be used to provide an additional 5-MHz separation between AP channels.

Data network specifications

This section contains specifications of the PMP 450 Ethernet interface.

Ethernet interface

The PMP 450 Ethernet port conforms to the specifications listed in Table 7.

Table 7 PMP 450 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	IEEE 802.3 compatible
QoS	IEEE 802.1p, IEEE 802.1Q, IEEE 802.1ad, DSCP IPv4
Interface	10/100BaseT, half/full duplex, rate auto negotiated
Data Rates	See Data throughput tables on page 2-49
Maximum Ethernet Frame Size	1522 Bytes

NOTE

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

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

Compliance with safety standards

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

Electrical safety compliance

The PMP 450 hardware has been tested for compliance to the electrical safety specifications listed in Table 8.

Table 8 PMP 450 safety compliance specifications

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

Electromagnetic compatibility (EMC) compliance

Table 9 lists the EMC specification type approvals that have been granted for PMP 450.

Table 9 EMC emissions compliance

Variant	Region	Specification (Type Approvals)
PMP 450	USA	FCC Part 15 Class B
	Canada	RSS Gen and RSS 210
	Europe	EN55022 CISPR 22

Human exposure to radio frequency energy

Standards

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

- ANSI IEEE C95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.
- Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC) and respective national regulations.
- *Directive 2004/40/EC of the European Parliament and of the Council of 29 April 2004* on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites_e.html and Safety Code 6.
- EN 50383:2002 Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz - 40 GHz).
- BS EN 50385:2002 Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz – 40 GHz) – general public.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

Power density exposure limit

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

The applicable power density exposure limit from the standards (see Human exposure to radio frequency energy on page 2-36) is:

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

Calculation of power density

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

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

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

Where:	Is:
S	power density in W/m^2
P	maximum average transmit power capability of the radio, in W
G	total Tx gain as a factor, converted from dB
d	distance from point source, in m

Rearranging terms to solve for distance yields:

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

Calculated distances and power compliance margins

Table 10 shows calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination. These are conservative distances that include compliance margins. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

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

Explanation of terms used in Table 10:

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

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

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

S – power density (W/m^2)

d – minimum distance from point source (meters)

R – recommended distances (meters)

C – compliance factor

Table 10 Power compliance margins

Freq. Band	Antenna	Variable			*d* (calc u-lated)	Recom-mended Separation Distance	Power Compliance Margin
		P	G	S			
5.8 GHz OFDM	Integrated SM, 9 dBi patch	0.158 W (22 dBm)	7.9 (9 dB)	10 W/m² or 1 mW/cm²	10 cm	20 cm (8 in)	40.27
	Integrated SM, 9 dBi patch with 9 dBi Cassegrain LENS	0.158 W (22 dBm)	39.8 (16 dB)	10 W/m² or 1 mW/cm²	22.3 cm	50 cm (20 in)	49.96
	Integrated SM, 9 dBi patch with 18 dBi Reflector Dish	0.158 W (22 dBm)	251 (24 dB)	10 W/m² or 1 mW/cm²	56.1 cm	100 cm (40 in)	31.69
	Connectorized AP, with 17 dBi Sector Antenna	0.158 W (22 dBm)	50 (17 dB)	10 W/m² or 1 mW/cm²	25.1 cm	50 cm (20 in)	39.77

NOTE

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

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

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

NOTE

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

Compliance with radio regulations

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

⚠ CAUTION

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

Type approvals

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

Table 9 lists the radio specification type approvals that have been granted for PMP 450 frequency variants.

Table 11 Radio certifications

Variant	Region	Specification (Type Approvals)
PMP 58450	USA	FCC Part 15 Class B
	CANADA	RSS Gen and RSS 210
	UK	EN55022 CISPR 22
	EU	FCC Part 15 Class B

FCC and ETSI compliance testing

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

NOTE

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

NOTE

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

Region Codes

Table 12 lists the region codes available on PMP 450 AP and SM units. Region code settings affect the radios in the following ways:

- Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain)
- DFS operation is enabled based on the configured region code, if applicable

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

Table 12 Region Code Information for PMP 450 AP

OFDM Radio Model	Channel Size	Region Code(s)	Range of Center Frequencies Available (MHz)	Center Channel Spacing	# of Center Channels
PMP 450 Series AP, 5.8-GHz	20 MHz	United States, Canada, Australia, Brazil & Russia	5735 – 5840	5 MHz	22
		Europe & Other	5735 – 5865	5 MHz	27
		Spain	5735 – 5785 5825 – 5845	5 MHz	16
		India	5835 – 5865	5 MHz	7
		Indonesia	5725 – 5825	5 MHz	21

Table 13 Region Code transmit power regulation

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

FCC and ICC IDs and certification numbers

Table 14 US FCC IDs and Industry Canada Certification Numbers and Covered Configurations

FCC ID	Industry Canada Cert Number	Frequencies	Module Families	Antenna (OFDM)	Maximum Tx Output Power
ABZ89FT7634	109W-5780	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5780APC	17 dBi Connectorized	19 dBm
ABZ89FT7635	109W-5790	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated	19 dBm
ABZ89FT7635	109W-5790	20 MHz channels, centered on 5735-5840 in 5 MHz increments (within the 5725-5850 MHz ISM band)	5790SM	9 dBi Integrated with 18 dBi Reflector Dish	19 dBm

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

Notifications

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

PMP 450 regulatory compliance

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

PMP 450 FCC and IC notification

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

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

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

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

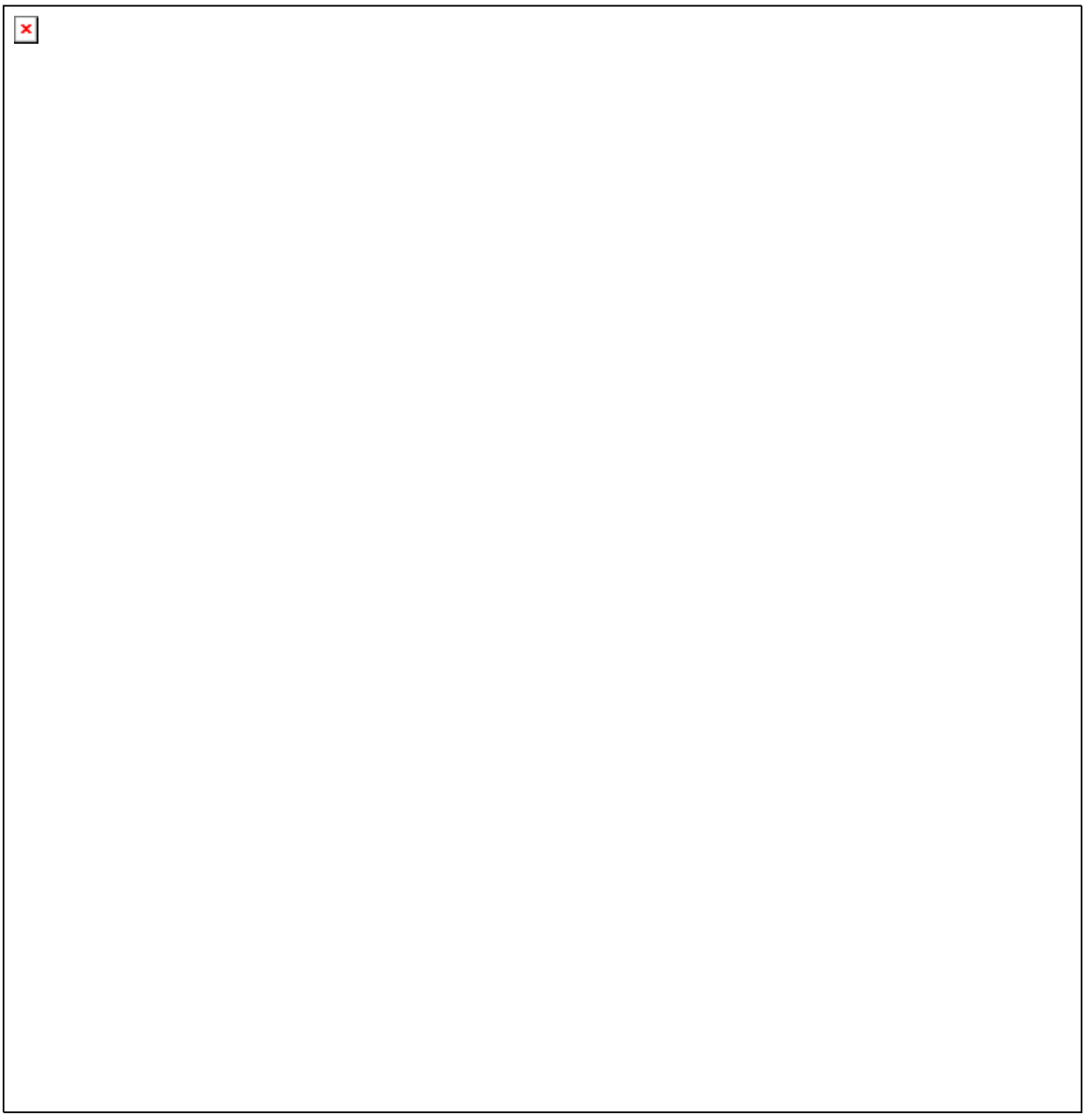
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules and with RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment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

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;

- Consult the dealer and/or experienced radio/TV technician for help.

FCC IDs and Industry Canada Certification Numbers are reproduced on the product label (Figure 8).

Figure 8 FCC and IC certifications on 5.8 GHz product label



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

PMP 450 European Union notification

The PMP 450 is a Class 2 device as it operates on frequencies that are not harmonized across the EU. Currently the product may only be operated in the UK, Eire (IRL), Germany, Norway and Denmark. However, the regulatory situation in Europe is changing and the radio spectrum may become available in other countries in future. See www.ero.dk for further information. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

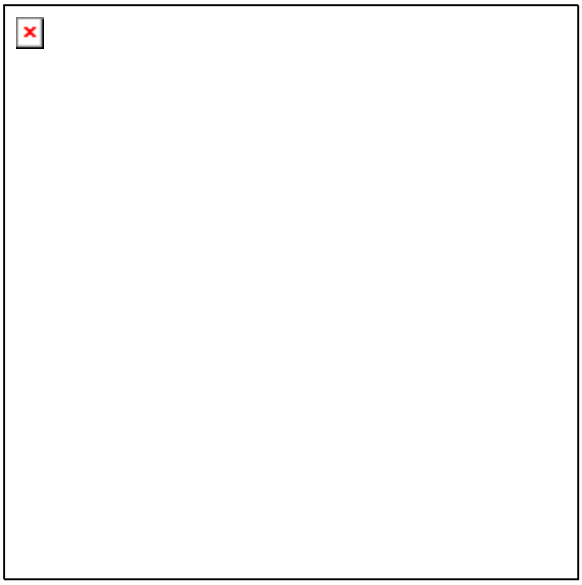
⚠ CAUTION

This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and must not cause harmful interference on systems operating as primary applications.

Hereby, Cambium declares that the PMP 450 product complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at the support website.

The European R&TTE directive 1999/5/EC Certification Number is reproduced on the product label (Figure 9).

Figure 9 European Union certification on 5.8 GHz product label



PMP 450 operation in the UK

The PMP 450 connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK Interface Requirement IR2007 specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

Data throughput tables

This section contains tables and graphs to support calculation of the data rate capacity that can be provided by PMP 450 configurations.

Data throughput capacity

Table 15 Throughput for PMP 450

Modulation Mode	20 MHz		
	Tx	Rx	Both
QPSK (1x)			
QPSK-MIMO-B (2x)			
16QAM-MIMO-B (4x)			
64QAM-MIMO-B (6x)			

Chapter 3: Preparing for installation

This chapter describes how to install and test the hardware for a PMP 450 network. This chapter is arranged as follows:

- Preparing for installation on page 3-51: Describes the precautions to be observed and checks to be performed before proceeding with the installation.
- Testing the Components on page 3-53: Describes the procedures for unpacking and performing and initial staging of the PMP 450 equipment
- Configuring a Point-to-Multipoint Link for Test on page 3-63: Describes the procedures for testing the equipment's radio links
- Preparing Components for Deployment on page 3-86: Describes methods for gathering component-specific information and ensuring continued access to the modules

Preparing for installation

This section describes the checks to be performed before proceeding with the installation.

Unit pre-configuration

It is common practice to pre-configure the units during staging before site installation by performing the following tasks from the *PMP 450 Configuration and User Guide*

- Task 1: Connecting to the unit
- Task 2: Configuring IP and Ethernet interfaces
- Task 3: Upgrading the software version and using CNUT
- Task 4: Configuring General and Unit settings
- Task 5: Configuring security
- Task 6: Configuring radio parameters
- Task 7: Setting up SNMP agent
- Task 8: Configuring syslog
- Task 9: Configuring remote access
- Task 10: Monitoring the AP-SM link
- Task 11: Configuring quality of service
- Task 12: Configuring a RADIUS server

If the units are to be pre-configured during staging, the safety precautions below MUST be observed.

Safety precautions before installation

All national and local safety standards must be followed while developing a site, installing equipment, or performing maintenance.

⚠ WARNING

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate as soon as they are powered up.

Observe the following guidelines:

- Never work in front of the antenna when the unit is powered.
- Always power down the module when connecting and disconnecting the drop cable from the power supply.

Protection requirements

The installation must meet the requirements defined in Grounding and lightning protection on page 1-14.

Preparing personnel

In no event shall Cambium Networks be liable for any injury or damage caused during the installation of the Cambium PMP 450 equipment.

Ensure that only qualified personnel undertake the installation of a PMP 450 system.

Ensure that all safety precautions are observed.

Preparing inventory

Perform the following inventory checks:

- Check that the correct components are available, as described in Ordering components on page 1-23.
- Check the contents of all packages against their packing lists.

Preparing tools

Check that following specific tools are available, in addition to general tools:

- RJ45 crimp tool (it must be the correct tool for the type of RJ45 being used).
- Personal Computer (PC) with 10, 100 or 1000 BaseT Ethernet.
- Either Internet Explorer 7, Internet Explorer 8, Firefox 3 or Firefox 3.5.
- Ethernet patch cables.

Testing the Components

The best practice is to connect all components—APs, SMs, GPS antenna (if applicable), and CMM (if applicable)—in a test setting and initially configure and verify them before deploying them to an installation. In this way, any configuration issues are worked out before going on-site, on a tower, in the weather, where the discovery of configuration issues or marginal hardware is more problematic and work-flow affecting.

Unpacking Components

When you receive these products, carefully inspect all shipping boxes for signs of damage. If you find damage, immediately notify the transportation company.

As you unpack the equipment, verify that all the components that you ordered have arrived. Save all the packing materials to use later, as you transport the equipment to and from installation sites.

Configuring for Test

You can use either of two methods to configure an AP:

- Use the Quick Start feature of the product. For more information on Quick Start, see Quick Start Page of the AP on Page 3-64.
- Manually set each parameter.

After you change configuration parameters on a GUI web page:

- Before you leave a web page, click the **Save** button to save the change(s).
- After making change(s) on multiple web pages, click the **Reboot** button to reboot the module and implement the change(s).

Configuring the Computing Device for Test

If your computer is configured for Dynamic Host Configuration Protocol (DHCP), disconnect the computer from the network. If your computer is instead configured for static IP addressing

- set the static address in the 169.254 network
- set the subnet mask to 255.255.0.0.

Default Module Configuration

From the factory, the APs and SMs are all configured to *not transmit* on any frequency. This configuration ensures that you do not accidentally turn on an unsynchronized module. Site synchronization of modules is required because

- modules
  - cannot transmit and receive signals at the same time.
  - use TDD (Time Division Duplexing) to distribute signal access of the downlink and uplink frames.
- when one module transmits while an unintended module nearby receives signal, the transmitting module may interfere with or desense the receiving module. In this context, interference is self-interference (within the same network).

AP interfaces

The AP interfaces are illustrated in Figure 10 and described in Table 16.

Figure 10 AP interfaces

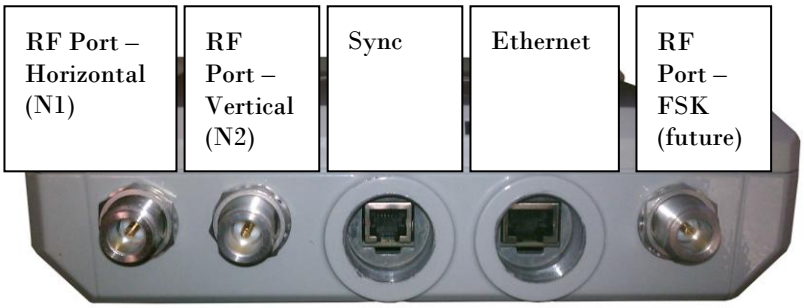


Table 16 AP Interfaces

Interface	Function	Cabling
RF Port – Horizontal (N1)	Horizontal RF connection to AP antenna	50 ohm RF cable, N-type
RF Port – Vertical (N2)	Vertical RF connection to AP antenna	50 ohm RF cable, N-type
Sync	GPS synchronization signaling, provides power to uGPS module	RJ11 cable

Interface	Function	Cabling
Power-over-Ethernet, Ethernet communications (management and data)	RJ45 cable	Power-over-Ethernet, Ethernet communications (management and data)
RF Port – FSK	For future use in "Combo" mode	50 ohm RF cable, N-type
Ground Lug (bottom of unit)	For grounding the unit	10 AWG copper wire

AP diagnostic LEDs

The diagnostic LEDs report the following information about the status of the module.

NOTE

The LED color helps you distinguish position of the LED. The LED color does not indicate any status.

Figure 11 AP diagnostic LEDs, viewed from unit front

Table 17 AP LEDs

LED	Color when active	Status information provided	Notes
PWR	red	DC power	Always lit when power is correctly supplied.
SYN/1	yellow	Presence of sync	Always lit on the AP.
SES/2	green	*Unused on the AP*	
GPS/3	red	Pulse of sync	Continuously lit as pulse as AP receives pulse.

LED	Color when active	Status information provided	Notes
ACT/4	yellow	Presence of data activity on the Ethernet link	Flashes during data transfer. Frequency of flash is not a diagnostic indication.
LNK/5	green	Ethernet link	Continuously lit when link is present.

SM interfaces

Figure 12 SM interfaces

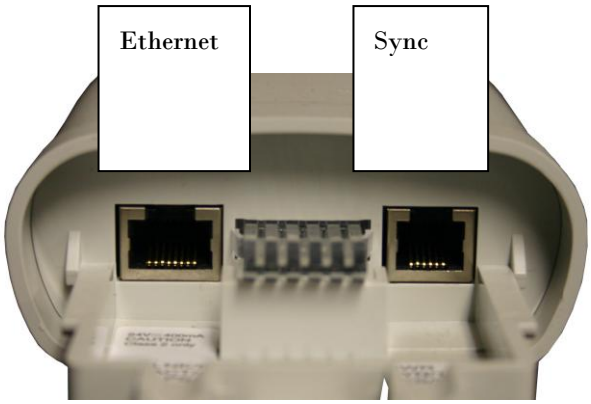


Table 18 SM Interfaces

Interface	Function	Cabling
Power-over-Ethernet, Ethernet communications (management and data)	Power-over-Ethernet, Ethernet communications (management and data)	RJ45 Cable
Synchronization/Default Plug Port	GPS synchronization signaling, provides power to uGPS module	RJ11 cable
Ground Lug (bottom of unit)	For grounding the unit	10 AWG copper wire

SM diagnostic LEDs

The diagnostic LEDs report the following information about the status of the module.

> **NOTE**
> The LED color helps you distinguish position of the LED. The LED color does not indicate any status.

Figure 13 SM diagnostic LEDs, viewed from unit front

Table 19 AP LEDs

LED	Color when active	Status information provided	Notes
LNK/5	green	Ethernet link	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.

LED	Color when active	Status information provided	Notes
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.

Standards for Wiring

Modules automatically sense whether the Ethernet cable in a connection is wired as straight-through or crossover. You may use either straight-through or crossover cable to connect a network interface card (NIC), hub, router, or switch to these modules. For a straight-through cable, use the EIA/TIA-568B wire color-code standard on both ends. For a crossover cable, use the EIA/TIA-568B wire color-code standard on one end, and the EIA/TIA-568A wire color-code standard on the other end.

Where you use the AC wall adapter

- the power supply output is +29.5 VDC.
- the power input to the SM is +11.5 VDC to +30 VDC.
- the maximum Ethernet cable run is 328 feet (100 meters).

Best Practices for Cabling

The following practices are essential to the reliability and longevity of cabled connections:

- Use only shielded cables to resist interference.
- For vertical runs, provide cable support and strain relief.
- Include a 2-ft (0.6-m) service loop on each end of the cable to allow for thermal expansion and contraction and to facilitate terminating the cable again when needed.
- Include a drip loop to shed water so that most of the water does not reach the connector at the device.
- Properly crimp all connectors.
- Use dielectric grease on all connectors to resist corrosion.
- Use only shielded connectors to resist interference and corrosion.

Recommended Tools for Wiring Connectors

The following tools may be needed for cabling the AP:

- RJ-11 crimping tool
- RJ-45 crimping tool
- electrician scissors
- wire cutters
- cable testing device.

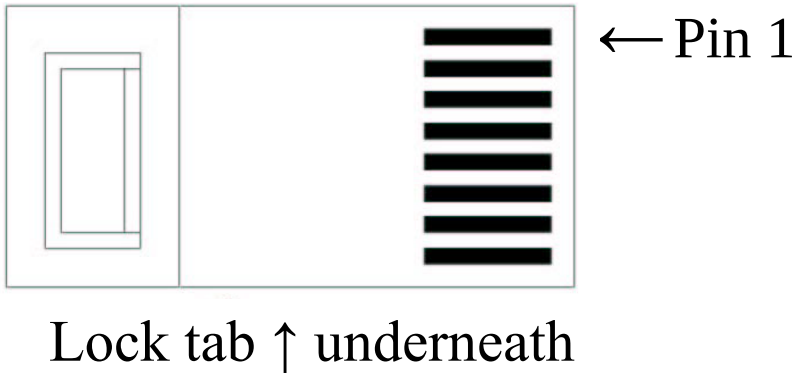
Wiring Connectors

The following diagrams correlate pins to wire colors and illustrate crossovers where applicable.

Location of Pin 1

Pin 1, relative to the lock tab on the connector of a straight-through cable is located as shown below.

Table 20 Pin 1 location

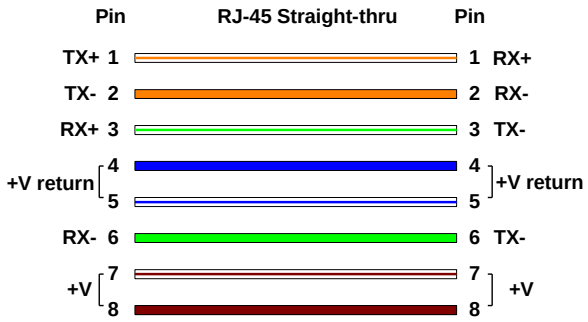


RJ-45 Pinout for Straight-through Ethernet Cable

Table 21 RJ-45 pinout for straight-through Ethernet cable

Pin 1 →	white / orange	← Pin 1
Pin 2 →	orange	← Pin 2
Pin 3 →	white / green	← Pin 3
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 6
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

Pins 7 and 8 carry power to the modules.

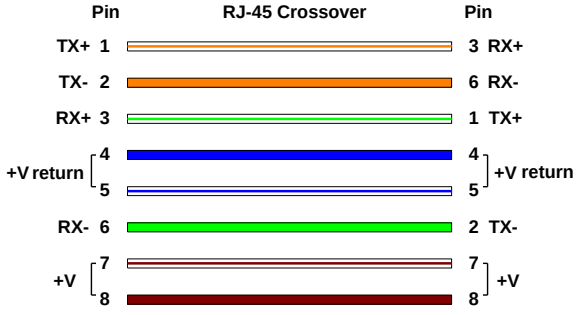


RJ-45 Pinout for Crossover Ethernet Cable

Table 22 RJ-45 pinout for crossover Ethernet cable

Pin 1 →	white / orange	← Pin 3
Pin 2 →	orange	← Pin 6
Pin 3 →	white / green	← Pin 1
Pin 4 →	blue	← Pin 4
Pin 5 →	white / blue	← Pin 5
Pin 6 →	green	← Pin 2
Pin 7 →	white / brown	← Pin 7
Pin 8 →	brown	← Pin 8

Pins 7 and 8 carry power to the modules.



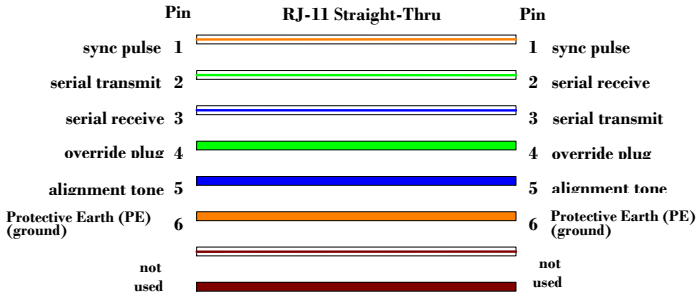
RJ-11 Pinout for Straight-through Sync Cable

The system uses a utility cable with RJ-11 connectors between the AP or BH and synchronization pulse. Presuming CAT 5 cable and 6-pin RJ-11 connectors, the following diagram shows the wiring of the cable for sync.

Table 23 RJ-11 pinout for straight through sync cable

Pin 1 → white / orange	← Pin 1
Pin 2 → white / green	← Pin 2
Pin 3 → white / blue	← Pin 3
Pin 4 → green	← Pin 4
Pin 5 → blue	← Pin 5
Pin 6 → orange	← Pin 6

NOTE: The fourth pair is not used.



Alignment Tone—Technical Details

The alignment tone output from a module is available on Pin 5 of the RJ-11 connector, and ground is available on Pin 6. Thus the load at the listening device should be between Pins 5 and 6. The listening device may be a headset, earpiece, or battery-powered speaker.

Overriding Forgotten IP Addresses or Passwords on AP and SM

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

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

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

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

Constructing an Override Plug

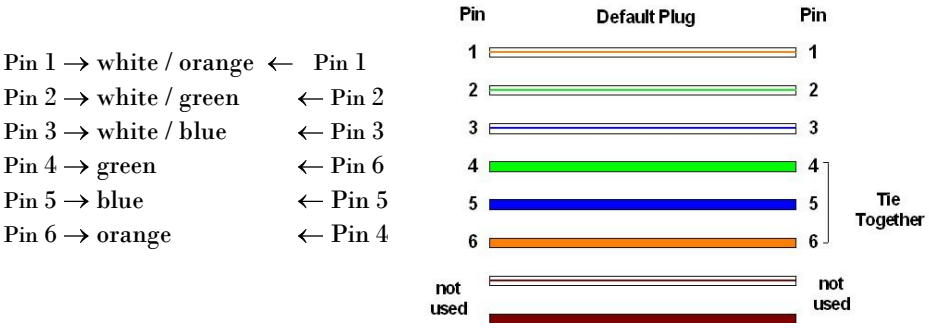
You can either purchase or fabricate an override plug as follows. To purchase an override plug for a nominal fee, order the plug at http://www.best-tronics.com. To fabricate an override plug, perform the following steps.

1 Install an RJ-11 6-pin connector onto a 6-inch length of CAT 5 cable

2 Pin out all 6-pins.

3 Short (solder together) Pins 4 and 6 on the other end. Do not connect any other wires to anything.

Figure 14 RJ-11 pinout for the override plug



Using the Override Plug

The following section details usage of the override plug to regain access to an AP or SM module.

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

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

1 Insert the override plug into the RJ-11 GPS utility port of the module.

2 Power cycle by removing, then re-inserting, the Ethernet cable.
RESULT: The module boots with the default IP address of 169.254.1.1, password fields blank, and all other configuration values as previously set.

3 Wait approximately 30 seconds for the boot to complete.

4 Remove the override plug.

5 Set passwords and IP address as desired.

6 Change configuration values if desired.

7 Click the Save Changes button.

8 Click the Reboot button.

Configuring a Point-to-Multipoint Link for Test

Powering the AP for test configuration

Perform the following steps to begin the test setup.

Table 24 Setting up the AP for Quick Start configuration

1. Plug one end of a CAT 5 Ethernet cable into the AP.
2. Plug the Ethernet cable connector labeled To Radio into the jack in the pig tail that hangs from the power supply.
3. Plug the other connector of the pig tail (this connector labeled To Computer) into the Ethernet jack of the computing device.
4. Plug the power supply into an electrical outlet.

   WARNING

   From this point until you remove power from the AP, stay at least as far from the AP as the minimum separation distance specified in Minimum separation distances on page II.
5. Power up the computing device
6. Start the browser in the computing device.
7. Start the browser in the computing device

The AP interface provides a series of web pages to configure and monitor the unit. You can access the web-based interface through a computing device that is either directly connected or connected through a network to the AP. If the computing device is not connected to a network when you are configuring the module in your test environment, and if the computer has used a proxy server address and port to configure a module, then you may need to first disable the proxy setting in the computer.

Perform the following procedure to toggle the computer to *not* use the proxy setting.

Table 25 Bypassing proxy settings to access module web pages

1. Launch Microsoft Internet Explorer
2. Select **Tools, Internet Options, Connections, LAN Settings.** Alternate web browser menu selections may differ.
3. Uncheck the **Use a proxy server...** box.

In the address bar of your browser, enter the IP address of the AP. (For example, enter **`http://169.254.1.1`** to access the AP through its default IP address). The AP responds by opening the General Status tab of its Home page.

Quick Start Page of the AP

To proceed with the test setup, click the **Quick Start** button on the left side of the General Status tab. The AP responds by opening the Quick Start page. The Quick Start tab of that page is displayed in Figure 15.

> **NOTE**
>
> If you cannot find the IP address of the AP, see Overriding Forgotten IP Addresses or Passwords on AP and SM.

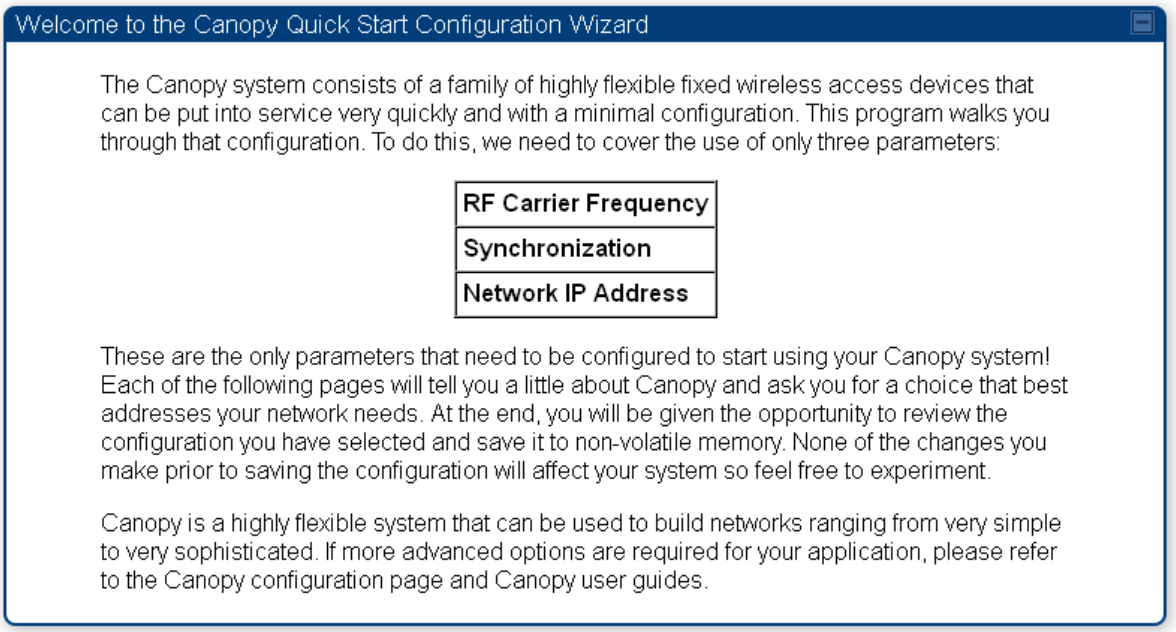


Figure 15: Quick Start tab of AP, example

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

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

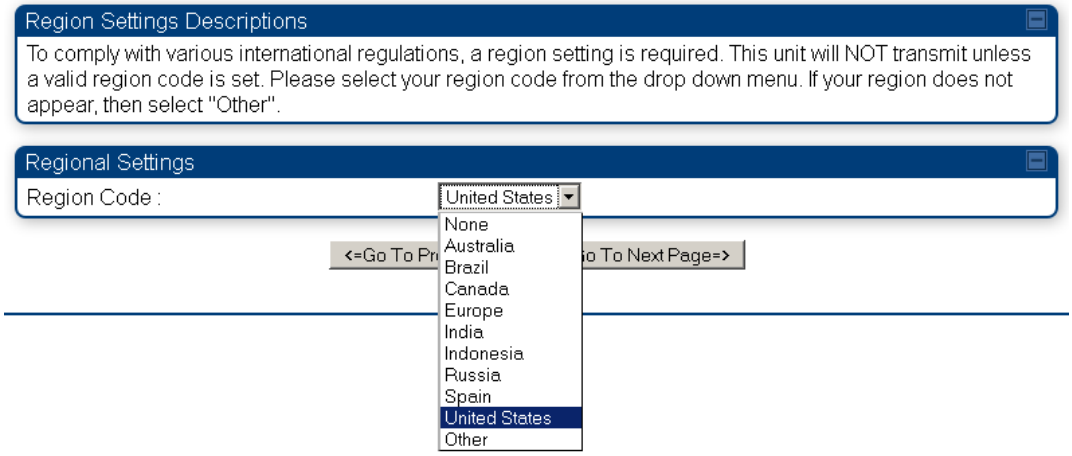
In each Quick Start tab, you can

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

Proceed with the test setup as follows.

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

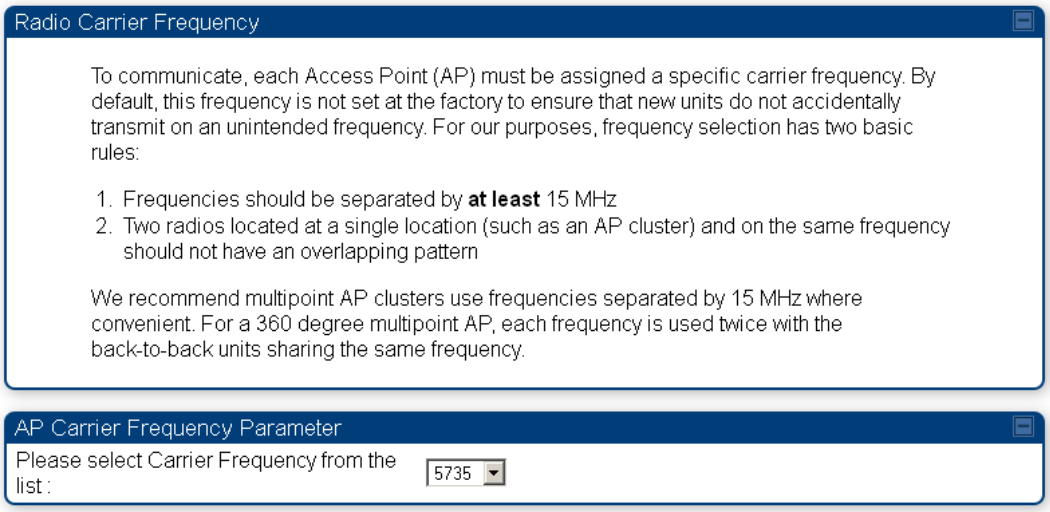
Figure 16 Regional Settings tab of AP



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

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

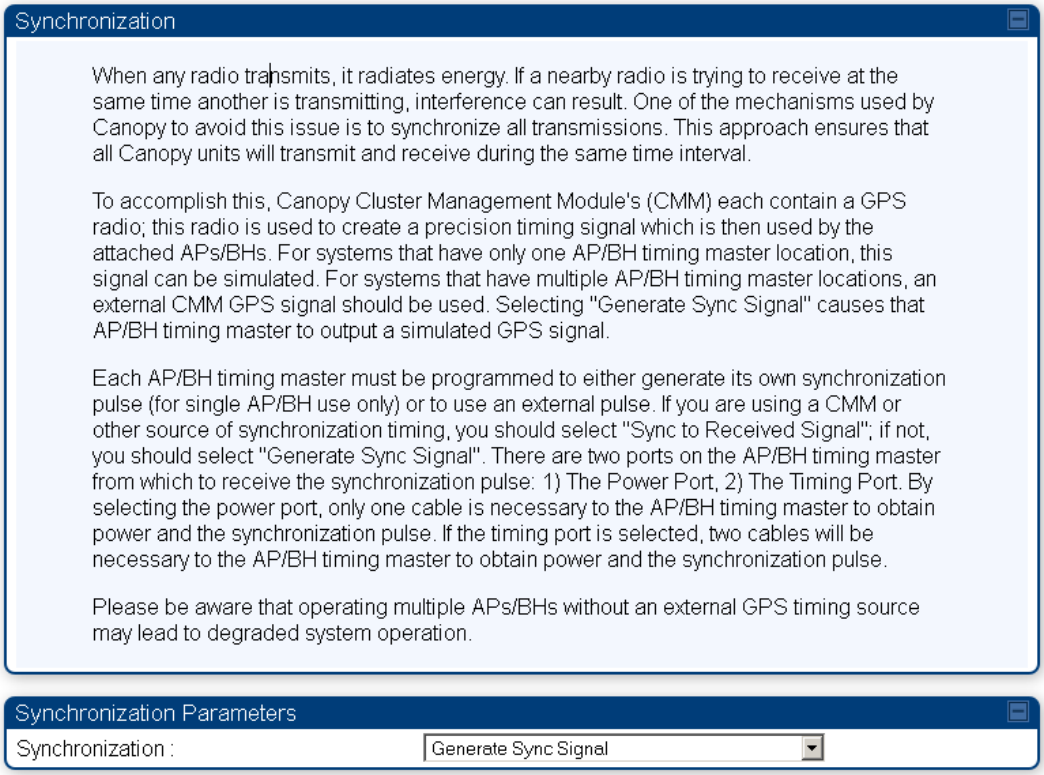
Figure 17 Radio Carrier Frequency tab of AP



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

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

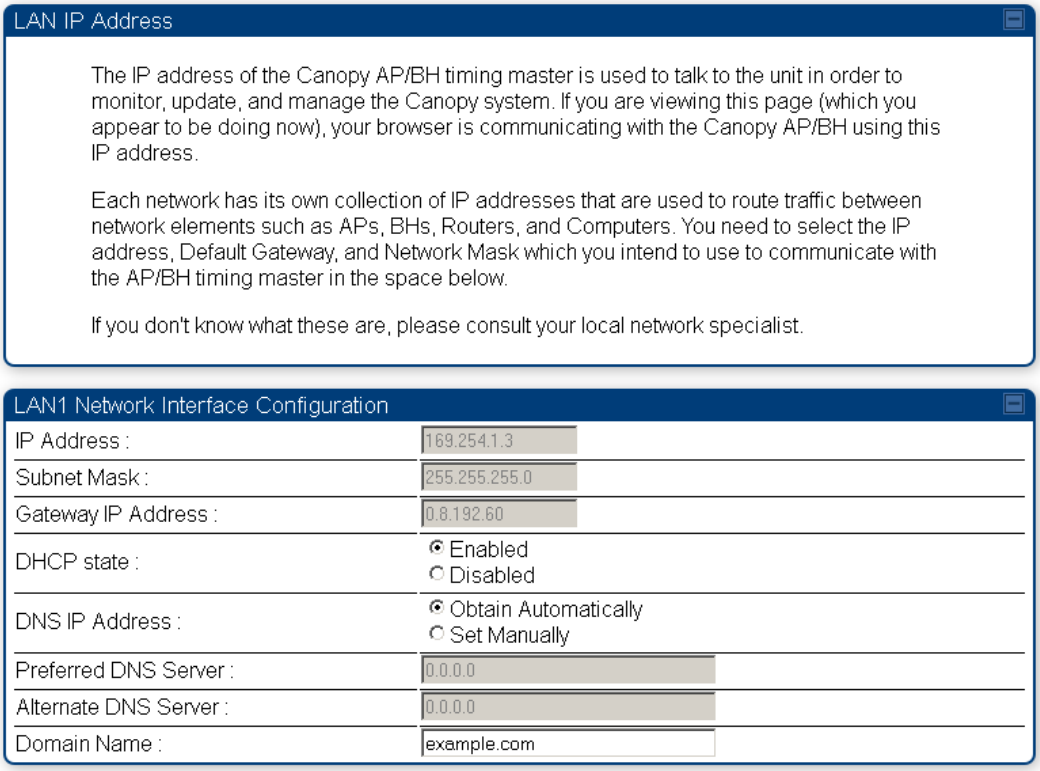
Figure 18 Synchronization tab of AP



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

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

Figure 19 LAN IP Address tab of the AP



8 At the bottom of this tab, either

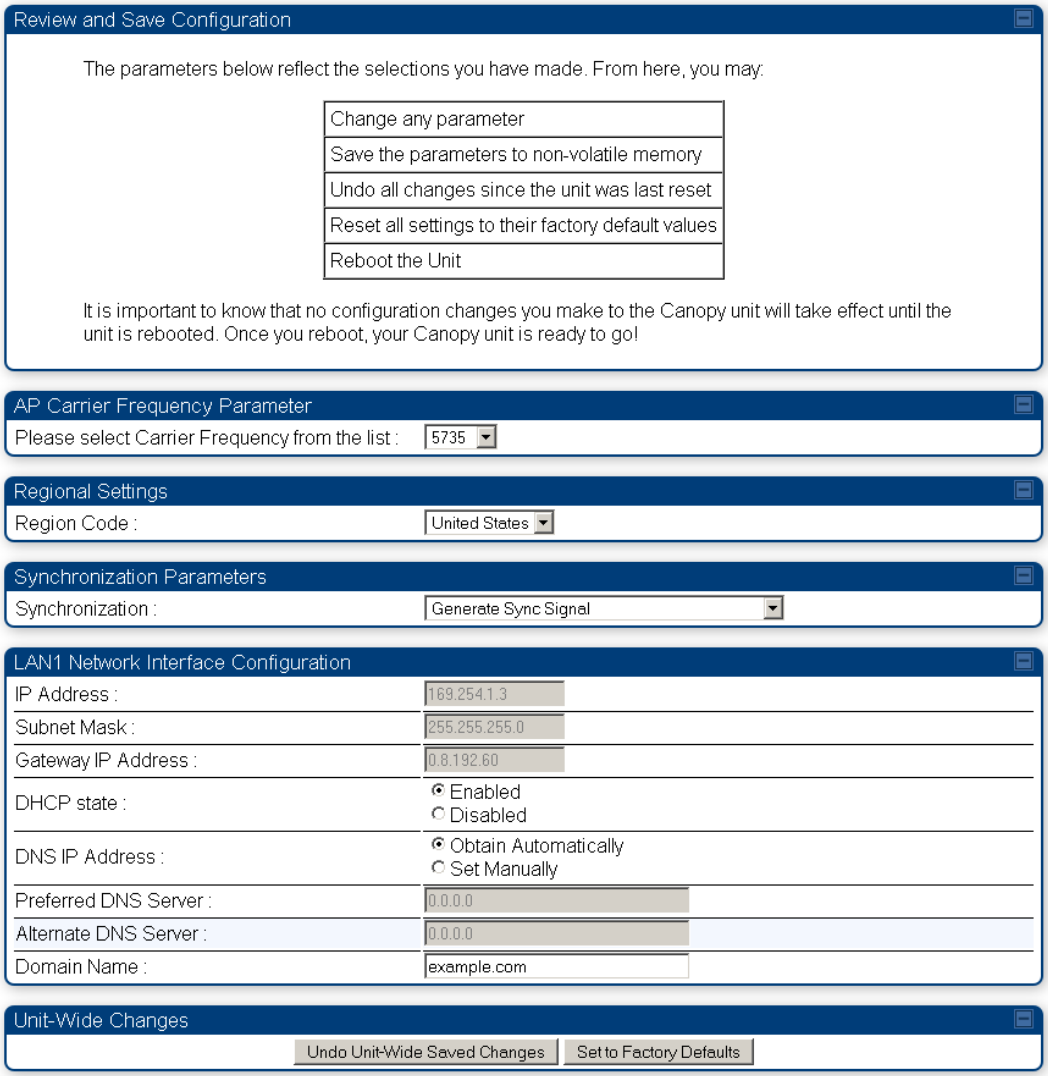
- specify an **IP Address**, a **Subnet Mask**, and a **Gateway IP Address** for management of the AP and leave the **DHCP state** set to **Disabled**.
- set the **DHCP state** to **Enabled** to have the IP address, subnet mask, and gateway IP address automatically configured by a domain name server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

NOTE

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

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

Figure 20 Review and Save Configuration tab of the AP



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

11 Click the **Save Changes** button.

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

13 Wait until the indicator LEDs are not red.

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

15 Wait until the red indicator LEDs are not lit.

Time Tab of the AP

To proceed with the test setup, click the **Configuration** link on the left side of the General Status tab. When the AP responds by opening the Configuration page to the General tab, click the Time tab. An example of this tab is displayed in Figure 21.

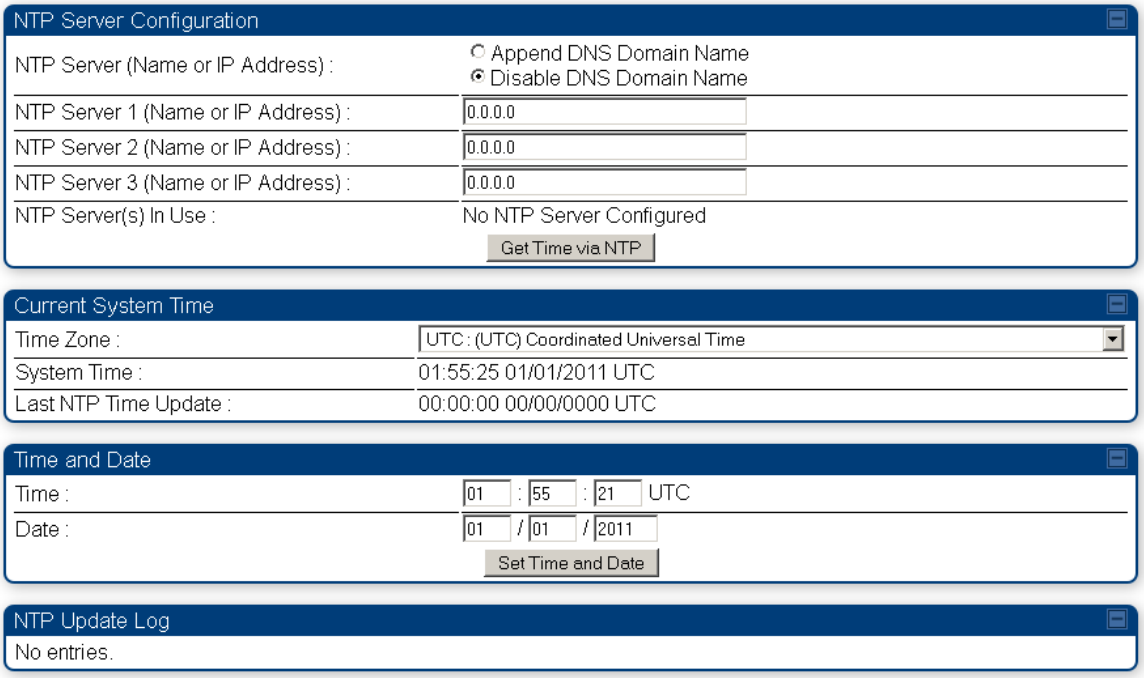


Figure 21: Time tab of AP, example

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

- A connected CMM passes time and date (GPS time and date, if received).
- A connected CMMmicro passes the time and date (GPS time and date, if received), but only if both the CMMmicro is operating on CMMmicro Release 2.1 or later release. (These releases include an NTP server functionality.)
- A separate NTP server is addressable from the AP.

If the AP should obtain time and date from a CMMmicro, CMM4, or a separate NTP server, enter the IP address of the CMM or NTP server on this tab. To force the AP to obtain time and date before the first (or next) 15-minute interval query of the NTP server, click **Get Time through NTP**.

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

Time : hh / mm / ss

Date : MM / dd / yyyy

where

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

Proceed with the time setup as follows.

1. Enter the appropriate information in the format shown above.
2. Then click the **Set Time and Date** button.
   NOTE: The time displayed at the top of this page is static unless your browser is set to automatically refresh

Powering the SM for test

1. In one hand, securely hold the top (larger shell) of the SM. With the other hand, depress the lever in the back of the base cover (smaller shell). Remove the base cover.
2. Plug one end of a CAT 5 Ethernet cable into the SM RJ-45 jack.
3. Plug the other end of the Ethernet cable into the jack in the pig tail that hangs from the power supply.
4. Roughly aim the SM toward the AP.
5. Plug the power supply into an electrical outlet.

⚠ WARNING

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

6. Repeat the foregoing steps for each SM that you wish to include in the test.
7. Back at the computing device, on the left side of the Time & Date tab, click **Home**.
8. Click the Session Status tab.

Session Status Tab of the AP

An example of the AP Session Status tab is displayed in Figure 22.

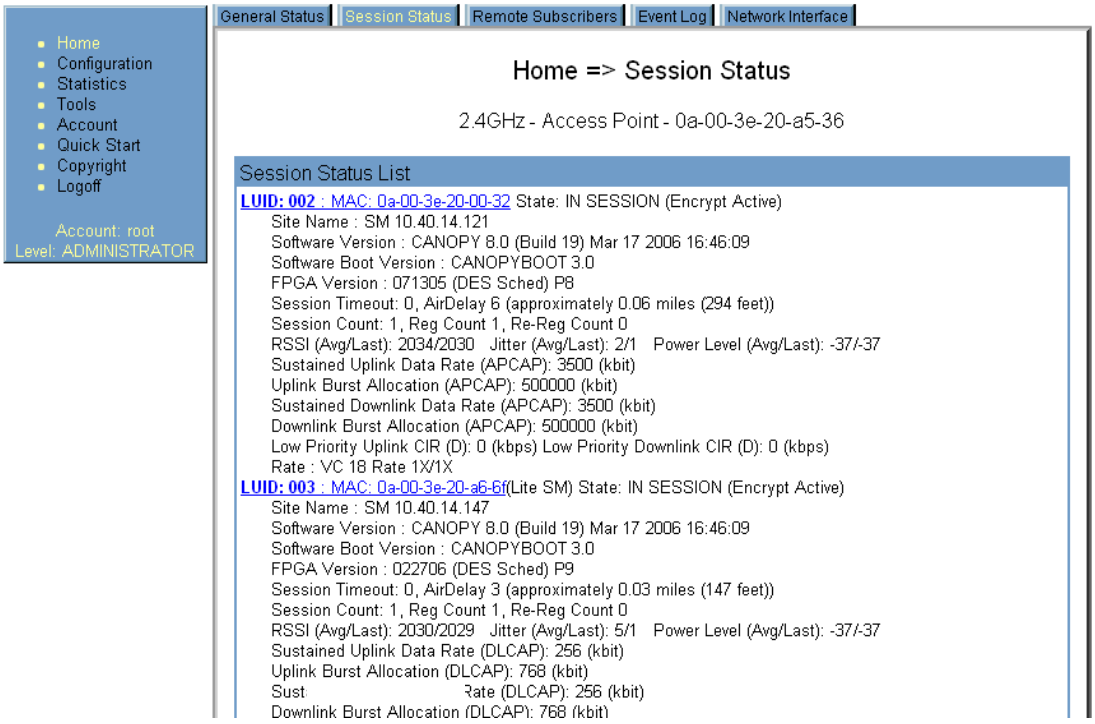


Figure 22: Session Status tab data from AP, example

If no SMs are registered to this AP, then the Session Status tab displays the simple message **No sessions**. In this case, try the following steps.

1. More finely aim the SM or SMs toward the AP.
2. Recheck the Session Status tab of the AP for the presence of LUIDs.
3. If still no LUIDs are reported on the Session Status tab, click the **Configuration** button on the left side of the Home page.
   RESULT: The AP responds by opening the AP Configuration page.
4. Click the Radio tab.
5. Find the **Color Code** parameter and note the setting.
6. In the same sequence as you did for the AP directly under Configuring a Point-to-Multipoint Link for Test on Page 3-63, connect the SM to a computing device and to power.
7. On the left side of the SM Home page, click the **Configuration** button.
   RESULT: The Configuration page of the SM opens.

8. Click the Radio tab.
9. If the transmit frequency of the AP is not selected in the **Custom Radio Frequency Scan Selection List** parameter, select the frequency that matches.
10. If the **Color Code** parameter on this page is not identical to the **Color Code** parameter you noted from the AP, change one of them so that they match.
11. At the bottom of the Radio tab for the SM, click the **Save Changes** button.
12. Click the **Reboot** button.
13. Allow several minutes for the SM to reboot and register to the AP.
14. Return to the computing device that is connected to the AP.
15. Recheck the Session Status tab of the AP for the presence of LUIDs.

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

The Session Status tab also includes the current active values on each SM (LUID) for MIR, CIR, and VLAN, as well as the source of these values (representing the SM itself, BAM, or the AP and cap, if any—for example, APCAP as shown in Figure 22 above). L indicates a Lite SM (CSM 110), and D indicates from the device. As an SM registers to the AP, the configuration source that this page displays for the associated LUID may change. After registration, however, the displayed source is stable and can be trusted.

The Session Status tab of the AP provides the following parameters.

Show Idle Sessions

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

Table 26 Session Status Attributes

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

Attribute	Meaning
Session Count	This field displays how many sessions the SM has had with the AP. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum. If the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.
Reg Count	When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field.
Re-Reg Count	When an SM makes a registration request, the AP checks its local data to see whether it considers the SM to be already registered. If the AP concludes that the SM is not, then the request increments the value of this field. Typically, a Re-Reg is the case where both • an SM attempts to reregister for having lost communication with the AP. • the AP has not yet observed the link to the SM as being down.
Sustained Uplink Data Rate	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified rate at which each SM registered to this AP is replenished with credits for transmission. The configuration source of the value is indicated in parentheses.
Uplink Burst Allocation	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified maximum amount of data that each SM is allowed to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. The configuration source of the value is indicated in parentheses.
Sustained Downlink Data Rate	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the specified the rate at which the AP should be replenished with credits (tokens) for transmission to each of the SMs in its sector. The configuration source of the value is indicated in parentheses.
Downlink Burst Allocation	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. This is the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. The configuration source of the value is indicated in parentheses.

Attribute	Meaning
Low Priority Uplink CIR	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses.
Low Priority Downlink CIR	This field displays the value that is currently in effect for the SM, with the source of that value in parentheses. The configuration source of the value is indicated in parentheses.
Rate	This field displays whether the high-priority channel is enabled in the SM and the status of rate adapt.

Beginning the Test of Point-to-Multipoint Links

To begin the test of links, perform the following steps:

1. In the Session Status tab of the AP, note the LUID associated with the MAC address of any SM you wish to involve in the test.
2. Click the Remote Subscribers tab.

Remote Subscribers Tab of the AP

An example of a Remote Subscribers tab is displayed in Figure 23.

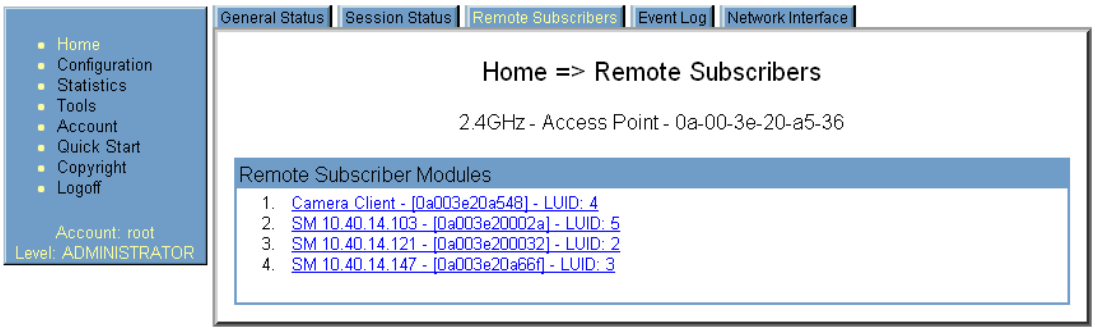


Figure 23: Remote Subscribers tab of AP, example

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.

General Status Tab of the SM

An example of the General Status tab of an SM is displayed in Figure 24.

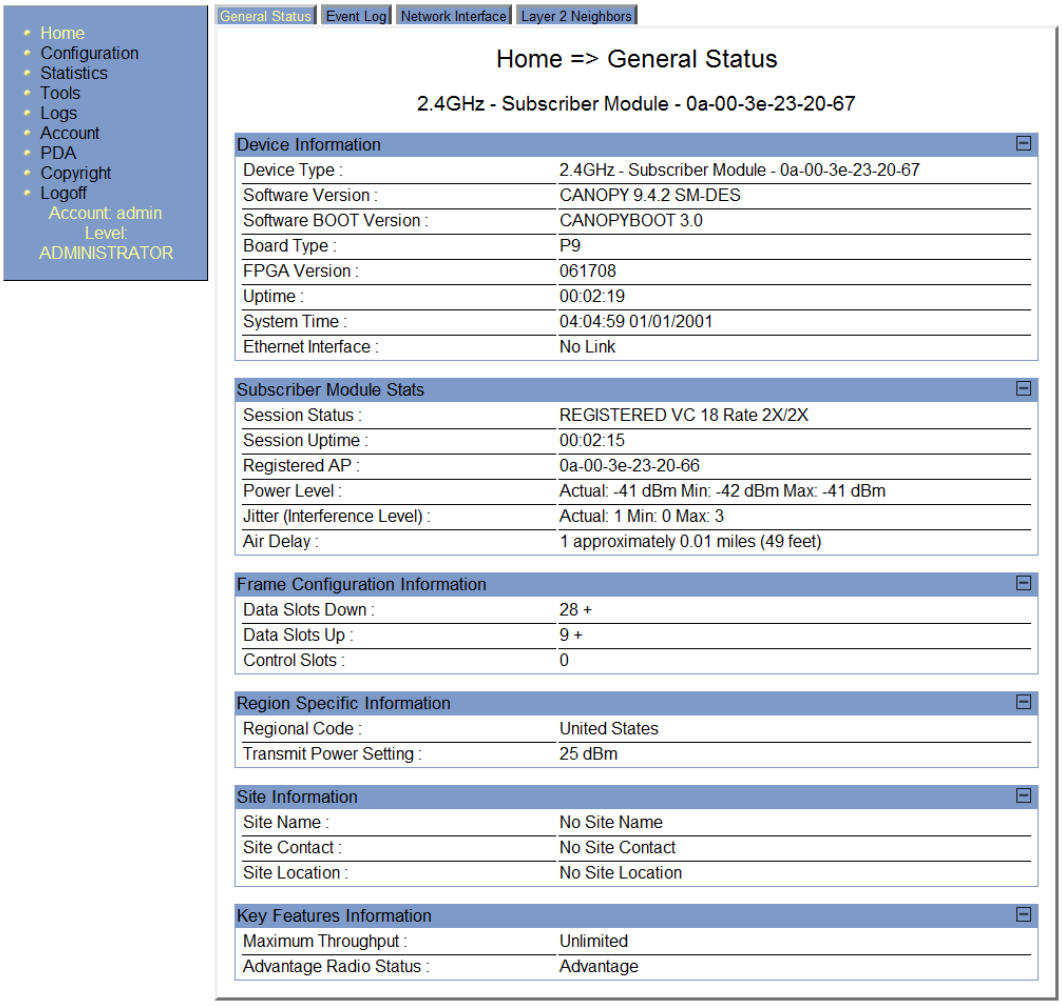


Figure 24: General Status tab of SM, example

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

Table 27 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.

Attribute	Meaning
Software BOOT Version	This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.
Board Type	This field indicates the series of hardware.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).
Ethernet Interface	This field indicates the speed and duplex state of the Ethernet interface to the SM.
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 and ready to transmit and receive data packets. • **Alignment** indicates that this SM is in an aiming mode.
Session Uptime	This field displays the duration of the current link. The syntax of the displayed time is *hh:mm:ss*.
Registered AP	This field displays the MAC address of the AP to which this SM is registered.

Attribute	Meaning
Power Level and Jitter	The General Status tab shows the received **Power Level** in dBm and **Jitter**. Proper alignment maximizes **Power Level** and minimizes **Jitter**. As you refine alignment, you should favor lower jitter over higher dBm. For example, if coarse alignment gives an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, use the refined alignment, with the following caveats: • When the receiving link is operating at 1X, the Jitter scale is 0 to 15 with desired jitter between 0 and 4. • When the receiving link is operating at 2X, the Jitter scale is 0 to 15 with desired jitter between 0 and 9. **NOTE** Unless the page is set to auto-refresh, the values displayed are from the instant the General Status tab was selected. To keep a current view of the values, refresh the browser screen or set to auto-refresh.
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.

Attribute	Meaning
Region Code	From the drop-down list, select the region in which the radio is operating. Selectable regions are: ◦ **Australia** ◦ **Brazil** ◦ **Canada** ◦ **Europe** ◦ **India** ◦ **Indonesia** ◦ **Russia** ◦ **Spain** ◦ **United States (locked)** ◦ **Other** When the appropriate region is selected in this parameter, the radio automatically implements the applicable required Dynamic Frequency Selection (DFS) standard. The SM radio automatically inherits the DFS type of the AP. This behavior ignores the value of the **Region Code** parameter in the SM, even when the value is **None**. Nevertheless, since future system software releases may read the value in order to configure some other region-sensitive feature(s), you should always set the value that corresponds to the local region. Unlike selections in other parameters, your **Region Code** selection requires a **Save Changes** and a **Reboot** cycle before it will force the context-sensitive GUI to display related options (for example, **Alternate Frequency Carrier *1 and 2*** in the Configuration => Radio tab). Thus, a proper configuration exercise in environments that are subject to DFS requirements has two imperative **Save Changes** and **Reboot** cycles: one after the **Region Code** is set, and a second after related options are set. PMP 450 equipment shipped to the United States is locked down with a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
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.

Attribute	Meaning
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.
Advantage Radio Status	This field reflects whether the SM is currently licensed for enhanced caps (Advantage, also known as Cap 2) on uplink and downlink traffic.

Continuing the Test of Point-to-Multipoint Links

To resume the test of links, perform the following steps.

1. Verify that the **Session Status** field of the General Status tab in the SM indicates **REGISTERED**.
2. While you view the General Status tab in the SM, note (or print) the values of the following fields:
   - Device type
   - Software Version
   - Software BOOT Version
   - Board Type
   - FPGA Version
3. Systematically ensure that you can retrieve this data (from a database, for example) when you later prepare to deploy the SM to subscriber premises.
4. Return to the Remote Subscribers tab of the AP.
5. Click the link of the next SM that you wish to test.
6. Repeat the test procedure from that point. When you have tested all of the SMs that you intend to test, return your browser to the General Status tab of the AP.

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

Figure 25 General Status tab of AP

Device Information	
Device Type :	5.7GHz MIMO OFDM - Access Point - 0a-00-3e-a0-01-75
Software Version :	CANOPY 12.0 (Build 111_512FFT) AP-DES
Board Type :	P12
Combo Radio Mode :	MIMO OFDM Only
FPGA Version :	060112
FPGA Type :	C200
PLD Version :	0
Uptime :	00:00:27
System Time :	02:07:37 01/01/2011 UTC
Last NTP Time Update :	00:00:00 00/00/0000 UTC
Ethernet Interface :	100Base-TX Full Duplex
Regulatory :	Passed
Antenna :	External (Connectorized)
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/4
Temperature :	34 °C / 92 °F

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

Frame Configuration Information	
Data Slots Down :	53
Data Slots Up :	18
Control Slots :	0

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

Key Features Information	
Time Updated and Location Code :	06/06/2012 19:09:59 - INTL

Table 28 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.
Software BOOT Version	This field indicates the version of the CANOPYBOOT file. If you request technical support, provide the information from this field.
Board Type	This field indicates the series of hardware.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.
FPGA Type	Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.
PLD Version	This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. If the AP is connected to a CMM, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.
Last NTP Time Update	This field displays when the AP last used time sent from an NTP server. If the AP has not been configured in the Time tab of the Configuration page to request time from an NTP server, then this field is populated by 00:00:00 00/00/00.
Ethernet Interface	This field indicates the speed and duplex state of the Ethernet interface to the AP.
Regulatory	This field indicates whether the configured **Region Code** and radio frequency are compliant with respect to their compatibility. PMP 450 equipment shipped to the United States is locked down with a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.

Attribute	Meaning
Antenna	The presence of this field depends on whether antenna options are available for the module. This field indicates the polarity of the antenna in the modules as one of the following: **Horizontal** **Vertical** **External (Connectorized)**
Registered SM Count	This field indicates how many SMs are registered to the AP.
GPS Sync Pulse Status	This field indicates the status of synchronization as follows: • **Generating sync** indicates that the module is set to *generate* the sync pulse. • **Receiving Sync** indicates that the module is set to *receive* a sync pulse from an outside source and is receiving the pulse. • **ERROR: No Sync Pulse** indicates that the module is set to *receive* a sync pulse from an outside source and is not receiving the pulse. NOTE When this message is displayed, the AP transmitter is turned off to avoid self-interference within the system.
Max Registered SM Count	This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.
Data Slots Down	This field indicates the number of frame slots that are designated for use by data 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) **Control Slots** configured by the operator. A + in this field (for example, 28+) indicates that there are additional bit times that the scheduler can take advantage of for internal system communication, but not enough for a full data slot.
Data Slots Up	This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data, and (reserved) Control Slots configured by the operator. A + in this field (for example, 9+) indicates that there are additional bit times that the scheduler can take advantage of for control slots (which are half the size of data slots), but not enough for a full data slot.
Control Slots	This field indicates the number of (reserved) control slots configured by the operator. Control slots are half the size of data slots. The SM uses reserved control slots and unused data slots for bandwidth requests.

Attribute	Meaning
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the *sysName* SNMP MIB-II object and can be polled by an SNMP management server.
Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.
Scheduling Type	This field indicates the type of frame scheduler that is active in the AP.
MP Double Rate	This field indicates whether 2X modulation rate is enabled for the sector.

Concluding the Test of Point-to-Multipoint Links

To conclude the test, perform the following steps.

Procedure 1 Verifying and recording information from the AP

1. Confirm that the **GPS Sync Pulse Status** field indicates **Generating Sync**.
   NOTE: This indication confirms that the AP is properly functional.
2. While your browser is directed to this General Status tab, note (or print) the values of the following fields:
   - Device type
   - Software Version
   - Software BOOT Version
   - Board Type
   - FPGA Version
3. Systematically ensure that you can retrieve this data (from a database, for example) when you later prepare to deploy the AP.

Preparing Components for Deployment

Your test of the modules not only verified that they are functional, but also yielded data that you have stored about them. Most efficiently preparing modules for deployment involves

- retrieving that data.
- systematically collecting the data into a single repository, while keeping a strong (quick) association between the data and the module.
- immediately merging module access data into this previously stored data.

Correlating Component-specific Information

You can use the data that you noted or printed from the Status pages of the modules to

- store modules for future deployment.
- know, at a glance, how well-stocked you are for upcoming network expansions.
- efficiently draw modules from stock for deployment.
- plan any software updates that you
  - wish to perform to acquire features.
  - need to perform to have the feature set be consistent among all modules in a network expansion.

You can make these tasks even easier by collecting this data into a sortable database.

Ensuring Continuing Access to the Modules

As you proceed through the steps of configuration, you will set values for parameters that specify the sync source, data handling characteristics, security measures, management authorities, and other variables for the modules. While setting these, you will also tighten access to the module, specifically in

- the **Color Code** parameter of Configuration page
- the **Display-Only Access** and **Full Access** password parameters of the Configuration page.
- the addressing parameters of the IP Configuration page.

Before you set these, consider whether and how you may want to set these by a self-devised scheme. A password scheme can help you when you have forgotten or misfiled a password. An IP addressing scheme may be essential to the operation of your network and to future expansions of your network.

As you set these, note the color code and note or print the parameters you set on the Configuration page tabs. Immediately associate them with the following previously stored data about the modules:

- device type, frequency band, and MAC address
- software version and encryption type
- software boot version
- FPGA version

Utilizing the Installation Color Code feature

With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. SMs with Installation Color Code enabled will first try any configured Color Code values first, then will use the Installation Color Code feature as a last result to connect to the AP. The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message "SM is registered via ICC – Bridging Disabled!" is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the **Rescan APs** functionality on the AP Eval page).

See below for an example of how the SM displays AP registration information when registered via primary Color Code – configured to a value of 210 for this case. Note that even though Installation Color Code is enabled on the AP and SM, since the Primary Color Code of 210 matches, the SM registers to the AP using this value.

Figure 26 AP configuration - Color Code 210 and Installation Color Code enabled

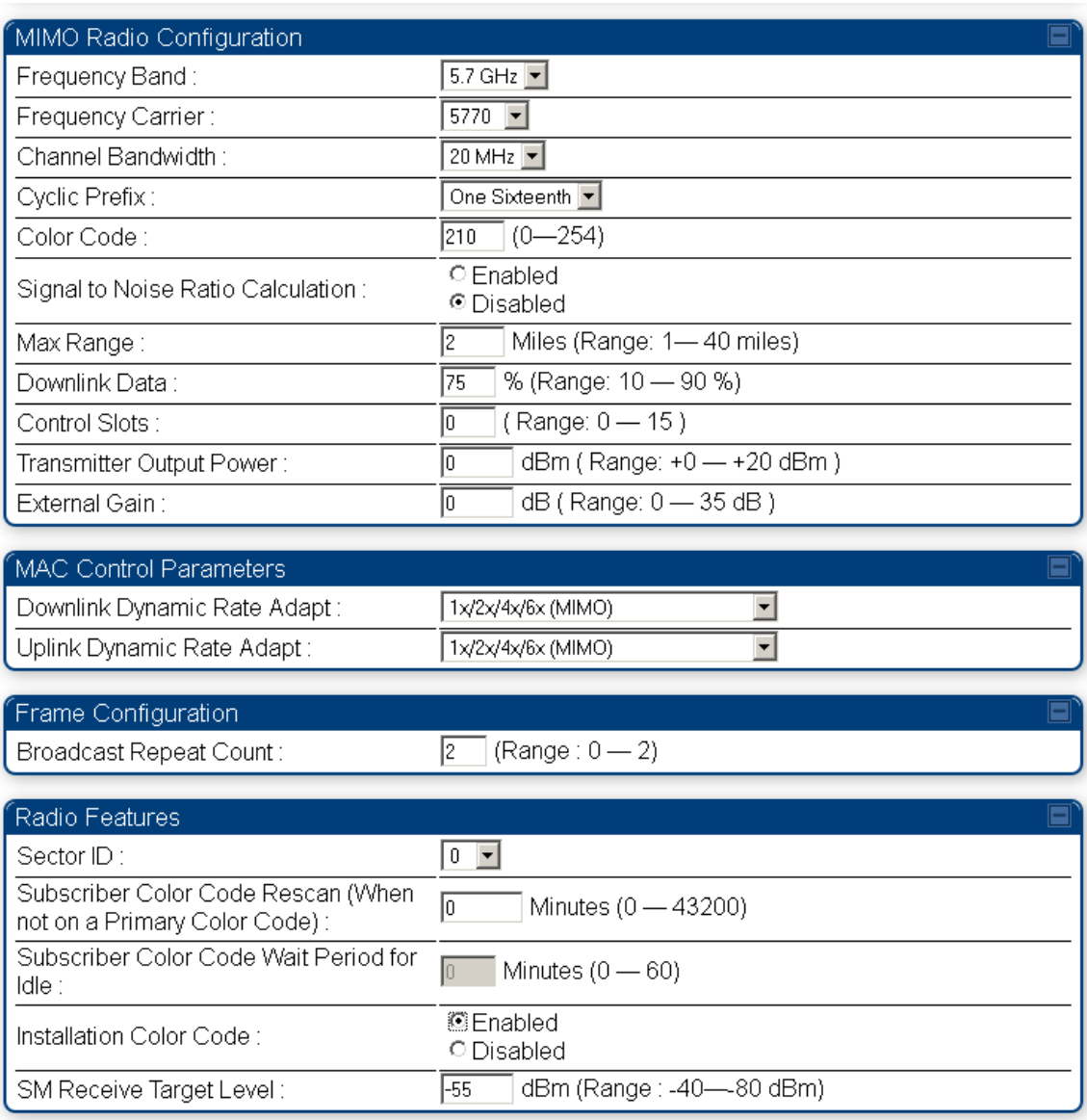


Figure 27 SM Configuration - Color Code 210 and Installation Color Code enabled

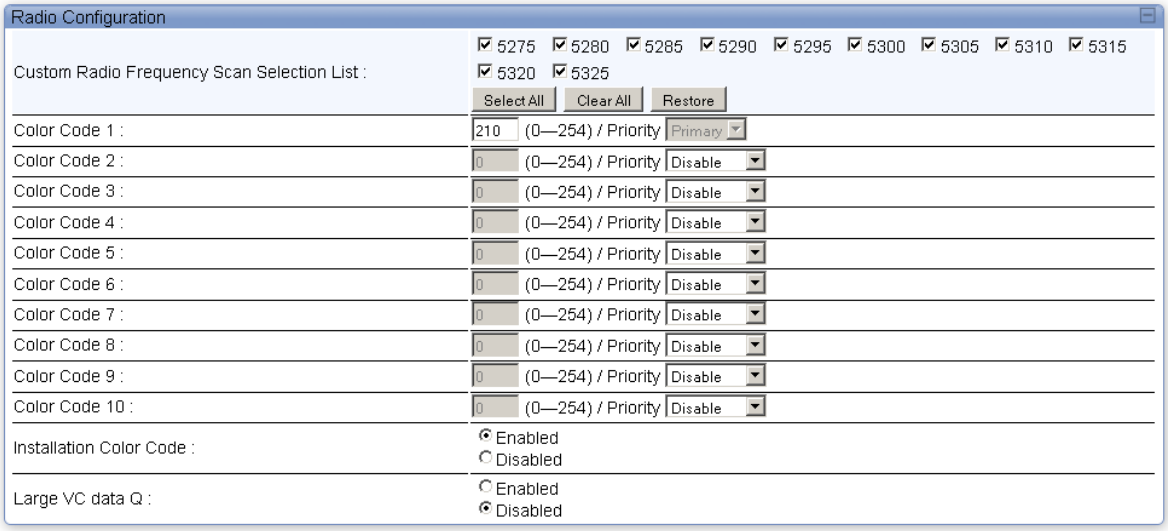


Figure 28 AP Eval Page - SM registered using Primary Color Code 210

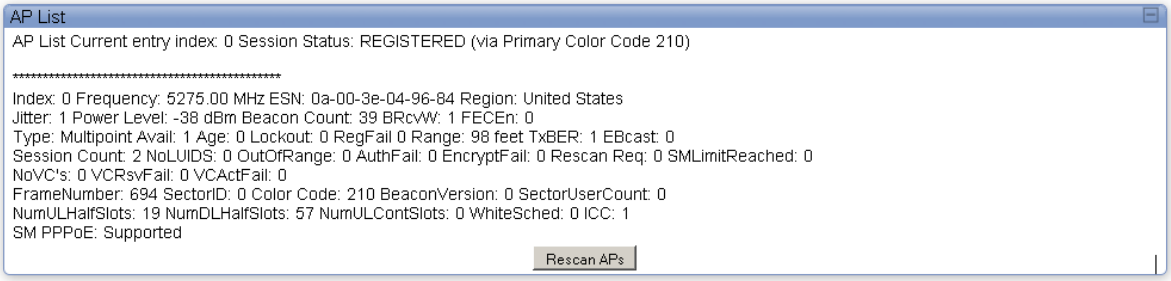
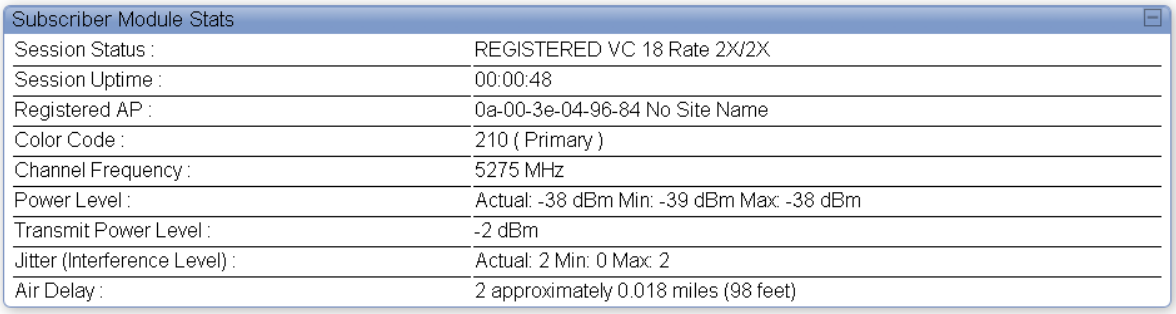


Figure 29 SM Main Status - SM registered using primary Color Code 210



See below for an example of how the SM displays registration information when registered via Installation Color Code. In this case the AP is configured with a Color Code value of 1 and Installation Color Code is enabled, and the SM is configured with a Color Code value of 210 and Installation Color Code is enabled. Since the Color Codes do not match between the AP and SM, the SM registers to the AP via the Installation Color Code feature. Note that when this connection is established, no user data is bridged between the AP and SM.

Figure 30 AP Configuration - Color Code 1 and Installation Color Code enabled

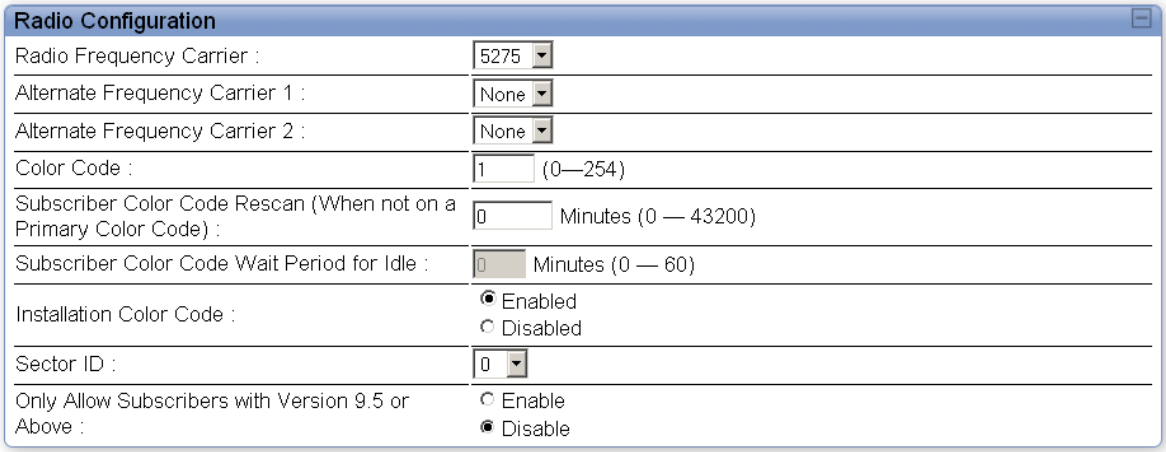


Figure 31 SM Configuration - Color Code 210 and Installation Color Code enabled

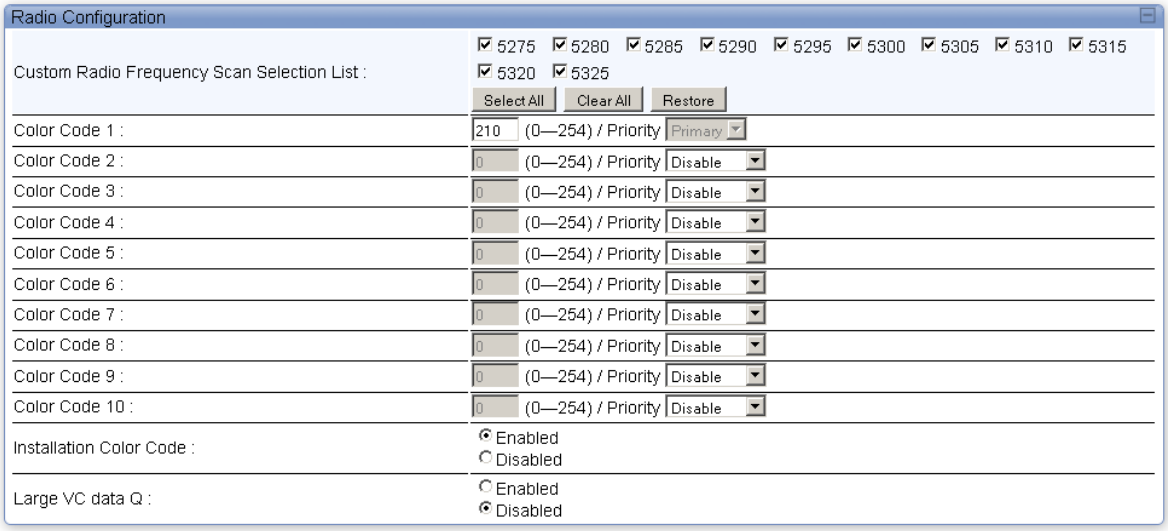


Figure 32 AP Eval - SM registered using Installation Color Code

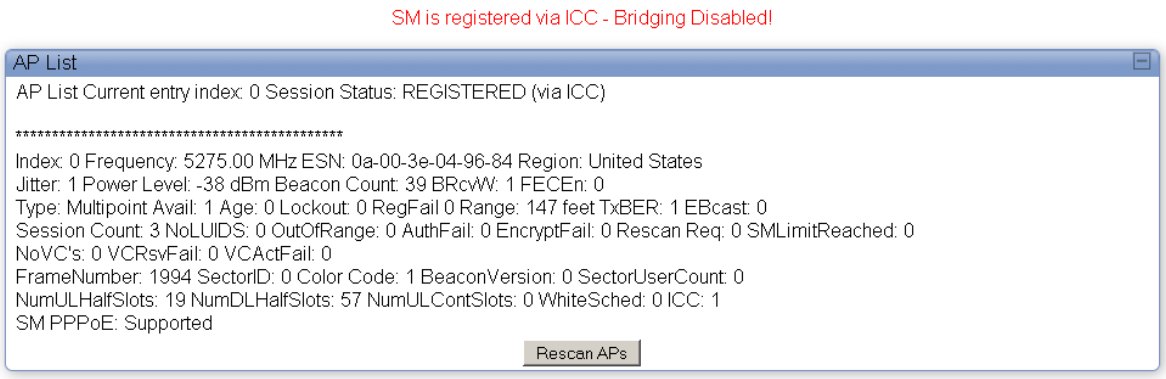
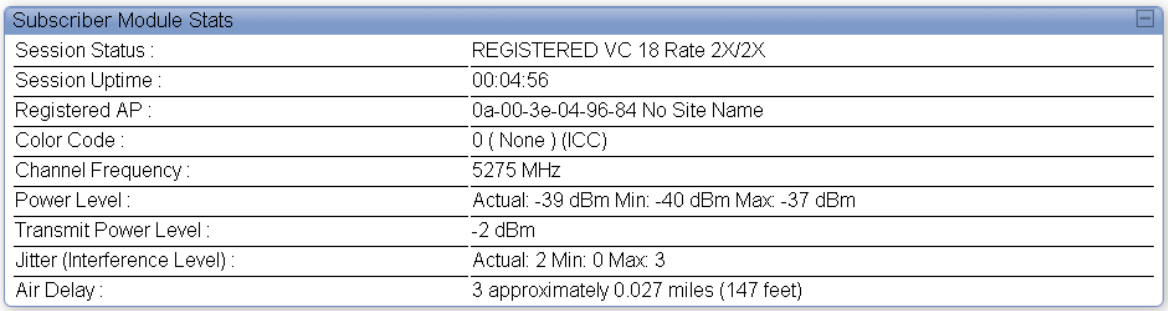


Figure 33 SM Main Status Page - SM registered using Installation Color Code



Subscriber Module Stats	
Session Status :	REGISTERED VC 18 Rate 2X/2X
Session Uptime :	00:04:56
Registered AP :	0a-00-3e-04-96-84 No Site Name
Color Code :	0 (None) (ICC)
Channel Frequency :	5275 MHz
Power Level :	Actual: -39 dBm Min: -40 dBm Max: -37 dBm
Transmit Power Level :	-2 dBm
Jitter (Interference Level) :	Actual: 2 Min: 0 Max: 3
Air Delay :	3 approximately 0.027 miles (147 feet)

Chapter 4: Installing Components

NOTE

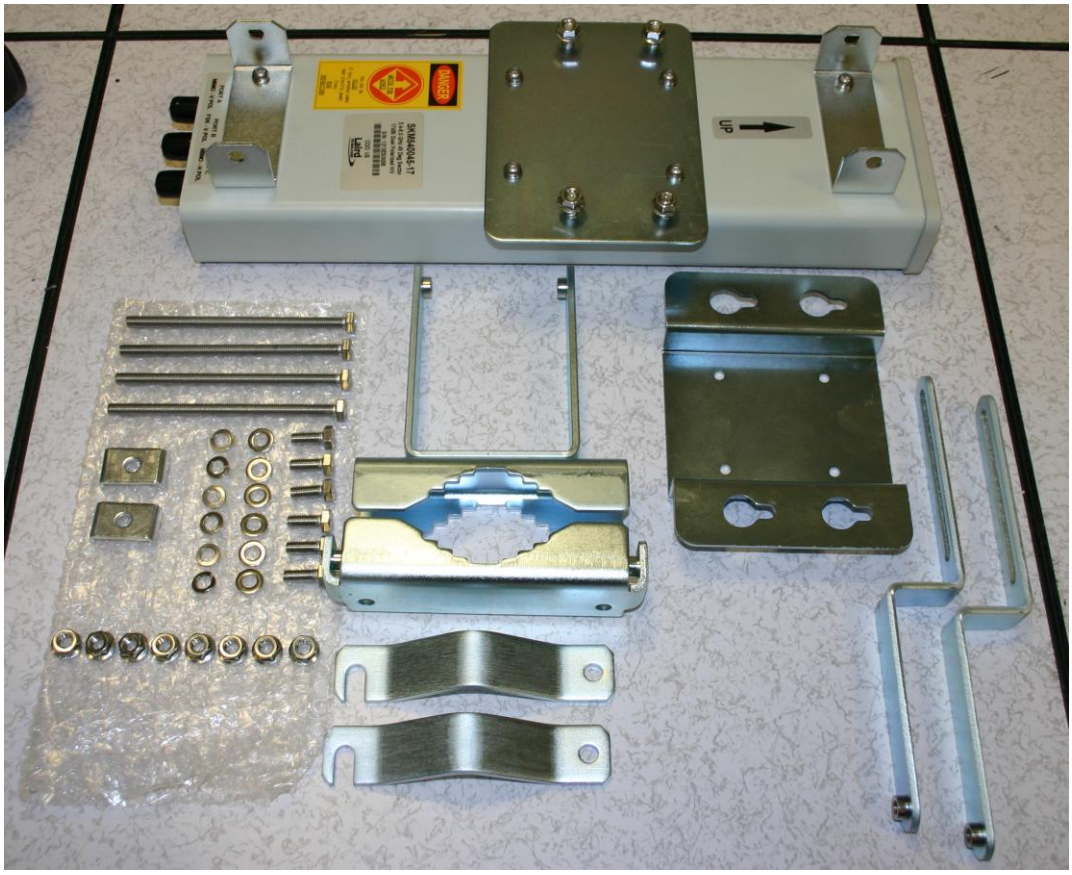
Use *shielded* cable for all infrastructure connections associated with APs, SMs, and CMMs. The environment that these modules operate in often has significant unknown or varying RF energy. Operator experience consistently indicates that the additional cost of shielded cables is more than compensated by predictable operation and reduced costs for troubleshooting and support.

Assembling the AP antenna

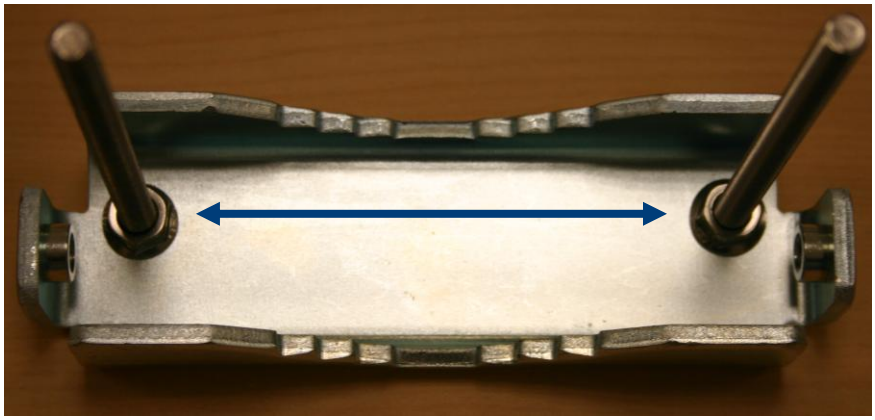
To install a PMP 450 Series AP, perform the following steps.

Procedure 2 Installing a PMP 450 AP

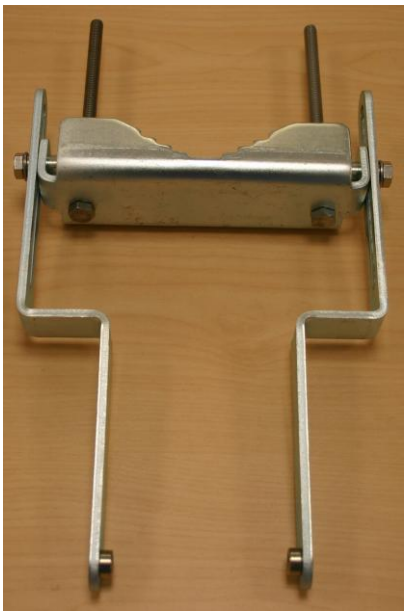
1 Inventory the parts to ensure that you have them all before you begin. The full set of parts is shown below.



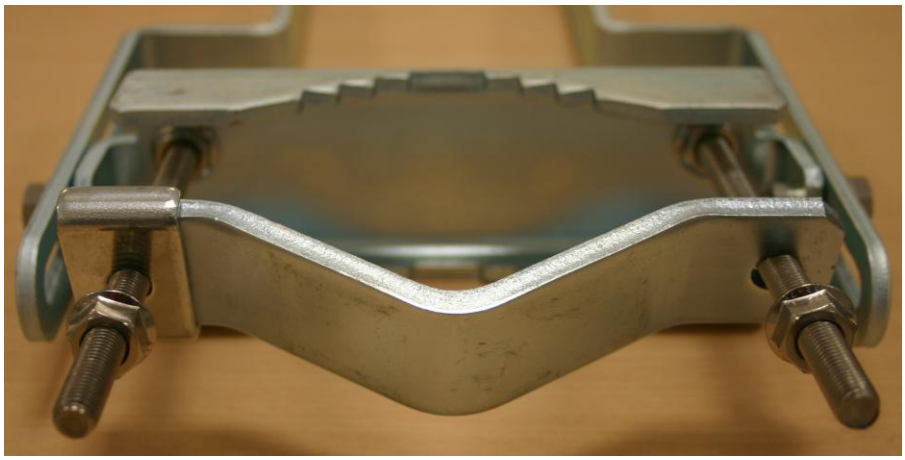
2 Begin assembling the upper bracket by attaching the (2) 7" hex bolts to the bracket using (2) serrated flange nuts



3 Attach the upper bracket to the adjustment arms using (2) hex bolts, (2) flat washers and (2) lock washers

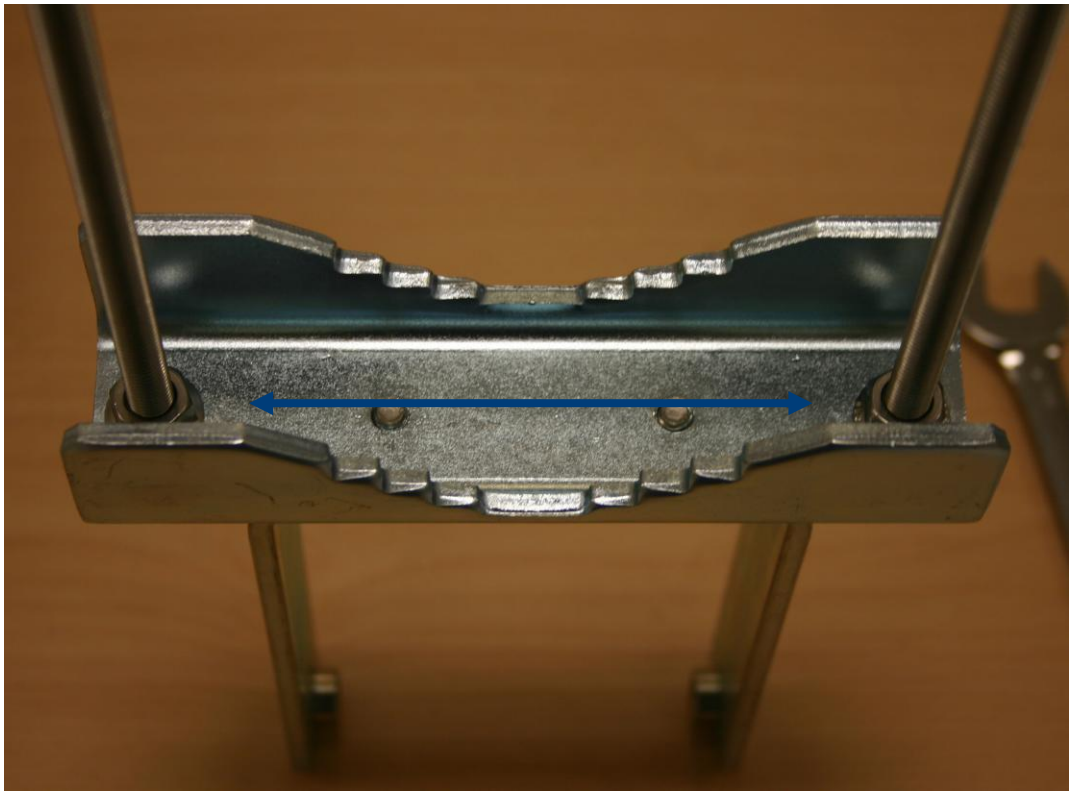


4 Attach the rear strap to the bracket using (2) serrated flange nuts and (1) retaining bracket. Do not tighten the nuts now.



5 Attach the entire upper bracket to the antenna using (2) hex bolts, (2) flat washers and (2) lock washers

6 Begin assembling the upper bracket by attaching the (2) 7" hex bolts to the bracket using (2) serrated flange nuts



7 Attach the rear strap to the bracket using (2) serrated flange nuts and (1) retaining bracket. Do not tighten the nuts now.

8 Attach the entire lower bracket to the antenna using (2) hex bolts, (2) flat washers and (2) lock washers

Attaching the AP to the antenna

To attach a PMP 450 Series AP to the antenna, perform the following steps.

Procedure 3 Attaching the AP to the sector antenna

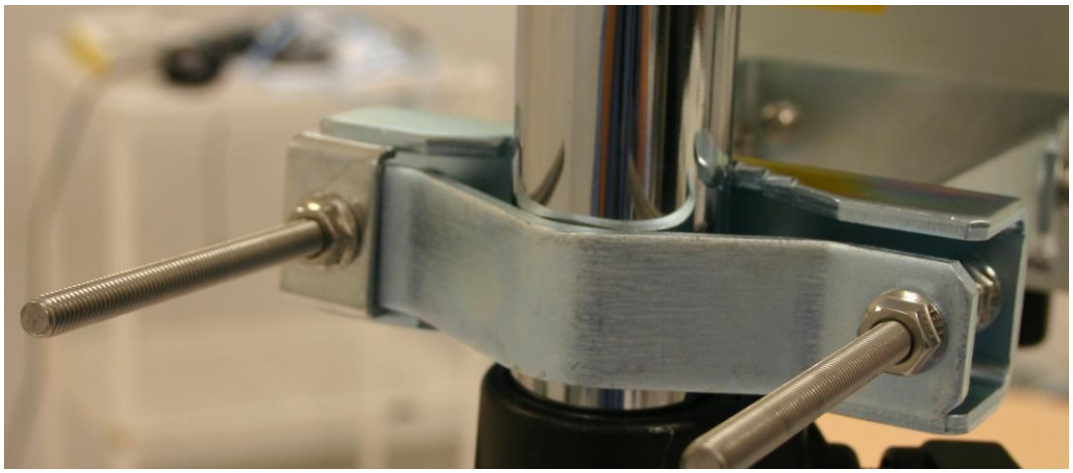
1 Attach the included bracket to the rear of the AP, then attach the AP to the antenna by sliding the bracket onto the bolts and tighten the (4) serrated flange nuts

Attaching the AP and antenna to the mount point

Procedure 4 Attaching the AP to the sector antenna

1 Attach the upper bracket of the antenna to the mount point by closing the rear strap around the pole and tightening the (2) serrated flange nuts. These must be tightened evenly on the pol to avoid jumping/stripping threads.

2 Attach the lower bracket of the antenna to the mount point by closing the rear strap around the pole and tightening the (2) serrated flange nuts. These must be tightened evenly on the pole to avoid jumping/stripping threads.



3 Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the 90° sector.

4 Ensure that the nearest and furthest SMs that must register to this AP are within the 3-dB beam pattern of 60° azimuth by 5° elevation with near-in null fill coverage.

5. Choose the best mounting location for your particular application.
   NOTE: Use the embedded spectrum analyzer or a commercial analyzer to evaluate the frequencies present in various locations. OFDM APs need not be mounted next to each other. They can be distributed throughout a given site. However, the 90° offset must be maintained. If you want to collocate these APs with PMP 100 Series APs of the 5.4-GHz frequency band range, plan to allow at least 25 MHz of separation between their center channels.
6. Secure a ground strap to the ground lug on the back of the AP.
7. Secure the ground strap to the pole, tower, or other trusted ground.
8. Adjust the initial down tilt of the AP/antenna assembly to 5°, −3 dB beam elevation, with near-in null fill.
9. Connect the coax cables to the antenna
10. Weather-seal the connector on the coax cables

Connecting an RJ45 and gland to a unit

Perform this task to connect the Ethernet cable to an AP.

To connect the Ethernet cable with a gland to an AP unit, proceed as follows:

Procedure 5 Connecting the Ethernet cable and gland to the AP

1. Insert the RJ45 cable through the gland components as shown:

2. Insert the RJ45 plug into the socket in the unit, making sure that the locking tab snaps home.

3 Support the drop cable and gently hand screw the gland body into the unit until the O ring seal is flush to the unit body.

NOTE

Do not fit the back shell prior to securing the gland body.

4 Once the gland is fully hand screwed into the unit, tighten it one full rotation only with a 1 1/8 inch spanner wrench.

5 When the gland body has been fitted, tighten the gland back shell.

CAUTION

Do not over-tighten the gland back shell, as the internal seal and structure may be damaged.

Disconnecting an RJ45 and gland from a unit

Perform this task to disconnect the Ethernet cable from an AP.

To disconnect the Ethernet cable with a gland from a unit, proceed as follows:

Procedure 6 Disconnecting an RJ45 and gland from a unit

1. Remove the gland back shell.
2. Unscrew the gland body.
3. Use a small screwdriver to depress the RJ45 locking clip
4. Unplug the RJ45.

Installing a GPS Antenna

For instructions on GPS antenna installation, see the user guide that is dedicated to the CMM product.

Installing a Cluster Management Module

For instructions on CMM2 (Cluster Management Module 2), CMM3 (CMMmicro), or CMM4 installation, including the outdoor temperature range in which it is acceptable to install the unit, tools required, mounting and cabling instructions, and connectivity verification, see the user guide that is dedicated to that particular product.

Installing an SM

Installing a PMP 450 Series SM consists of two procedures:

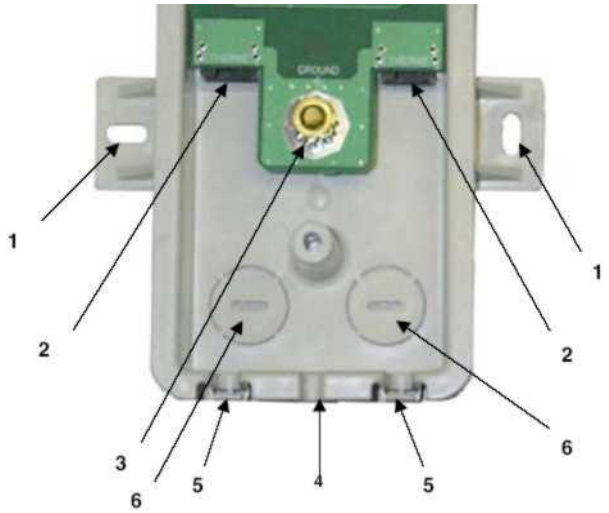
- Physically installing the SM on a residence or other location and performing a course alignment using the alignment tone.
- Verifying the AP to SM link and finalizing alignment using review of power level, link tests, and review of registration and session counts.

Procedure 7 Installing the PMP 450 SM

1. Choose the best mounting location for the SM based on section Installation planning.
2. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.
3. Remove the base cover of the SM.
4. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the SM.
5. Wrap a drip loop in the cable.
6. Optionally, attach the SM to the arm of the Passive Reflector dish assembly or snap a LENS onto the SM.

7 Remove the cover of the 600SS Surge Suppressor. The inside of the surge suppressor is shown in Figure 34.

Figure 34 600SS Surge Suppressor - Inside



KEY TO CALLOUTS

Table 29 Key to Callouts - 600SSD

1 Holes—for mounting the Surge Suppressor to a flat surface (such as an outside wall). The distance between centers is 4.25 inches (108 mm).

2 RJ-45 connectors—One side (neither side is better than the other for this purpose) connects to the product (AP, SM, or cluster management module). The other connects to the AC adaptor's Ethernet connector.

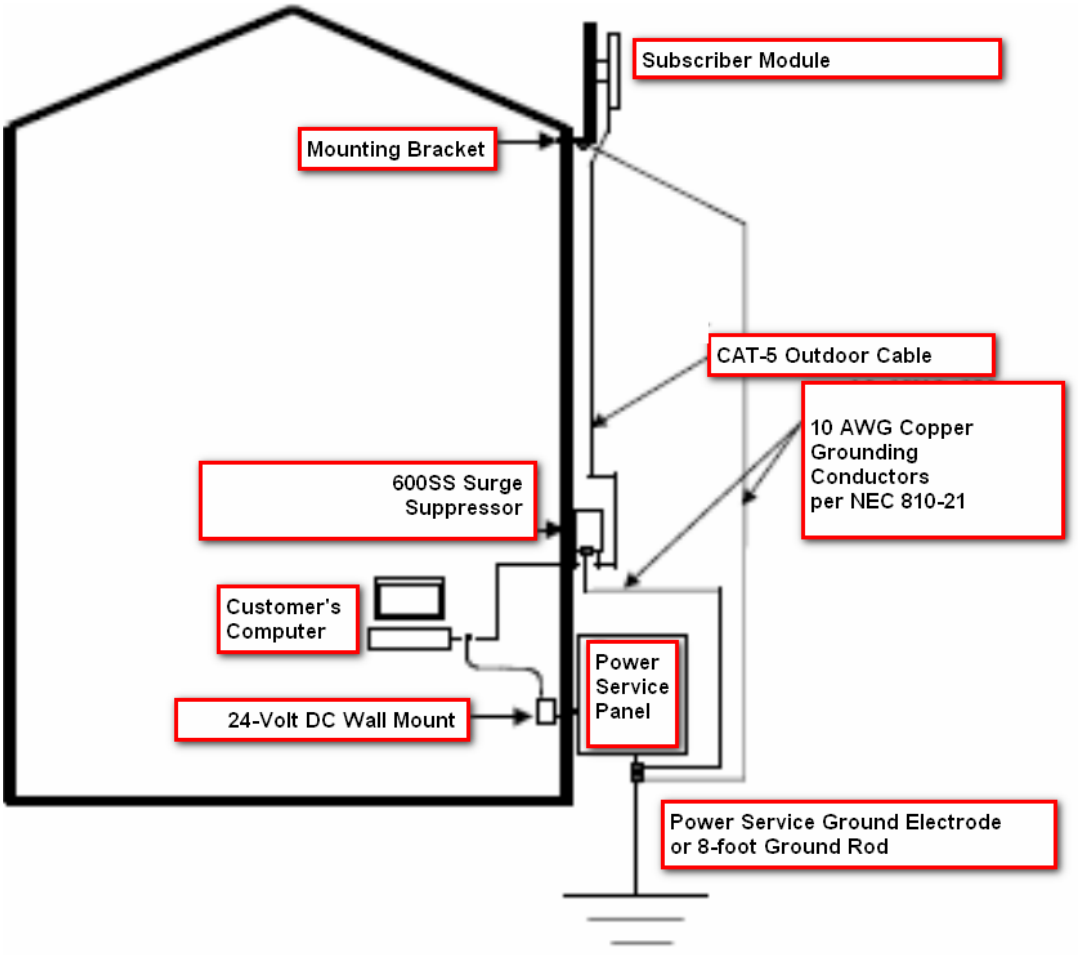
3 Ground post—use heavy gauge (10 AWG or 6 mm^2) copper wire for connection. Refer to local electrical codes for exact specifications.

4 Ground Cable Opening—route the 10 AWG (6 mm^2) ground cable through this opening.

5 CAT-5 Cable Knockouts—route the two CAT-5 cables through these openings, or alternatively through the Conduit Knockouts.

6 Conduit Knockouts—on the back of the case, near the bottom. Available for installations where cable is routed through building conduit.

8 With the cable openings facing downward, mount the 600SS to the *outside* of the subscriber premises, as close to the point where the Ethernet cable penetrates the residence or building as possible, and as close to the grounding system (Protective Earth) as possible.



9 Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 600SS.

10 Tighten the Ground post locking nut in the 600SS onto the copper wire.

11 Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.

12 Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.

13 Pack both of the surge suppressor Ethernet jacks with dielectric grease.

14 Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 600SS.

15 Tighten the Ground post locking nut in the 600SS onto the copper wire.

16 Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.

17 Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 600SS.

18 Pack both of the surge suppressor Ethernet jacks with dielectric grease.

19 Wrap a splice loop in the loose end of the Ethernet cable from the SM.

20 Connect that cable to one of the Ethernet jacks.

21 Connect an Ethernet cable to the other Ethernet jack of the 600SS and to the power adapter.

22 Replace the cover of the 600SS.

23 Connect the power supply to a power source.

24 Connect the Ethernet output from the power supply to the Ethernet port of your laptop.

25 Climb your ladder to the SM.

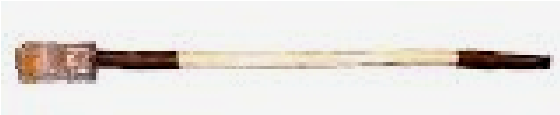
26 Launch your web browser.

27 In the URL address bar, enter **169.254.1.1**.

28 If the browser in your laptop fails to access the interface of the SM, perform the following steps:

Insert your override plug into the RJ11 GPS utility port of the SM.

Figure 35 Default plug



Remove and reinsert the RJ45 Ethernet cable connector at the SM.
NOTE: This triggers a power cycle, which causes the SM to reboot.

Wait for the reboot to conclude (about 30 seconds).

When the reboot is finished, remove the override plug.

In the left-side menu of the SM interface, click **Login**.

Consistent with local operator policy, reset both the `admin` and the `root` user passwords.

In the left-side menu, click **Configuration**.

Click the IP tab.

Consistent with local operator practices, set an

- IP Address
- Subnet Mask
- Gateway IP Address
- Click the Save Changes button.
- Click the Reboot button.

29 Log in as either `admin` or `root` on the SM.

30 Configure a password for the `admin` account and a password for the `root` account.

31 Log off of the SM.

32 Log back into the SM as `admin` or `root`, using the password that you configured

34 For coarse alignment of the SM, use the Audible Alignment Tone feature as follows:

In the left-side menu of the SM interface, click **Configuration**.

Click the General tab.

Set the **2X Rate** parameter in the SM to **Disabled**.

Connect the RJ-11 6-pin connector of the Alignment Tool Headset to the RJ-11 utility port of the SM.

Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.

Listen to the alignment tone for

- pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
- volume, which indicates better signal quality (lower jitter) by higher volume.

Figure 36 Audible Alignment Tone kit, including headset and connecting cable

Adjust the module slightly until you hear the highest pitch and highest volume.

In the General tab of the Configuration web page of the SM, set the **2X Rate** parameter back to **Enable**.

35 When you have achieved the best signal (highest pitch, loudest volume), lock the SM in place with the mounting hardware.

36 Log off of the SM.

37 Disconnect the Ethernet cable from your laptop.

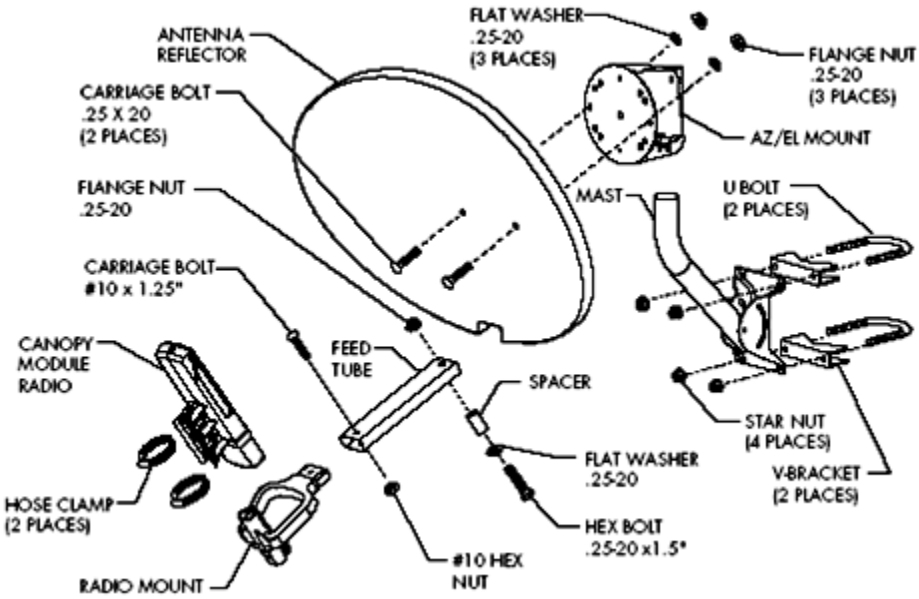
38 Replace the base cover of the SM.

39 Connect the Ethernet cable to the computer that the subscriber will be using.

Installing an SM reflector dish

The internal patch antenna of the module illuminates the Passive Reflector Dish from an offset position. The module support tube provides the proper angle for this offset.

Figure 37 Reflector dish assembly, exploded view



Both modules mounted at same elevation

For cases where the other module in the link is mounted at the same elevation, fasten the *mounting hardware leg* of the support tube vertical for each module. When the hardware leg is in this position

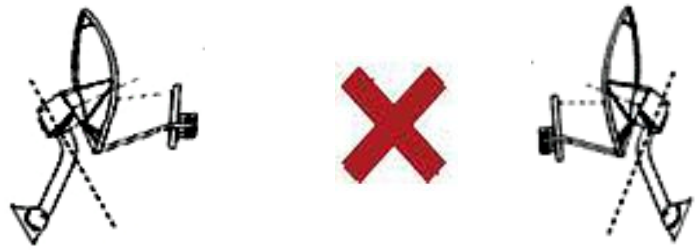
- the reflector dish has an obvious downward tilt.
- the *module leg* of the support tube *is not* vertical.

For a mount to a non-vertical structure such as a tapered tower, use a plumb line to ensure that the hardware leg is vertical when fastened. Proper dish, tube, and module positions for a link in this case are illustrated in Figure 38. The dish is tipped forward, not vertical, but the focus of the signal is horizontal.

Figure 38 Correct SM angle mounting with reflector dish

Improper dish, tube, and module positions for this case are illustrated in Figure 39.

Figure 39 Incorrect SM angle mounting with reflector dish



Modules Mounted at Different Elevations

For cases where the other module in the link is mounted at a different elevation, the assembly hardware allows tilt adjustment. The proper angle of tilt can be calculated as a factor of both the difference in elevation and the distance that the link spans. Even in this case, a plumb line and a protractor can be helpful to ensure the proper tilt. This tilt is typically minimal.

The number of degrees to offset (from vertical) the mounting hardware leg of the support tube is equal to the angle of elevation from the lower module to the higher module (b in the example provided in section "Calculating the Aim Angles" of the *PMP 450 Planning Guide*).

Configuring an AP-SM Link

To initially configure the AP-SM over-the-air link after the SM has been installed, perform the following steps.

Procedure 8 Configuring the AP-SM link

1. Using a computer (laptop, desktop, portable device) connected to the SM, open a browser and access the SM using the default IP address of http://169.254.1.1 (or the IP address configured in the SM, if one has been configured.)
2. In the left-side menu, select **Configuration**.
3. Click the General tab.
5. In the left-side menu, select **Tools**.
6. Click the AP Evaluation tab.

7 Among the listed APs (each shown with a unique Index number), find the AP whose **Power Level** value is highest (or find the ESN of the AP to which you were instructed to establish a link).

8 Write down the **Frequency** and **Color Code** values of the AP in the link.

9 In the left-side menu of the SM interface, select **Configuration**.

10 Click the Radio tab.

11 At the **Custom Radio Frequency Scan Selection List** parameter, uncheck all frequencies except the one on which the AP in the link is broadcasting.

12 At the **Color Code** parameter, enter the code number that was shown for that AP in the AP Evaluation tab.

13 Click the **Save Changes** button.

14 Click the **Reboot** button.

15 Fine-adjust the SM mounting, if needed, to improve **Power Level** according to your company standards.

16 Retighten the hardware that secures the mounting.

17 In the left-side menu, select **Tools**.

18 Click the Link Capacity Test tab..

- Perform several link tests of 10-second duration as follows:
- Type into the **Duration** field how long (in seconds) the RF link should be tested.
- Leave the **Packet Length** field (when present) set to the default of 1522 bytes or type into that field the packet length at which you want the test conducted.
- Leave the **Number of Packets** field set to 0 (to flood the link).
- Click the **Start Test** button.
- View the results of the test.

19 If these link tests fail to consistently show 90% or greater efficiency in 1X operation or 50 to 60% efficiency in 2X, troubleshoot the link, using the data as follows:

- If the downlink is consistently 90% efficient, but the uplink is only 40%, this indicates trouble for the SM transmitting to the AP. Have link tests performed for nearby SMs. If their results are similar, investigate a possible source of interference local at the AP.
- If the uplink is consistently 90% efficient, but the downlink is only 40%, this indicates trouble for the AP transmitting to the SM. Investigate a possible source of interference near the SM.
- If these link tests consistently show 90% or greater efficiency in 1X operation, or 50 to 60% efficiency in 2X operation, in both uplink and downlink, continue this procedure.

20 In the left-side menu, select **Configuration**.

21 In the General tab, set the **2X Rate** parameter to **Enabled**.

22 Click the **Save Changes** button.

23 If an element management system such as Wireless Manager will be used to manage the SM via SNMP, perform the following steps:

- Click the SNMP tab.
- At the **Read Permissions** parameter, select **Read/Write**.
- Under **Site Information**, type complete data into the three parameters: **Site Name**, **Site Contact**, **Site Location**.
- Click the **Save Changes** button.

24 Click the **Reboot** button.

Monitoring an AP-SM Link

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

Procedure 9 Monitoring the AP-SM link for performance

1 Access the interface of the AP.

2 In the left-side menu of the AP interface, select **Home**.

3 Click the Session Status tab.

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

   If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link.

Appendix A: Glossary

Term	Definition
~.	The command that terminates an SSH Secure Shell session to another server. Used on the Bandwidth and Authentication Manager (BAM) master server in the database replication setup.
10Base-T	Technology in Ethernet communications that can deliver 10 Mb of data across 328 feet (100 meters) of CAT 5 cable.
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.
169.254.x.x	IP address default in Microsoft and Apple operating systems without a DHCP (Dynamic Host Configuration Protocol) server.
255.255.0.0	Subnet mask default in 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 1,200 or fewer subscribers. Each Access Point Module covers a 60° sector. This cluster covers as much as 360°. Also known as AP cluster.
Access Point Module	Also known as AP. One module that distributes network or Internet services in a 60° sector to 200 subscribers or fewer.
ACT/4	Second-from-left LED in the module. In the operating mode, this LED is lit when data activity is present on the Ethernet link. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Activate	To provide feature capability to a module, but not to *enable* (turn on) the feature in the module. See also Enable.

Term	Definition
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 200 subscribers or fewer.
APs MIB	Management Information Base file that defines objects that are specific to the Access Point Module or Backhaul timing master. See also Management Information Base.
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
ASN.1	Abstract Syntax Notation One language. The format of the text files that compose the Management Information Base.
Attenuation	Reduction of signal strength caused by the travel from the transmitter to the receiver, and caused by any object between. In the absence of objects between, a signal that has a short wavelength experiences a high degree of attenuation nevertheless.
BER	Bit Error Rate. The ratio of incorrect data received to correct data received.
Bit Error Rate	Ratio of incorrect data received to correct data received.
Box MIB	Management Information Base file that defines module-level objects. See also Management Information Base.
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
Bridge Entry Timeout Field	Value that the operator sets as the maximum interval for no activity with another module, whose MAC address is the Bridge Entry. This interval should be longer than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.
Buckets	Theoretical data repositories that can be filled at preset rates or emptied when preset conditions are experienced, such as when data is transferred.
Burst	Preset amount limit of data that may be continuously transferred.
C/I Ratio	Ratio of intended signal (carrier) to unintended signal (interference) received.

Term	Definition
Canopy	A trademark of Cambium, Inc.
Carrier-to-interference Ratio	Ratio of intended reception to unintended reception.
CarSenseLost Field	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
CAT 5 Cable	Cable that delivers Ethernet communications from module to module. Later modules auto-sense whether this cable is wired in a straight-through or crossover scheme.
chkconfig	A command that the Linux® operating system accepts to enable MySQL® and Apache™ Server software for various run levels of the mysqld and httpd utilities.
CIR	See Committed Information Rate.
Cluster Management Module	Module that provides power, GPS timing, and networking connections for an AP cluster. Also known as CMM. If this CMM is connected to a Backhaul Module, then this CMM is the central point of connectivity for the entire site.
CMM	Cluster Management Module. A module that provides power, GPS timing, and networking connections for an Access Point cluster.
CodePoint	See DiffServ.
Color Code Field	Module parameter that identifies the other modules with which communication is allowed. The range of values is 0 to 255. When set at 0, the Color Code does not restrict communications with any other module.
Committed Information Rate (CIR)	For an SM or specified group of SMs, a level of bandwidth that can be guaranteed to never fall below a specified minimum. In the 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.
Community String Field	Control string that allows a network management station to access MIB information about the module.
CPE	Customer premises equipment.
CRCError Field	This field displays how many CRC errors occurred on the Ethernet controller.
CRM	Customer relationship management system.
Data Encryption Standard	Over-the-air link option that uses secret 56-bit keys and 8 parity bits. Data Encryption Standard (DES) performs a series of bit permutations, substitutions, and recombination operations on blocks of data.

Term	Definition
Date of Last Transaction	A field in the data that the `cmd show esn` command generates from data in the SQL database in the Bandwidth and Authentication Manager (BAM) server. This field identifies the date of the most recent authentication attempt by the SM. Expressed in the database output as DLT.
Dell	A trademark of Dell, Inc.
Demilitarized Zone	Internet Protocol area outside of a firewall. Defined in RFC 2647. See http://www.faqs.org/rfcs/rfc2647.html.
DES	Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
Desensed	Received an undesired signal that was strong enough to make the module insensitive to the desired signal.
DFS	See Dynamic Frequency Selection.
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system. See http://www.faqs.org/rfcs/rfc2131.html. See also Static IP Address Assignment.
Diffraction	Partial obstruction of a signal. Typically diffraction attenuates a signal so much that the link is unacceptable. However, in some instances where the obstruction is very close to the receiver, the link may be acceptable.
DiffServ	Differentiated Services, consistent with RFC 2474. A byte in the type of service (TOS) field of packets whose values correlates to the channel on which the packet should be sent. The value is a numeric code point. Cambium modules map each of 64 code points to values of 0 through 7. Three of these code points have fixed values, and the remaining 61 are settable. Values of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities. (However, configuring DiffServ does not automatically enable the VLAN feature.) Among the settable parameters, the values are set in the AP for all downlinks within the sector and in the SM for each uplink.
Disable	To turn off a feature in the module after both the feature activation file has *activated* the module to use the feature and the operator has *enabled* the feature in the module. See also Activate and Enable.
DMZ	Demilitarized Zone as defined in RFC 2647. An Internet Protocol area outside of a firewall. See http://www.faqs.org/rfcs/rfc2647.html.

Term	Definition
Dynamic Frequency Selection (DFS)	A requirement in certain countries and regions for systems to detect interference from other systems, notably radar systems, and to avoid co-channel operation with these systems. See also Region Code.
Dynamic Host Configuration Protocol	See DHCP.
Electronic Serial Number	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number. Same as MAC Address.
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.
ESN Data Table	Table in which each row identifies data about a single SM. In tab-separated fields, each row stores the ESN, authentication key, and QoS information that apply to the SM. The operator can create and modify this table. This table is both an input to and an output from the Bandwidth and Authentication Manager (BAM) SQL database, and should be identically input to redundant BAM servers.
/etc/services	File that stores telnet ports on the Bandwidth and Authentication Manager (BAM) server.
EthBusErr Field	This field displays how many Ethernet bus errors occurred on the Ethernet controller.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
Fade Margin	The difference between strength of the received signal and the strength that the receiver requires for maintaining a reliable link. A higher fade margin is characteristic of a more reliable link. Standard operating margin.
FCC	Federal Communications Commission of the U.S.A.
Feature Activation Key	Software key file whose file name includes the ESN of the target module. When installed on the module, this file *activates* the module to have the feature *enabled* or disabled in a separate operator action.
Field-programmable Gate Array	Array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.

Term	Definition
File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See http://www.faqs.org/rfcs/rfc959.html.
FPGA	Field-programmable Gate Array. An array of logic, relational data, and wiring data that is factory programmed and can be reprogrammed.
Frame Spreading	Transmission of a beacon in only frames where the receiver expects a beacon (rather than in every frame). This avoids interference from transmissions that are not intended for the receiver.
Frame Timing Pulse Gated Field	Toggle parameter that prevents or allows the module to continue to propagate GPS sync timing when the module no longer receives the timing.
Free Space Path Loss	Signal attenuation that is naturally caused by atmospheric conditions and by the distance between the antenna and the receiver.
Fresnel Zone	Space in which no object should exist that can attenuate, diffract, or reflect a transmitted signal before the signal reaches the target receiver.
FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See http://www.faqs.org/rfcs/rfc959.html.
Global Positioning System	Network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
GPS/3	Third-from-left LED in the module. In the operating mode for an Access Point Module or Backhaul timing master, this LED is continuously lit as the module receives sync pulse. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
GUI	Graphical user interface.
High-priority Channel	Channel that supports low-latency traffic (such as Voice over IP) over low-latency traffic (such as standard web traffic and file downloads). To recognize the latency tolerance of traffic, this channel reads the IPv4 Type of Service DiffServ Control Point (DSCP) bits. Enabling the high-priority channel reduces the maximum number of SMs that can be served in the sector.

Term	Definition
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See http://www.faqs.org/rfcs/rfc2068.html.
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See http://www.faqs.org/rfcs/rfc792.html.
indiscards count Field	How many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors count Field	How many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
innucastpkts count Field	How many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
inoctets count Field	How many octets were received on the interface, including those that deliver framing information.
Intel	A registered trademark of Intel Corporation.
inucastpkts count Field	How many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
inunknownprotos count Field	How many inbound packets were discarded because of an unknown or unsupported protocol.
IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See http://www.faqs.org/rfcs/rfc791.html.
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
L2TP over IPSec	Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.

Term	Definition
Late Collision Field	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Latency Tolerance	Acceptable tolerance for delay in the transfer of data to and from a module.
Line of Sight	Wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
Linux	A registered trademark of Linus Torvalds.
LNK/5	Furthest left LED in the module. In the operating mode, this LED is continuously lit when the Ethernet link is present. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Logical Unit ID	Final octet of the 4-octet IP address of the module.
LOS	Line of sight. The wireless path (not simply visual path) direct from module to module. The path that results provides both ideal aim and an ideal Fresnel zone.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Management Information Base	Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Cambium implementation, this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
Media Access Control Address	Hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MIR	See Maximum Information Rate.

Term	Definition
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See http://www.faqs.org/rfcs/rfc1631.html.
NBI	See Northbound Interface.
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.
NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. RFC 1001 defines the concepts and methods. RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html.
Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See http://www.faqs.org/rfcs/rfc1631.html.
Network Management Station	See NMS.
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects). See also Simple Network Management Protocol.
Object	Network variable that is defined in the Management Information Base.
OSS	Operations support system, such as a customer relationship management (CRM), billing, or provisioning system. The application programming interface (API) for Prizm supports integrating Prizm with an OSS.
outdiscards count Field	How many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
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.

Term	Definition
outucastpkts count Field	How many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Override Plug	Device that enables the operator to regain control of a module that has been locked by the No Remote Access feature, the 802.3 Link Disable feature, or a password or IP address that cannot be recalled. This device can be either fabricated on site or ordered.
PMP	See Point-to-Multipoint Protocol.
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.
Power Control	Feature in Release 4.1 and later that allows the module to operate at less than 18 dB less than full power to reduce self-interference.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
PPTP	Point to Point Tunneling Protocol. One of several virtual private network implementations. Regardless of whether the Network Address Translation (NAT) feature enabled, Subscriber Modules support VPNs that are based on this protocol.
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.
QoS	Quality of Service. A frame field that Bandwidth and Authentication Manager (BAM) provides to the AP and SM about the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields.
Quality of Service	A frame bit that Bandwidth and Authentication Manager (BAM) provides to the AP and SM the sustained data rates and burst data limits of the SM. The format of this field is 64 hexadecimal characters of 0 to 9 and a to f. The BAM SQL database expresses this field as five contiguous subfields. Also known as QoS.

Term	Definition
Quick Start	Interface page that requires minimal configuration for initial module operation.
Radio Signal Strength Indicator	Relative measure of the strength of a received signal. An acceptable link displays an Radio Signal Strength Indicator (RSSI) value of greater than 700.
Random Number	Number that the Bandwidth and Authentication Manager (BAM) generates, invisible to both the SM and the network operator, to send to the SM as a challenge against an authentication attempt.
Reader	A registered trademark of Adobe Systems, Incorporated.
Recharging	Resumed accumulation of data in available data space (buckets). See Buckets.
Red Hat	A registered trademark of Red Hat, Inc.
Reflection	Change of direction and reduction of amplitude of a signal that encounters an object larger than the wavelength. Reflection may cause an additional copy of the wavelength to arrive after the original, unobstructed wavelength arrives. This causes partial cancellation of the signal and may render the link unacceptable. However, in some instances where the direct signal cannot be received, the reflected copy may be received and render an otherwise unacceptable link acceptable.
Region Code	A parameter that offers multiple fixed selections, each of which automatically implements either the Dynamic Frequency Selection (DFS) standard that is required by law or regulatory to apply or no DFS, based on the frequency band range and the selected region. PMP 450 equipment shipped to the United States is locked down with a Region Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
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.
RF	Radio frequency. How many times each second a cycle in the antenna occurs, from positive to negative and back to positive amplitude.
RJ-11	Standard cable that is typically used for telephone line or modem connection.
RJ-45	Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later modules auto-sense whether the cable is straight-through or crossover.
Router	Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.
RPM	Red Hat® Package Manager.

Term	Definition
RSSI	Radio Signal Strength Indicator. A relative measure of the strength of a received signal. An acceptable link displays an RSSI value of greater than 700.
RxBabErr Field	This field displays how many receiver babble errors occurred.
RxOverrun Field	This field displays how many receiver overrun errors occurred on the Ethernet controller.
SDK	*PrizmEMS™ Software Development Kit (SDK)*—the document that provides server administrator tasks, GUI developer information for console automation that allows higher-level systems to launch and appropriately display the Prizm management console. The SDK also describes the how to define new element types and customize the Details views.
Secure Shell	A trademark of SSH Communications Security.
Self-interference	Interference with a module from another module in the same network.
SES/2	Third-from-right LED in the module. In the Access Point Module and Backhaul timing master, this LED is unused. In the operating mode for a Subscriber Module or a Backhaul timing slave, this LED flashes on and off to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
SFTP	Secure File Transfer Protocol.
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See http://www.faqs.org/rfcs/rfc1157.html.
SM	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
SM MIB	Management Information Base file that defines objects that are specific to the Subscriber Module or Backhaul timing slave. See also Management Information Base.
SNMP	See Simple Network Management Protocol, defined in RFC 1157.
SNMP Trap	Capture of information that informs the network monitor through Simple Network Management Protocol of a monitored occurrence in the module.
Standard Operating Margin	See Fade Margin.

Term	Definition
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See http://www.faqs.org/rfcs/rfc2050.html. See also DHCP.
su -	A command that opens a Linux® operating system session for the user `root`.
Subnet Mask	32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.
Subscriber Module	Customer premises equipment (CPE) device that extends network or Internet services by communication with an Access Point Module or an Access Point cluster.
Sustained Data Rate	Preset rate limit of data transfer.
Switch	Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.
SYN/1	Second-from-right LED in the module. In the Access Point Module or Backhaul timing master, as in a registered Subscriber Module or Backhaul timing slave, this LED is continuously lit to indicate the presence of sync. In the operating mode for a Subscriber Module or Backhaul timing slave, this LED flashes on and to indicate that the module is not registered. In the aiming mode for a Subscriber Module or a Backhaul timing slave, this LED is part of a bar graph that indicates the quality of the RF link.
Sync	GPS (Global Positioning System) absolute time, which is passed from one module to another. Sync enables timing that prevents modules from transmitting or receiving interference. Sync also provides correlative time stamps for troubleshooting efforts.
TCP	Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See http://www.faqs.org/rfcs/rfc793.html.
tcp	Transport Control type of port. The system uses Port 3306:tcp for MySQL® database communications, Port 9080:tcp for SSE `telnet` communications, and Port 9090:tcp for Engine `telnet` communications.

Term	Definition
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.
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.