Cambium
PMP 450 Planning 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 4-92.

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 Planning Guide

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

The guide consists of the following chapters:

- Chapter 1: Product description
- Chapter 2: Planning considerations
- Chapter 3: Legal information
- Chapter 4: Reference information

General information

Version information

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

Issue	Date of issue	Remarks
000v001	May 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: Product description

This chapter provides a high level description of the PMP 450 product. It describes in general terms the function of the product, the main product variants and typical deployment. It also describes the main hardware components.

The chapter consists of the following topics:

- Overview of PMP 450 on page 1-2: Introduces the key features, typical uses, product variants and components of the PMP 450.
- Access Point (AP) on page 1-5: Describes the AP and its interfaces
- Subscriber Module (SM) on page 1-8: Describes the SM and its interfaces
- Cabling and lightning protection on page 1-10: Describes the cabling and lightning protection components of a PMP 450 installation.
- Wireless operation on page 1-11: Describes how the PMP 450 wireless link is operated, including modulation modes, power control and security.
- System management on page 1-15: Introduces the PMP 450 management system, including the web interface, installation, configuration, alerts and upgrades.

Overview of PMP 450

This section introduces the key features, typical uses, product variants and components of the PMP 450.

Purpose

Cambium PMP 450 Series networks are designed for wireless point-to-multipoint links in the unlicensed 5.8 GHz band. Users must ensure that the PMP 450 Series complies with local operating regulations.

The PMP 450 Series adds dramatically increased network throughput and capacity. The PMP 450 Series enables network operators to grow their business by offering more capacity for data, voice and video applications.

An upcoming release of the PMP 450 Series Access Point will support simultaneous communication with PMP 100 series FSK and PMP 430 series OFDM subscriber modules (PMP 450 AP “Combo Mode”).

Key features

The Cambium PMP 450 Series offers the following benefits:

- Cambium’s highest performing point-to-multipoint solution, with up to 80 Mbps usable throughput
- State-of-the-art MIMO (Multi-In Multi-Out) technology
- Better spectral efficiency than other MIMO alternatives
- Efficient GPS synchronized, scheduled TDD operation for easy Access Point site deployment and performance that is consistent regardless of subscriber loading
- A range of cost-effective subscriber device solutions to meet the business case of any network application

There are three major sub-features that comprise the MIMO techniques utilized in the PMP 450 product:

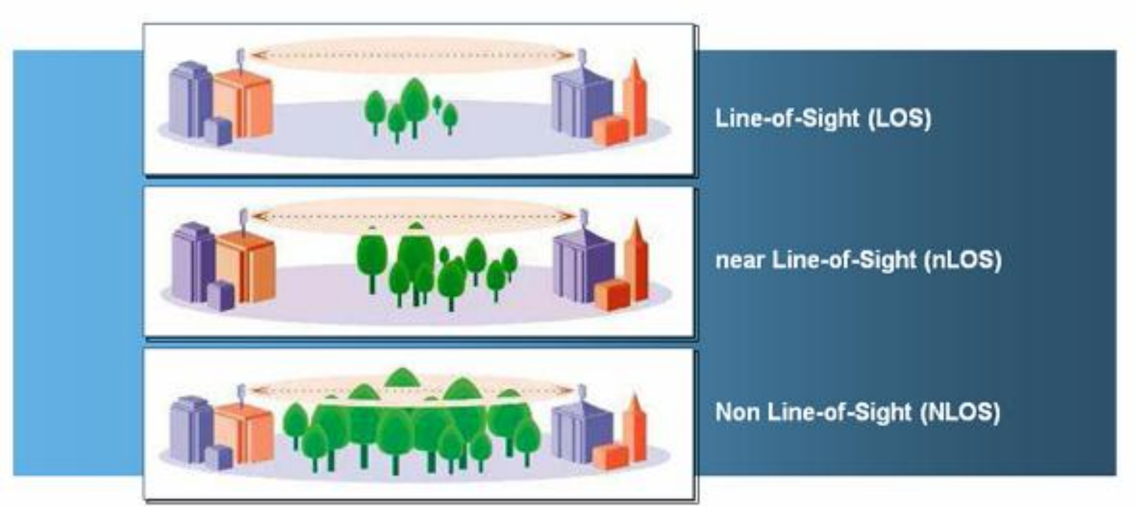
- Matrix B: This technique provides for the ability to double the throughput of a radio transmission under proper RF conditions. Different data streams are transmitted simultaneously on two different antennas.
- Matrix A: This technique is also called Alamouti Space Time Coding. The same data stream is transmitted at the same time on two different antennas with special coding.
- MRC: MRC stands for Maximal Ratio Combining which is a form of receive diversity. With this technique, two receivers and their associated antennas receive the transmitted signal. The two received signals are combined into a single higher quality signal. This technique increases the link budget of a system.

nLOS benefits and limitations

In addition to providing LOS (Line-Of-Sight) connectivity, use of OFDM technology can provide nLOS (near Line-Of-Sight) connectivity and sometimes NLOS (Non-Line-Of-Sight) connectivity:

- LOS: the installer can see the AP from the SM and the first Fresnel zone is clear.
- nLOS: the installer can see the AP from the SM, but a portion of the first Fresnel zone is blocked.
- NLOS: the installer cannot see the AP from the SM and a portion or even much of the first Fresnel zone is blocked, but subsequent Fresnel zones are open.

Figure 1 Line Of Sight Diagram



Whereas multi-pathing degrades a link in some technologies (FSK, for example), OFDM can often use multi-pathing to an advantage to overcome nLOS, especially in cases where the Fresnel zone is only partially blocked by buildings, “urban canyons”, or foliage. OFDM tends to help especially when obstacles are near the middle of the link, and less so when the obstacles are very near the SM or AP.

However, attenuation through walls and trees is substantial for any use of the 5.8 GHz frequency band. Even with OFDM, these products should not be expected to penetrate walls or extensive trees and foliage.

Typical deployment

The PMP 450 Series consists of Access Point Modules and Subscriber Modules. The radio link operates on a single frequency channel in each direction using Time Division Duplex (TDD).

Applications for the PMP 450 Series include:

- High throughput enterprise applications
- nLOS video surveillance in metro areas
- Urban area network extension
- Network extension into areas with foliage

Greenfield deployment

The PMP 450 Series equipment may be deployed as a standalone network deployment offering a high-speed access network.

System components

PMP 450 Access Point

- **Access Point Module (AP):** A connectorized outdoor transceiver unit containing all the radio, networking, antenna, and surge suppression electronics.
- **Access Point Power Supply:** An indoor power supply module providing Power-over-Ethernet (PoE) supply to the Access Point.
- **Cabling:** Cat 5e cables, grounding cables, and connectors.

PMP 450 Subscriber Module

- **Subscriber Module (SM):** An integrated-antenna outdoor transceiver unit containing all the radio, antenna, and networking electronics.
- **Subscriber Module Power Supply:** An indoor power supply module providing Power-over-Ethernet (PoE) supply to the Subscriber Module.
- **Cabling and lightning protection:** Cat 5e cables, grounding cables, connectors and lightning protection (surge suppression).

Product variants

The PMP 450 Series is available in the following product variants:

Table 1 PMP 450 frequency variants

Variant	Region	Frequency Coverage (MHz)	Channel Bandwidth (MHz)
PMP 58450	ETSI 5 GHz Band C	5725-5875	20

Access Point (AP)

The AP is a self-contained unit that houses both radio and networking electronics. The AP is supplied in a connectorized configuration for use with an external antenna. Connectorized units with external antennas can cope with more difficult radio conditions.

Figure 2 AP, Radio unit

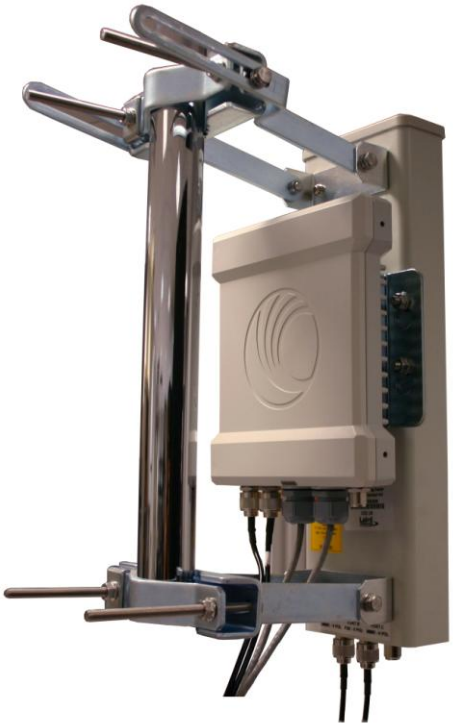
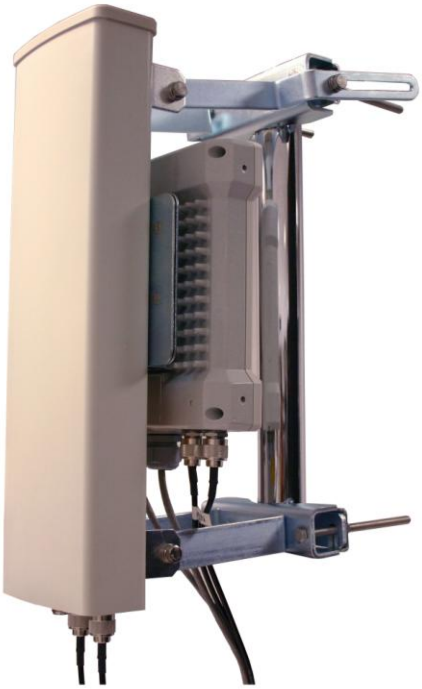


Figure 3 AP, antenna



AP interfaces

The AP interfaces are illustrated in Figure 4 and described in Table 2.

Figure 4 AP interfaces

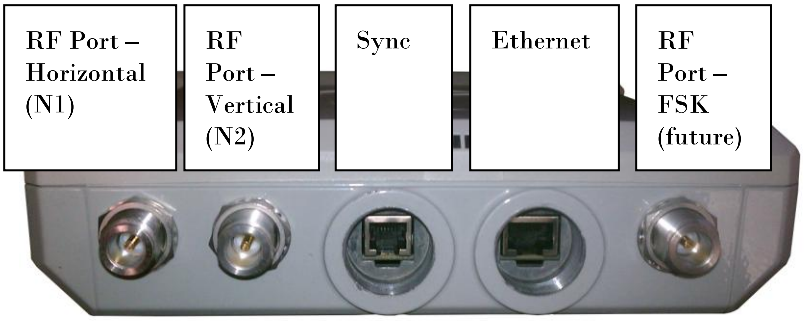


Table 2 AP Interfaces

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
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

Mounting brackets

The AP is supplied with a bracket for mounting it to a pole of 50mm (2") to 75mm (3") in diameter. For more information on hardware installation, reference the *PMP 450 Installation Guide*.

Network connection

The network connection to a PMP 450 Series AP is made via a 1000BaseT or 100BaseT Ethernet connection. Power is provided to the AP over the Ethernet connection using a patented non-standard powering technique.

AP power supply

The AP power supply generates the AP supply voltage (24 VDC) from the external DC source and injects the supply voltage into the AP.

The power supply is connected to the AP and network equipment using Cat5e cable with RJ45 connectors. Refer to Cabling and lightning protection on page 1-10.

Further reading on the AP

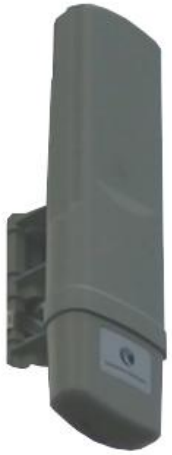
For more information on the AP, refer to the following:

- AP or SM site selection on page 2-14 describes how to select a site for the AP or SM.

Subscriber Module (SM)

The SM is a self-contained unit that houses both radio and networking electronics. The SM is supplied in an integrated antenna configuration.

Figure 5 PMP 450 Series SM (front view)



SM interfaces

Figure 6 SM interfaces

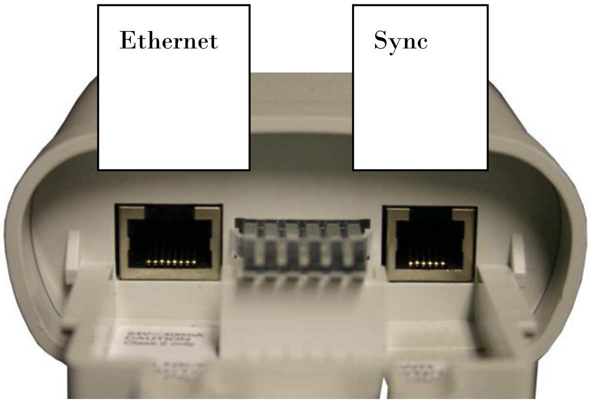


Table 3 SM Interfaces

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

Interface	Function	Cabling
Ground Lug (bottom of unit)	For grounding the unit	10 AWG copper wire

Mounting brackets

For mounting PMP 450 SMs, Cambium Networks offers the SMMB1A mounting bracket.

Network connection

The network connection to a PMP 450 Series SM is made via a 1000BaseT or 100 BaseT Ethernet connection. Power is provided to the SM over the Ethernet connection using a patented non-standard powering technique.

SM power supply

The SM power supply generates the SM supply voltage (30 VDC) from the external DC source and injects the supply voltage into the SM.

The power supply is connected to the SM and network equipment using Cat5e cable with RJ45 connectors. Refer to Cabling and lightning protection on page 1-10.

Further reading on the SM

For more information on the SM, refer to the following:

- AP or SM site selection on page 2-14 describes how to select a site for the SM.

Cabling and lightning protection

This section describes the cabling and lightning protection components of a PMP 450 installation.

PMP and lightning protection

Due to the full metallic connection to the tower or support structure through the AP antenna, grounding the AP and installing a 600SS surge suppressor within 3 ft (1 m) of the AP is strongly recommended. This suppresses overvoltages and overcurrents such as those caused by near-miss lightning. APs provide a grounding lug for grounding to the tower or support structure. A pole mount kit is available for the 600SS. The pole mount kit provides a grounding point on one of its U-bolts that can be used for terminating ground straps from both the 600SS and the AP.

⚠ CAUTION

The PMP 450 Series is not designed to survive direct lightning strikes. For this reason the unit should not be installed as the highest point in a localized area.

Outdoor connections

The term 'drop cable' refers to the cable that is used for all connections that terminate outside the building, for example, connections between the AP/SM, surge supressors (if installed), GPS receivers (if installed) and the power supply injector.

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

- Use only shielded cables and connectors to resist interference and corrosion
- 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

Wireless operation

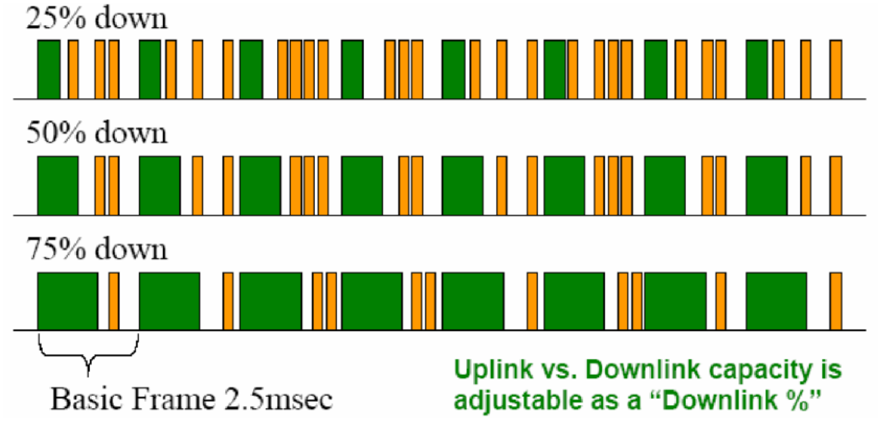
This section describes how the PMP 450 wireless link is operated, including modulation modes, power control and security.

Time division duplexing

The system uses Time Division Duplexing (TDD) – one channel alternately transmits and receives rather than using one channel for transmitting and a second channel for receiving. To accomplish TDD, the AP must provide sync to its SMs. Furthermore, collocated APs must be synced together – an unsynchronized AP that transmits during the receive cycle of a collocated AP can prevent a second AP from being able to decode the signals from its SMs. In addition, across a geographical area, APs that can "hear" each other benefit from using a common sync to further reduce self interference within the network.

Modules use TDD on a common frequency to divide frames for uplink (orange) and downlink (green) usage, as shown in Figure 7.

Figure 7 TDD frame division



Uplink vs. Downlink capacity is adjustable as a "Downlink %"

OFDM and channel bandwidth

The PMP 450 Series transmits using Orthogonal Frequency Division Multiplexing (OFDM). The channel bandwidth of the OFDM signal 20 MHz.

Link operation – Dynamic Rate Adapt

PMP 450 Series products offer four levels or speeds of operation – 1x (QPSK), 2x (QPSK-MIMO-B), 4x (16QAM-MIMO-B), and 6X (64QAM-MIMO-B). If received power is less due to distance between the AP and the SM or due to obstructions, or interference affects the RF environment, the system will automatically and dynamically adjust links to the best operation level. Distance, rates and other information associated with the operation levels are shown in Table 4 on page 1-13.

The system chooses its operation rate dynamically, based on an internal ARQ (Automatic Repeat reQuest) error control method. With ARQ, every data slot of every frame sent over the air (except downlink broadcast) is expected to be acknowledged by the receiver, and if acknowledgement is not received, the data is resent. The sending unit monitors these resends, and adjusts the operation rate accordingly. A normal system may have links that change levels of operation as the RF environment changes. Furthermore, the links operate independently; normal operation can have a downlink running at 6X while the uplink RF environment only supports 2x.

The default is for both AP and SM to be enabled for 6X operation. An operator may "lock down" a link to the following modes of operation:

- 1x (No Rate Adapt)
- 1x (MIMO duplicate on both paths)
- 1x/2x
- 1x/2x (MIMO)
- 1x/2x/3x
- 1x/2x/3x/4x
- 1x/2x/4x (MIMO)
- 1x/2x/4x/6x (MIMO)

An operator may lock down an entire sector to a particular Dynamic Rate Adapt setting using the **Dynamic Rate Adapt** parameter on the AP's **Configuration, General** page. This parameter locks down uplink or downlink of all links in the sector, and overrides any SM settings. For example, if an individual link is set for 1x/2x/4x/6x (MIMO) operation at the SM and the sector is set for 1x operation at the AP, all links in the sector will be locked down to 1x operation.

In most cases an operator is well-served to leave the setting at 1x/2x/4x/6x (MIMO) and let the system automatically and dynamically choose the best rate for each link. Cases when it may be useful to lock down a link to a lesser rate adapt is:

- If you are having trouble aiming a link or getting it to register, locking the link down may help in some cases.
- If the link is suspected to be oscillating between operation rates to the detriment of throughput, locking the link down may increase throughput. Usually, even if the link is moving rapidly between operation rates, overall link throughput and sector capacity are highest if the link is left at 1x/2x/4x/6x (MIMO) and the link can choose its own rate dynamically.
- General link troubleshooting

Optimal sector utilization involves having as many links as possible running at 6x. This provides as much capacity as possible for the sector. As an example, you want to limit throughput to an individual subscriber to 1x rates. This *does not* mean you should set that link to 1x operation. Use MIR (Maximum Information Rate) settings to cap the SM's bandwidth use, but let the link run at as high an operation rate as the RF environment will allow. This ensures that any transmission uses as little "air time" as possible, leaving more "air time" for other SMs.

Table 4 Performance Details – Dynamic Rate Adapt

Product	**Parameter**		**Performance Details**			
			1x	**2x**	**4x**	**6x**
PMP 58450	Modulation		QPSK	16 QAM		
	5.8-GHz Max. LOS Range	with Integrated SM antenna	6.4 miles / 10.24 km	5 miles / 8 km		
		with LENS that adds 6 dB to SM Range	13 miles / 20.8 km	10 miles / 16 km		
		with Reflector Dish that adds 15 dB to SM Range	30 miles / 48 km	29 miles / 46.4 km		
	5.8-GHz Max. Aggregate Throughput with 1/16 Cyclic Prefix	20 MHz Channel: (up+down)	16.5 Mbps	32 Mbps		
	5.8-GHz Nominal Receive Sensitivity (including FEC)	20MHz Channel	-87 dBm	-84 dBm	-77 dBm	-70 dBm

Adaptive modulation

PMP 450 units can transport data over the wireless link using a number of different modulation modes. The radio automatically selects QPSK (Quadrature Phase Shift Keying), 16-QAM (Quadrature Amplitude Modulation), or 64-QAM based on RF environment to provide 1x, 2x, 4x, and 6x operation.

MIMO

Multiple-Input Multiple-Output (MIMO) techniques provide protection against fading and increase the probability that the receiver will decode a usable signal. When the effects of MIMO are combined with those of OFDM techniques and a high link budget, there is a high probability of a robust connection over a non-line-of-sight path.

There are three major sub-features that comprise the MIMO techniques utilized in the PMP 450 product:

- Matrix B: This technique provides for the ability to double the throughput of a radio transmission under proper RF conditions. Different data streams are transmitted simultaneously on two different antennas.
- Matrix A: This technique is also called Alamouti Space Time Coding. The same data stream is transmitted at the same time on two different antennas with special coding.
- MRC: MRC stands for Maximal Ratio Combining which is a form of receive diversity. With this technique, two receivers and their associated antennas receive the transmitted signal. The two received signals are combined into a single higher quality signal. This technique increases the link budget of a system.

Cyclic Prefix

OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol (slot) to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.

Encryption

The Cambium PMP 450 Series supports optional encryption for data transmitted over the wireless link. The PMP 450 Series supports the following form of encryption for security of the wireless link:

- **DES (Data Encryption Standard)**: An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system.

Further reading on wireless operation

For information on planning wireless operation, refer to the following:

- Regulatory planning on page 2-4 describes the regulatory restrictions that affect radio spectrum usage, such as frequency range.

System management

This section introduces the PMP 450 management system, including the web interface, installation, configuration, alerts and upgrades, and management software.

Management agent

PMP 450 equipment is managed through an embedded management agent. Management workstations, network management systems or PCs can be connected to this agent using the module's Ethernet port or over-the air (SM).

The management agent supports the following interfaces:

- Hyper text transfer protocol (HTTP)
- HTTP over transport layer security (HTTPS/TLS)
- RADIUS authentication
- TELNET
- Simple network management protocol (SNMP)
- Network time protocol (SNTP)
- System logging (Syslog)
- Wireless Manager (WM) software
- Canopy Network Updater Tool (CNUT) software

Web server

The PMP 450 management agent contains a web server. The web server supports access via HTTP and HTTPS/TLS interfaces.

Web-based management offers a convenient way to manage the PMP 450 equipment from a locally connected computer or from a network management workstation connected through a management network, without requiring any special management software. The web-based interfaces are the only interfaces supported for installation of PMP 450, and for the majority of PMP 450 configuration management tasks.

Web pages

The web-based management interfaces provide comprehensive web-based fault, configuration, performance and security management functions organized into the following web-pages and groups:

Access Point web-pages:

- **Home:** The Home web-page reports the general device status, session status, remote subscriber status, event log information, network interface status, and layer 2 neighbor information.
- **Configuration:** The Configuration web-page may be utilized for configuring general device parameters, as well as IP, radio, SNMP, Quality of Service (QoS), security, time, VLAN, DiffServ, protocol filtering, and unit settings.
- **Statistics:** The Statistics web-page reports detailed operating statistics for the scheduler, SM registration failures, bridge control block, bridging table, Ethernet, radio, VLAN, data VC, throughput, filter, ARP, overload, DHCP relay, pass through, and DNS.
- **Tools:** The Tools web-page offers useful tools for device installation, configuration, and operation including link capacity test, frame calculator, subscriber configuration, link status, remote spectrum analyzer, sessions, and DNS test.
- **Logs:** The Logs web-page displays logs related to device operation including AP sessions, AP authentication state machine, AP authorization state machine, and EAP Radius.
- **Accounts:** These web-pages are used to configure device user accounts.
- **Quick Start:** The Quick Start web-page provides a walkthrough of configuring radio parameters for initial operation.
- **Copyright:** The Copyright web-page displays pertinent device copyright information.

Subscriber Module web-pages:

- **Home:** The Home web-page reports the general device status, event log information, network interface status, and layer 2 neighbor information.
- **Configuration:** The Configuration web-page may be utilized for configuring general device parameters, as well as IP, radio, SNMP, Quality of Service (QoS), security, VLAN, DiffServ, protocol filtering, NAT, PPPoE, NAT port mapping, and unit settings.
- **Statistics:** The Statistics web-page reports detailed operating statistics for the scheduler, bridge control block, bridging table, translation table, Ethernet, radio, VLAN, data VC, filter, NAT, NAT DHCP, ARP, overload, PPPoE, peer information, and DNS.
- **Tools:** The Tools web-page offers useful tools for device installation, configuration, and operation including a spectrum analyzer, alignment configuration and tool, link capacity test, AP evaluation, frame calculator, BER results, link status, and DNS test.
- **Logs:** The Logs web-page displays logs related to device operation including the NAT table, SM session, SM authentication, SM authorization, PPPoE session, and EAP Radius.
- **Accounts:** These web-pages are used to configure device user accounts.
- **PDA:** The PDA web-page includes 320 x 240 pixel formatted displays of information important to installation and alignment for installers using legacy PDA devices. All device web pages are compatible with touch devices such as smart phones and tablets.
- **Copyright:** The Copyright web-page displays pertinent device copyright information.

Identity-based user accounts

When identity-based user accounts are configured, a security officer can define from one to four user accounts, each of which may have one of the four possible roles:

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

See Table 21 Identity-based user account permissions - AP on page 2-56 and Table 22 Identity-based user account permissions - SM on page 2-58 for detailed information on account permissions.

Remote Authentication Dial In User Service (RADIUS)

The PMP 450 system includes support for RADIUS (Remote Authentication Dial In User Service) protocol functionality including:

- **Authentication:** Allows only known SMs onto the network (blocking "rogue" SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to "rogue" APs). RADIUS authentication is used for SMs, but not used for APs.
- **SM Configuration:** Configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when an SM registers to an AP.
- **Centralized AP and SM user name and password management:** Allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does not track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Wireless Manager. This accounting is not the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed-IP-Address:** Operators may use a RADIUS server to assign management IP addressing to SM modules.

SNMP

The management agent supports fault and performance management by means of an SNMP interface. The management agent is compatible with SNMP v1 and SNMP v2c using 5 Management Information Base (MIB) files which are available for download from the Cambium Networks Support website (http://www.cambiumnetworks.com/support/pmp/software/).

Network Time Protocol (NTP)

The clock supplies accurate date and time information to the system. It can be set to run with or without a connection to a network time server (NTP). It can be configured to display local time by setting the time zone and daylight saving in the Time web page.

If an NTP server connection is available, the clock can be set to synchronize with the server time at regular intervals.

PMP 450 devices may receive NTP data from a CMM3 or CMM4 module, or from an NTP server configured in the system's management network.

The Time Zone option is configurable on the AP's Time Configuration page, and may be used to offset the received NTP time to match the operator's local time zone. When set on the AP, the offset will be set for the entire sector (SMs will be notified of the current Time Zone upon initial registration). If a Time Zone change is applied, the SMs will be notified of the change in a best effort fashion, meaning some SMs may not pick up the change until the next re-registration. Time Zone changes are noted in the Event Log of the AP and SM.

Wireless Manager (WM)

Cambium Networks Wireless Manager 4.0 is recommended for managing PMP 450 networks. You can achieve better uptime through better visibility of your network with the Cambium Wireless Manager. This network management software tool offers breakthrough map-based visualization capabilities using embedded Google maps, and combined with advanced configuration, provisioning, alerting and reporting features you can control your entire outdoor wireless network including Mesh Wide Area Network, and Point-to-Multipoint and Point-to-Point solutions as well as other SNMP enabled devices. With its powerful user interface you will not only be able to control your network's access, distribution and backhaul layers, but you will also have visibility to WLAN sites and be able to quickly launch indoor network management systems.

Some key features of Wireless Manager are:

- **Template-Based Configuration:** With Wireless Manager's user-defined templates you can accelerate the process for the configuration of the devices you add to your network resulting in quicker and easier deployments. The template-based functionality provides an automated way to configure large numbers of network devices with just a few mouse clicks, and can be scheduled to occur at any time via Wireless Manager's Task Scheduler.
- **Ultralight Thin Client:** With the growing mobile workforce it is important to have access to the status of your network at any time. With Wireless Manager you can view the status and performance of your entire wireless network via a compact web interface accessible by your smart phone.
- **Map-Based Visualization:** Wireless Manager overlays sophisticated real-time information about your network elements onto building layouts and dynamic Google maps. Visuals can be scaled to view an entire city or building or a specific area, floor or link.
- **High Availability Architecture Support:** Wireless Manager offers a high availability option, providing a highly reliable and redundant network management solution that ensures you always have management access to your network.

- **High Scalability:** The enhanced Wireless Manager offers you server scalability with support for up to 10,000 nodes as well as support for distributed server architecture.

Cambium's Wireless Manager 4.0 available for download at: http://www.cambiumnetworks.com/support under "Management Tools".

Canopy Network Updater Tool (CNUT)

CNUT 4.1 (Canopy Network Updater Tool) is the stand-alone software update tool for PMP 450 Series products.

The Canopy Network Updater Tool:

- automatically discovers all network elements
- executes a UDP command that initiates and terminates the Autoupdate mode within APs. This command is both secure and convenient:
  - For security, the AP accepts this command from only the IP address that you specify in the Configuration page of the AP.
  - For convenience, Network Updater automatically sets this Configuration parameter in the APs to the IP address of the Network Updater server when the server performs any of the update commands.
- allows you to choose among updating
  - your entire network.
  - only elements that you select.
  - only network branches that you select.
- provides a Script Engine that you can use with any script that
  - you define.
  - Cambium supplies.

CNUT is available at http://www.cambiumnetworks.com/support under "Management Tools".

Capacity upgrades

Capacity upgrades are supplied as an access key purchased from your Cambium Point-to-Multipoint distributor or solutions provider. The upgrade is applied by entering the supplied URL in a PMP 450 module-connected web browser address bar.

Software upgrade

CNUT 4.1 (Canopy Network Updater Tool) is the stand-alone software update tool for PMP 450 Series products.

CNUT is available at http://www.cambiumnetworks.com/support under "Management Tools".

PMP 450 software images are digitally signed, and the AP/SM will accept only images that contain a valid Cambium PMP digital signature. The AP/SM always requires a reboot to complete a software upgrade.

NOTE

Obtain the application software and this user guide from the support website BEFORE warranty expires.

Further reading on system management

For more information on system management, refer to the following:

- Security planning on page 2-55 describes how to plan for PMP 450 links to operate in secure modes.

Chapter 2: Planning considerations

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 2-4 describes how to plan PMP 450 links to conform to the regulatory restrictions that apply in the country of operation.
- Network migration planning on page 2-5 presents migration scenarios to aid in planning a network deployment
- Site planning on page 2-13 describes factors to be considered when choosing sites for the equipment
- 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) = 0.1045aV2

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 11 Lateral force - metric and Table 12 Lateral force - US.

Table 11 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) = 0.0042Av2

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 12.

Table 12 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
- Link planning on page 2-15 describes factors to be taken into account when planning links, such as range, path loss and throughput.
- Analyzing the RF Environment on page 2-20 describes how to map RF neighbor frequencies, anticipate reflection, assess RF obstructions in the Fresnel Zone, and plan channel usage.
- Selecting Sites for Network Elements on page 2-24 describes how to survey sites, find expected coverage areas, clear the radio horizon, and calculate aim angles.
- Diagramming Network Layouts on page 2-27 includes tips on how to avoid self interference as well as interference from external sources.
- Grounding and lightning protection on page 2-29 discusses wiring standards, the need for surge protection, lightning protection zones, and general protection requirements.
- Configuration options for TDD synchronization on page 2-38 covers the importance of GPS synchronization as well as planning for installation
- Data network planning on page 2-41 discusses IP networking and other networking features provided with the PMP 450 product
- Security planning on page 2-55 can be referenced for information regarding security features of the product.

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 Calculating maximum power level for connectorized AP units on page 2-18.

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

Network migration planning

The PMP 450 Series offers current network operators the ability to migrate to PMP 450 for expanded network capacity and capability. The following sections are provided to aid in establishing a planning framework for deploying a PMP 450 system.

PMP 450 deployment scenarios

The following sections detail network deployment scenarios and strategies for the PMP 450 product. This table may be referenced to begin planning the PMP 450 deployment based on the current network configuration (if applicable).

Definitions of deployment scenario terminology

Table 5 Deployment scenario terminology descriptions

Term	Definition
Existing System Release	The current running system software release
Existing Number of Sectors	The total number of AP sectors co-located in the current system
Existing Modulation	The type of modulation used in the current network. "FSK" indicates an existing PMP 1x0 series network, and "OFDM" indicates an existing PMP 430 network.
Existing Frequency Re-use Pattern	The current deployment's usage of frequency across tower sectors. For example, in a six AP sector deployment, the following represents an ABC frequency re-use pattern. • Sector 1 (A): 5745 • Sector 2 (B): 5765 • Sector 3 (C): 5785 • Sector 4 (A): 5745 • Sector 5 (B): 5765 • Sector 6 (C): 5785
Existing Ch BW	The channel size, or channel bandwidth used in the current system. For FSK (PMP 1x0 series) deployments, the channel bandwidth is always 20 MHz. For OFDM (PMP 430) deployments, the channel size may be 5, 10, or 20 MHz.

Term	Definition
Existing Total Bandwidth Used	The total amount of spectrum, in MHz, which is used by the existing system (including guard bands).
Existing Aggregate Tower Throughput (Mbps)	The total amount of throughput, in Mbps, available in the current network deployment.
Existing Additional Frequencies Available (MHz)	The number of additional frequencies unused by the current deployment that are available for usage by PMP 450 equipment.
Existing Migration method (Abrupt vs Graceful cutover)	An “abrupt” migration or cutover is implemented by replacing existing network equipment with PMP 450 equipment then routing network traffic through the new PMP 450 network. A “graceful” migration or cutover involves co-locating PMP 450 equipment with existing network equipment then incrementally routing traffic through the new PMP 450 equipment.
FINAL: Aggregate Throughput	The aggregate throughput available after upgrading to a PMP 450 network.
Resulting Number of Sectors	The number of sectors configured in the new PMP 450 network installation.
Resulting Modulation	The modulation scheme utilized in the new PMP 450 network installation.
Resulting Frequency Re-use Pattern	The new frequency re-use patter utilized in the new PMP 450 network installation. For example, in a six AP sector deployment, the following represents an ABC frequency re-use pattern. • Sector 1 (A): 5745 • Sector 2 (B): 5765 • Sector 3 (C): 5785 • Sector 4 (A): 5745 • Sector 5 (B): 5765 • Sector 6 (C): 5785
Resulting Ch BW	The resulting channel bandwidth must be 20 MHz (supported by PMP 450).
Resulting Total Bandwidth Used	The total amount of spectrum, in MHz, which is used by the existing system (including guard bands).
Resulting Aggregate Tower Throughput (Mbps)	The aggregate throughput available after upgrading to a PMP 450 network.

Term	Definition
Resulting Percentage Increase in Aggregate Tower Throughput	The amount of increase in tower (all sectors) throughput after upgrading to a PMP 450 network.
Total Bandwidth Used (During Migration) (MHz)	The total amount of spectrum (in MHz) used when migrating to a PMP 450 deployment (including guard bands and transitional frequency usage).

Sector capacity

The following table exhibits the maximum aggregate sector throughput for several Cambium network deployments. This table may be used as a reference for planning new networks or for planning network upgrades.

Table 6 Examples of aggregate sector throughput – various air interfaces

Air Interface	Rate Adapt	Ch BW (MHz)	Cyclic Prefix	Maximum Aggregate Sector Throughput (Mbps)
FSK (PMP 1x0 Series)	1x	20	N/A	7
FSK (PMP 1x0 Series)	2x	20	N/A	14
OFDM (PMP 430 Series)	1x	5	CP 1/16	4
OFDM (PMP 430 Series)	2x	5	CP 1/16	8
OFDM (PMP 430 Series)	3x	5	CP 1/16	12
OFDM (PMP 430 Series)	1x	10	CP 1/16	7
OFDM (PMP 430 Series)	2x	10	CP 1/16	15
OFDM (PMP 430 Series)	3x	10	CP 1/16	24
OFDM (PMP 430 Series)	1x	20	CP 1/16	15
OFDM (PMP 430 Series)	2x	20	CP 1/16	32
OFDM (PMP 430 Series)	3x	20	CP 1/16	50
OFDM (MIMO) (PMP 450 Series)	1x	20	CP 1/16	28
OFDM (MIMO) (PMP 450 Series)	4x	20	CP 1/16	59
OFDM (MIMO) (PMP 450 Series)	3x	20	CP 1/16	95

Deployment scenario 1

Deployment scenario 1 assumes that the existing network is comprised of PMP 1x0 equipment with the configuration listed below in Table 7. The migration in this scenario results in a complete replacement of PMP 1x0 series equipment with PMP 450 equipment.

In this scenario there is 10 MHz additional spectrum available to include the 5 MHz guard bands required by the PMP 450 equipment. Scenario 1 assumes that neighboring frequencies are free and that a guard band is not required.

Table 7 Deployment scenario 1

Term	Definition
Existing System Release	12.0
Existing Number of Sectors	6
Existing Modulation	FSK
Existing Frequency Re-use Pattern	ABC ABC
Existing Ch BW	20
Existing Aggregate Tower Throughput (Mbps)	84
Existing Total Bandwidth Used	60
Existing Additional Frequencies Available (MHz)	10
Existing Migration method (Abrupt vs Graceful cutover)	Abrupt
Replace Legacy Subscribers with 450 SMs	Required
Resulting Number of Sectors	6
Resulting Modulation	OFDM (MIMO)
Resulting Frequency Re-use Pattern	ABC ABC
Resulting Ch BW	20
Allow for OFDM Guard-band from out-of-network interferers	No
Resulting Total Bandwidth Used	70
Resulting Aggregate Tower Throughput (Mbps)	570
Resulting Percentage Increase in Aggregate Tower Throughput	679%

Table 8 Scenario 1 spectrum usage

Beginning frequency usage			Resulting frequency usage (assuming no interference at band edges)	
5725	▨		▨	
5730	▨		▨	
5735	🟦		🟪	
5740	🟦	**FSK (A)**	🟪	**MIMO (A)**
5745	🟦		🟪	
5750	🟦		🟪	
5755	🟩			
5760	🟩	**FSK (B)**	🟨	
5765	🟩		🟨	**MIMO (B)**
5770	🟩		🟨	
5775	🟥		🟨	
5780	🟥	**FSK (C)**		
5785	🟥		🟧	
5790	🟥		🟧	**MIMO (C)**
5795	▨		🟧	
5800	▨		🟧	
5805	▨		▨	
5810	▨		▨	
5815	▨		▨	
5820	▨		▨	
5825	▨		▨	
5830	▨		▨	
5835	▨		▨	
5840	▨		▨	

Deployment scenario 1 migration procedure

This procedure assumes that there are no temporary frequencies available and that the PMP 450 AP will be overlayed into an existing FSK sector sharing the frequency range around frequency "A".

Procedure 1a Deployment scenario 1 migration procedure

1 Identify proximity to potential system interferers by running a spectrum analysis scan where the PMP 450 equipment will be deployed. It is recommended to run this scan at several different times of day and night

2 Record all AP and SM configuration parameters within the current operating network, if applicable (screen scrapes? or SNMP walk?)

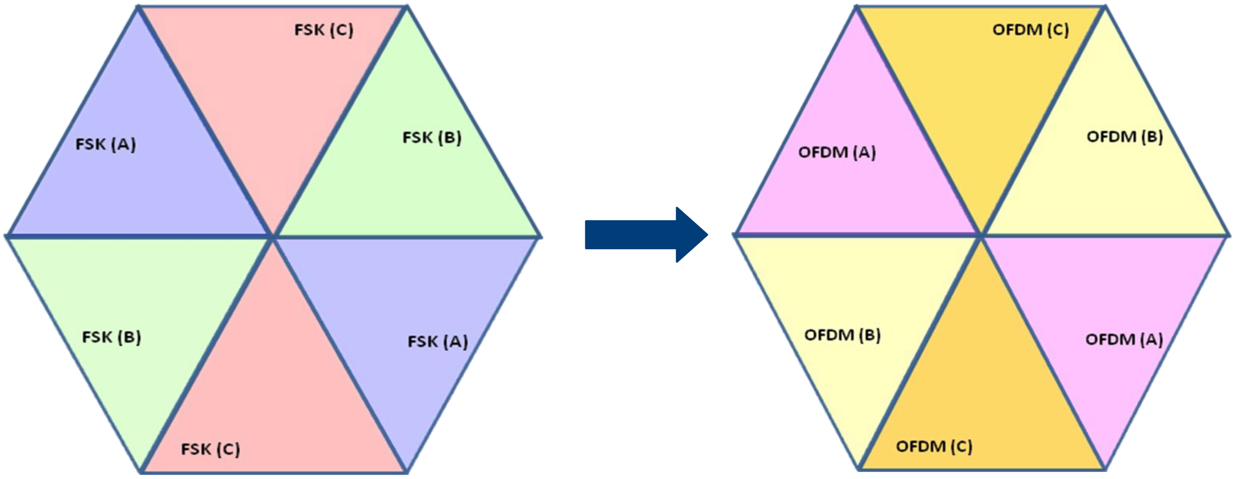
3 Configure the PMP 450 AP and SMs for deployment

4 Install the PMP 450 AP

5 Install the PMP 450 MIMO(A) SMs – powered on

6 Verify SM registration, link quality, and link performance to determine impact of upgrade to OFDM

Existing Sector Layout	Resulting Sector Layout



Deployment scenario 2

Deployment scenario 2 assumes that the existing network is comprised of PMP 1x0 equipment with the configuration listed below in Table 9. The migration in this scenario results in a complete replacement of PMP 1x0 series equipment with PMP 450 equipment.

In this scenario there is 20 MHz additional spectrum available to include the 5 MHz guard bands required by the PMP 450 equipment. Scenario 2 assumes that neighboring frequencies are cluttered and that a guard band is required.

Table 9 Deployment scenario 2

Term	Definition
Existing System Release	12.0
Existing Number of Sectors	6
Existing Modulation	FSK
Existing Frequency Re-use Pattern	ABC ABC
Existing Ch BW	20
Existing Aggregate Tower Throughput (Mbps)	84
Existing Total Bandwidth Used	60
Existing Additional Frequencies Available (MHz)	20
Existing Migration method (Abrupt vs Graceful cutover)	Abrupt
Replace Legacy Subscribers with 450 SMs	Required
Resulting Number of Sectors	6
Resulting Modulation	OFDM (MIMO)
Resulting Frequency Re-use Pattern	ABC ABC
Resulting Ch BW	20
Allow for OFDM Guard-band from out-of-network interferers	Yes
Resulting Total Bandwidth Used	80
Resulting Aggregate Tower Throughput (Mbps)	570
Resulting Percentage Increase in Aggregate Tower Throughput	679%

Table 10 Deployment scenario 2 spectrum usage

Beginning frequency usage			Resulting frequency usage (assuming interference at band edges)	
5725	▨		▨	
5730	▨		▨	
5735	🟦			
5740	🟦	**FSK (A)**	🟪	
5745	🟦		🟪	**MIMO (A)**
5750	🟦		🟪	
5755	🟩		🟪	
5760	🟩	**FSK (B)**		
5765	🟩		🟨	
5770	🟩		🟨	**MIMO (B)**
5775	🟥		🟨	
5780	🟥	**FSK (C)**	🟨	
5785	🟥			
5790	🟥		🟧	
5795	▨		🟧	**MIMO (C)**
5800	▨		🟧	
5805	▨		🟧	
5810	▨			
5815	▨		▨	
5820	▨		▨	
5825	▨		▨	
5830	▨		▨	
5835	▨		▨	
5840	▨		▨	
5845	▨		▨	
5850	▨		▨	
5855	▨		▨	
5860	▨		▨	

Deployment scenario 2 migration procedure

This procedure assumes that there are no temporary frequencies available and that the PMP 450 AP will be overlayed into an existing FSK sector sharing the frequency range around frequency “A”.

Directly replace the FSK AP at frequency “A” . There will be a 5 MHz shift in frequency “A” to accommodate the required OFDM guard band of 5 MHz.

Procedure 2 Deployment scenario 2 migration procedure

1 Identify proximity to potential system interferers by running a spectrum analysis scan where the PMP 450 equipment will be deployed. It is recommended to run this scan at several different times of day and night

2 Record all AP and SM configuration parameters within the current operating network, if applicable (screen scrapes? or SNMP walk?)

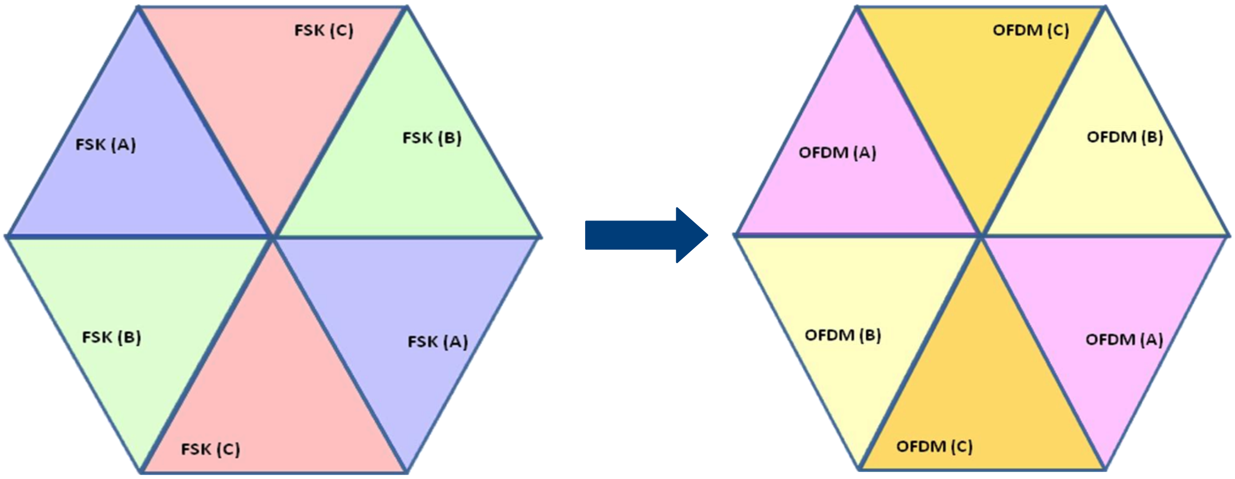
3 Configure the PMP 450 AP and SMs for deployment

4 Install the PMP 450 AP

5 Install the PMP 450 MIMO(A) SMs – powered on

6 Verify SM registration, link quality, and link performance to determine impact of upgrade to OFDM

Existing Sector Layout	Resulting Sector Layout



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 **Calculated distances and power compliance margins** on page 4-92.
- Height and location to achieve the best radio path.
- Ability to meet the requirements specified in Grounding and lightning protection on page 2-29.
- Aesthetics and planning permission issues.
- Cable lengths; see Maximum cable lengths on page 2-14.
- The effect of strong winds on the installation; see Wind loading on page 2-15.

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 LED and connecting Ethernet cables.
- Cable lengths; see Maximum cable lengths on page 2-14.

Maximum cable lengths

When installing PMP 450 Series APs or SMs, the maximum permitted length of the copper Ethernet interface cable is 100m (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 11 Lateral force - metric and Table 12 Lateral force - US.

Table 11 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 12.

Table 12 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

Link planning

This section describes factors to be taken into account when planning links, such as range, obstacles path loss and throughput.

Range and obstacles

Calculate the range of the link and identify any obstacles that may affect radio performance.

Perform a survey to identify all the obstructions (such as trees or buildings) in the path and to assess the risk of interference. This information is necessary in order to achieve an accurate link feasibility assessment.

The PMP 450 Series is designed to operate in Near-Line-of-Sight (nLOS), Non-Line-of-Sight (NLOS) and Line-of-Sight (LOS) environments. An NLOS environment is one in which there is no optical line-of-sight, that is, there are obstructions between the antennas. See Figure 1 Line Of Sight Diagram.

OFDM technology can often use multi-pathing to an advantage to overcome nLOS, especially in cases where the Fresnel zone is only partially blocked by buildings, “urban canyons”, or foliage. OFDM tends to help especially when obstacles are near the middle of the link, and less so when the obstacles are very near the SM or AP.

However, attenuation through walls and trees is substantial for any use of the 5.8 GHz frequency band. Even with OFDM, these products should not be expected to penetrate walls or extensive trees and foliage.

Table 13 shows range performance details for PMP 450 Series AP with a registered PMP 450 Series SM (OFDM link). Round trip latency is 5-7 msec for all platforms.

Table 13 Performance details – OFDM link

Product	Parameter		Performance Details			
			1x	2x	4x	6x
PMP 450 OFDM SM registered to PMP 450 AP)	Modulation		QPSK	QPSK-MIMO-B	16QAM-MIMO-B	64QAM-MIMO-B
	5.8-GHz Max. LOS Range	with Integrated SM antenna				
		with LENS that adds 6 dB to SM Range				
		with Reflector Dish that adds 15 dB to SM Range				

Path loss considerations

Path loss is the amount of attenuation the radio signal undergoes between the two ends of the link.

Calculating path loss

The path loss is the sum of the attenuation of the path if there were no obstacles in the way (Free Space Path Loss), the attenuation caused by obstacles (Excess Path Loss) and a margin to allow for possible fading of the radio signal (Fade Margin). The following calculation needs to be performed to judge whether a particular link can be installed:

$$L_{free\_space} + L_{excess} + L_{fade} + L_{seasonal} < L_{capability}$$

Where:	**Is:**
L_{free_space}	Free Space Path Loss (dB)
L_{excess}	Excess Path Loss (dB)
L_{fade}	Fade Margin Required (dB)
$L_{seasonal}$	Seasonal Fading (dB)
$L_{capability}$	Equipment Capability (dB)

Calculating maximum power level for connectorized AP units

If a connectorized PMP 450 AP is to be installed in a country that imposes an EIRP limit in the selected band, calculate the highest setting of Maximum Power Level that will be permitted using this formula:

Maximum Power Level (dBm) = Allowed EIRP (dBm) – Antenna Gain (dBi) + Cable Loss (dB)

Where:	**Is:**
Maximum Power Level (dBm)	the highest permissible setting of the transmitter output power,
Allowed EIRP (dBm)	the EIRP limit allowed by the regulations,
Antenna Gain (dBi)	the gain of the chosen antenna,
Cable Loss (dB)	the loss of the RF cable connecting the AP to the antenna.

The maximum allowed EIRP depends on the operating bandwidth of the radio as shown in Table 14.

Table 14 Normal EIRP limits with operating channel bandwidth

Radio/ Frequency	Channel Size	Region(s)	Max EIRP (Tx + Antenna Gain)
PMP 450 5.8 GHz	20 MHz	United States, Canada, Europe and India	36 dBm

Understanding Attenuation

An RF signal in space is attenuated by atmospheric and other effects as a function of the distance from the initial transmission point. The further a reception point is placed from the transmission point, the weaker is the received RF signal.

Calculating Link Loss

The link loss is the total attenuation of the wireless signal between two point-to-multipoint units. The link loss calculation is presented below:

$$P_{ll} = P_{T_x} - P_{R_x} + g_{T_x} + g_{R_x}$$

Where:

P_{ll} = Link Loss (dB)

P_{T_x} = Transmit power of the remote wireless unit (dBm)

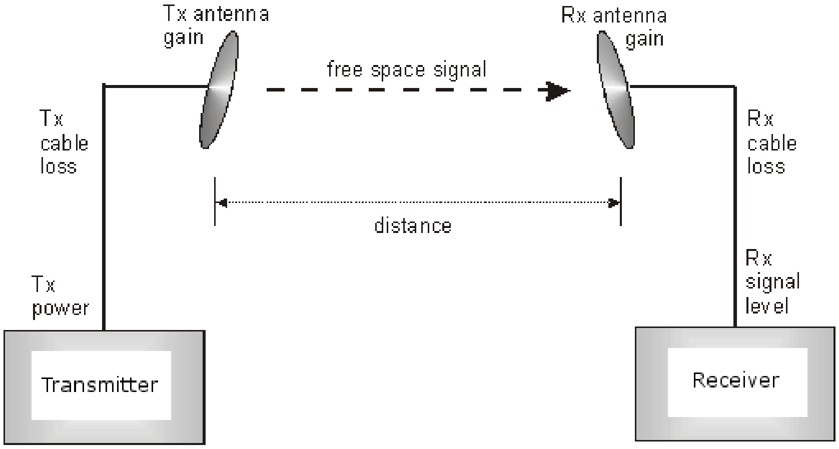
P_{R_x} = Received signal power at the local unit (dBm)

g_{T_x}, g_{R_x} = Antenna gain at the remote and local units respectively (dBi).

Calculating Rx Signal Level

The Rx sensitivity of each module is provided at http://www.cambiumnetworks.com. The determinants in Rx signal level are illustrated in Figure 8.

Figure 8 Determinants in Rx signal level



Rx signal level is calculated as follows:

$$\text{Rx signal level dB} = \textit{Tx power} - \textit{Tx cable loss} + \textit{Tx antenna gain} - \textit{free space path loss} + \textit{Rx antenna gain} - \textit{Rx cable loss}$$

NOTE

This Rx signal level calculation presumes that a clear line of sight is established between the transmitter and receiver and that no objects encroach in the Fresnel zone.

Calculating Fade Margin

Free space path loss is a major determinant in Rx (received) signal level. Rx signal level, in turn, is a major factor in the system operating margin (fade margin), which is calculated as follows:

$$\text{system operating margin (fade margin) dB} = \text{Rx signal level dB} - \text{Rx sensitivity dB}$$

Thus, fade margin is 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.

Analyzing the RF Environment

An essential element in RF network planning is the analysis of spectrum usage and the strength of the signals that occupy the spectrum you are planning to use. Regardless of how you measure and log or chart the results you find (through the Spectrum Analyzer in SM feature or by using a spectrum analyzer), you should do so:

- at various times of day.
- on various days of the week.
- periodically into the future.

As new RF neighbors move in or consumer devices in your spectrum proliferate, this will keep you aware of the dynamic possibilities for interference with your network.

Mapping RF Neighbor Frequencies

These modules allow you to

- use an SM or an AP that is temporarily transformed into an SM, as a spectrum analyzer.
- view a graphical display that shows power level in RSSI and dBm at 5-MHz increments throughout the frequency band range, regardless of limited selections in the **Custom Radio Frequency Scan Selection List** parameter of the SM.
- select an AP channel that minimizes interference from other RF equipment.

⚠ CAUTION

The following procedure causes the SM to drop any active RF link. If a link is dropped when the spectrum analysis begins, the link can be re-established when either a 15-minute interval has elapsed or the spectrum analyzer feature is disabled.

Analyzing the spectrum

To use the built-in spectrum analyzer functionality of the SM (or AP that is temporarily configured as an SM for spectrum analysis via the AP's GUI) proceed as follows:

Procedure 3 Analyzing the spectrum

1 Predetermine a power source and interface that will work for the SM in the area you want to analyze.

2 Take the SM, power source, and interface device to the area.

3 Access the Tools web page of the SM.
RESULT: The Tools page opens to its Spectrum Analyzer tab.

4 Click **Enable**.
RESULT: The feature is enabled.

5 Click **Enable** again.
RESULT: The system measures RSSI and dBm for each frequency in the spectrum.

6 Travel to another location in the area.

7 Click **Enable** again.
RESULT: The system provides a new measurement of RSSI and dBm for each frequency in the spectrum.

NOTE

Spectrum analysis mode times out 15 minutes after the mode was invoked.

8 Repeat Steps 6 and 7 until the area has been adequately scanned and logged.

As with any other data that pertains to your business, a decision today to put the data into a retrievable database may grow in value to you over time.

> **NOTE**
>
> Wherever you find the measured noise level is greater than the sensitivity of the radio that you plan to deploy, use the noise level (rather than the link budget) for your link feasibility calculations.

Anticipating Reflection of Radio Waves

In the signal path, any object that is larger than the wavelength of the signal can reflect the signal. Such an object can even be the surface of the earth or of a river, bay, or lake. The wavelength of the signal is approximately

- 2 inches for 5.7-GHz signals.

A reflected signal can arrive at the antenna of the receiver later than the non-reflected signal arrives. These two or more signals cause the condition known as multipath. When multipath occurs, the reflected signal cancels part of the effect of the non-reflected signal so, overall, attenuation beyond that caused by link distance occurs. This is problematic at the margin of the link budget, where the standard operating margin (fade margin) may be compromised.

Noting Possible Obstructions in the Fresnel Zone

The Fresnel (pronounced *fre·NEL*) Zone is a theoretical three-dimensional area around the line of sight of an antenna transmission. Objects that penetrate this area can cause the received strength of the transmitted signal to fade. Out-of-phase reflections and absorption of the signal result in signal cancellation.

The foliage of trees and plants in the Fresnel Zone can cause signal loss. Seasonal density, moisture content of the foliage, and other factors such as wind may change the amount of loss. Plan to perform frequent and regular link tests if you must transmit though foliage.

5.7-GHz Channels

Channel selections for the AP in the 5.7-GHz frequency band range depend on whether the AP is deployed in cluster.

5.7-GHz 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 15 5.7-Ghz available channels (in GHz) – single AP

5.735	5.765	5.795	5.825

5.740	5.770	5.800	5.830
5.745	5.775	5.805	5.835
5.750	5.780	5.810	5.840
5.755	5.785	5.815	
5.760	5.790	5.820	

The channels of *adjacent* APs should be separated by at least 10 MHz. However, 20 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:

Table 16 5.7-Ghz non-overlapping channels (in GHz) – AP cluster

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.

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.

Example Channel Plan for OFDM AP Cluster

An example for assignment of frequency channels and sector IDs is provided in the following table. Each frequency is reused on the sector that is at a 180° offset. The entry in the Symbol column of each table refers to the layout in Figure 9 on page 2-24.

See section Network migration planning on page 2-5 for more information on migrating to a PMP 450 network.

> **NOTE**
>
> The operator specifies the sector ID for the module. See the *PMP 450 Administration and Configuration Guide* for more information on configuring this parameter.

Table 17 Example 5.8-GHz OFDM channel assignment by sector

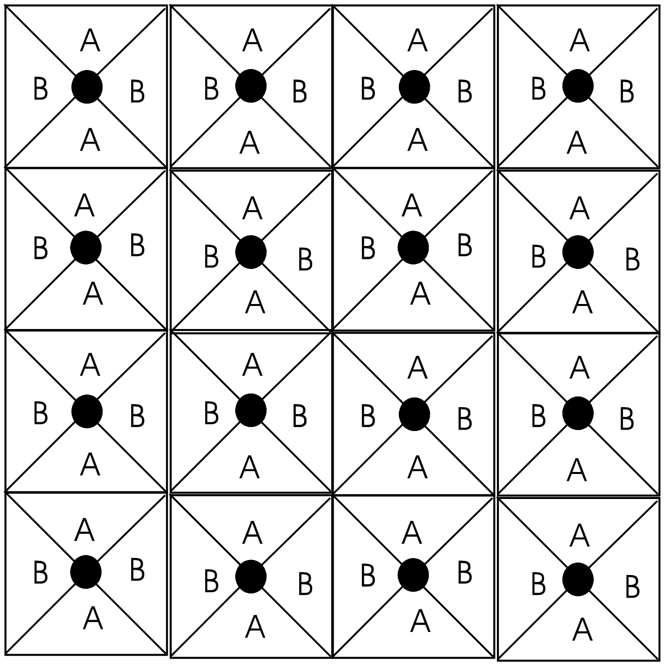
Direction of Access Point Sector	Frequency	Sector ID	Symbol
North (0°)	5.735 GHz	0	A
East (90°)	5.835 GHz	1	B

South (180°)	5.735 GHz	2	A
West (270°)	5.835 GHz	3	B

Multiple OFDM Access Point Clusters

When deploying multiple AP clusters in a dense area, consider aligning the clusters as shown in Figure 9. However, this is only a recommendation. An installation may dictate a different pattern of channel assignments.

Figure 9 Example layout of 16 OFDM Access Point sectors



Selecting Sites for Network Elements

The APs must be positioned

- with hardware that the wind and ambient vibrations cannot flex or move.
- where a tower or rooftop is available or can be erected.
- where a grounding system is available.
- with lightning arrestors to transport lightning strikes away from equipment.
- at a proper height:
    - higher than the tallest points of objects immediately around them (such as trees, buildings, and tower legs).
    - at least 2 feet (0.6 meters) below the tallest point on the tower, pole, or roof (for lightning protection).

- away from high-RF energy sites (such as AM or FM stations, high-powered antennas, and live AM radio towers).
- in line-of-sight paths
  - to the SMs.
  - that will not be obstructed by trees as they grow or structures that are later built.

> **NOTE**
>
> Visual line of sight does not guarantee radio line of sight.

Surveying Sites

Factors to survey at potential sites include

- what pre-existing wireless equipment exists at the site. (Perform spectrum analysis.)
- whether available mounting positions exist near the lowest elevation that satisfies line of site, coverage, and other link criteria.
- whether you will always have the right to decide who climbs the tower to install and maintain your equipment, and whether that person or company can climb at any hour of any day.
- whether you will have collaborative rights and veto power to prevent interference to your equipment from wireless equipment that is installed at the site in the future.
- whether a pre-existing grounding system (path to Protective Earth ⏚) exists, and what is required to establish a path to it.
- who is permitted to run any indoor lengths of cable.

Clearing the Radio Horizon

Because the surface of the earth is curved, higher module elevations are required for greater link distances. This effect can be critical to link connectivity in link spans that are greater than 8 miles (12 km).

To use metric units to find the angle of elevation, use the following formula:

$$h = (d/4.12)^2$$

Where:	Is:
h	minimum height of AP or SM expressed in meters
d	distance between transmitter and receiver expressed in kilometers

To use English standard units to find the angle of elevation, use the following formula:

$$h = (d/1.42)^2$$

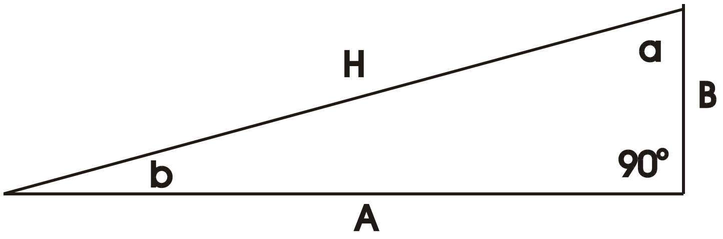
Where:	**Is:**
h	minimum height of AP or SM expressed in feet
d	distance between transmitter and receiver expressed in miles

Calculating the Aim Angles

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 Figure 10).

Figure 10 Variables for calculating angle of elevation (and depression)



Where:	**Is:**
b	angle of elevation
B	vertical difference in elevation
A	horizontal distance between modules

Calculating the Angle of Elevation

To use metric units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{1000A}$$

Where:	**Is:**
B	expressed in meters
A	expressed in kilometers

To use English standard units to find the angle of elevation, use the following formula:

$$\tan b = \frac{B}{5280A}$$

Where:	**Is:**
B	expressed in feet
A	expressed in miles

The angle of depression from the higher module is identical to the angle of elevation from the lower module.

Diagramming Network Layouts

Avoiding Self Interference

The following section includes information maximizing tower performance by minimizing self-interference.

Physical Proximity

An AP cluster on the same tower requires a CMM. The CMM properly synchronizes the *transmit start* times of all modules to prevent interference and desensing of the modules. At closer distances without sync from a CMM, the frame structures cause self interference.

Furthermore, APs on the same tower require that the effects of their differing *receive start* times be mitigated by either

- 100 vertical feet (30 meters) or more and as much spectral separation as possible within the same frequency band range
- the use of the frame calculator to tune the **Downlink Data** parameter in each, so that the receive start time in each is the same

The constraints for collocated modules in the same frequency band range are to avoid self-interference that would occur between them. Specifically, unless the uplink and downlink data percentages match, intervals exist when one is transmitting while the other is receiving, such that the receiving module cannot receive the signal from the far end.

The interference is less a problem during low throughput periods and intolerable during high. Typically, during low throughput periods, sufficient time exists for the far end to retransmit packets lost because of interference from the collocated module.

Spectrum Analysis

You can use an SM as a spectrum analyzer. See Mapping RF Neighbor Frequencies on Page 2-21. Through a toggle of the **Device Type** parameter, you can temporarily transform an AP into an SM to use it as a spectrum analyzer.

SM Automatic Transmit Power Control

The PMP 450 AP automatically sets the transmitter output power in its SMs through a feature named Auto-TPC (Transmit Power Control). The conceptual reason for this feature is OFDM reception in the AP is sensitive to large differences in power levels received from its SMs, and by limiting power levels of close-in SMs the overall RF noise floor is lowered.

Avoiding Other Interference

Where signal strength cannot dominate noise levels, the network experiences

- bit error corrections.
- packet errors and retransmissions.
- lower throughput (because bandwidth is consumed by retransmissions) and high latency (due to resends).

Certain other actions, which may seem to be potential remedies, *do not* resolve high noise level problems:

- *Do not* deploy an omnidirectional antenna.
- *Do not* set the antenna gain above the regulated level.
- *Do not* deploy a band-pass filter in the expectation that this can mitigate co-channel interference.

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.

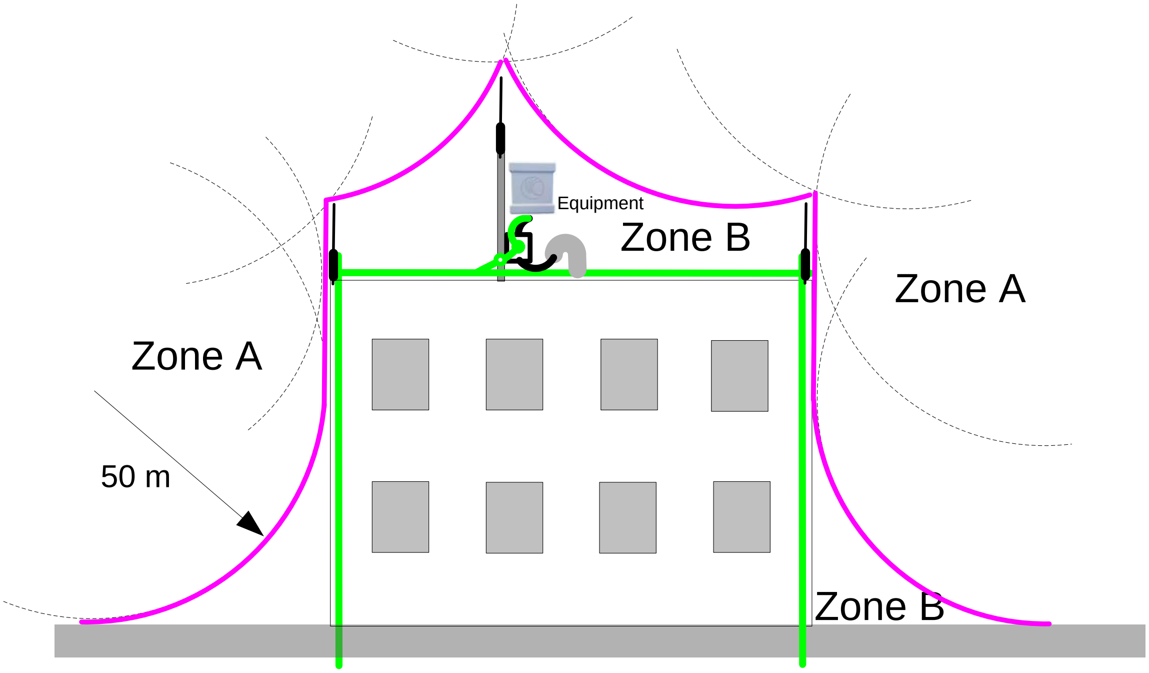
Standards

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 11) 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 11 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:

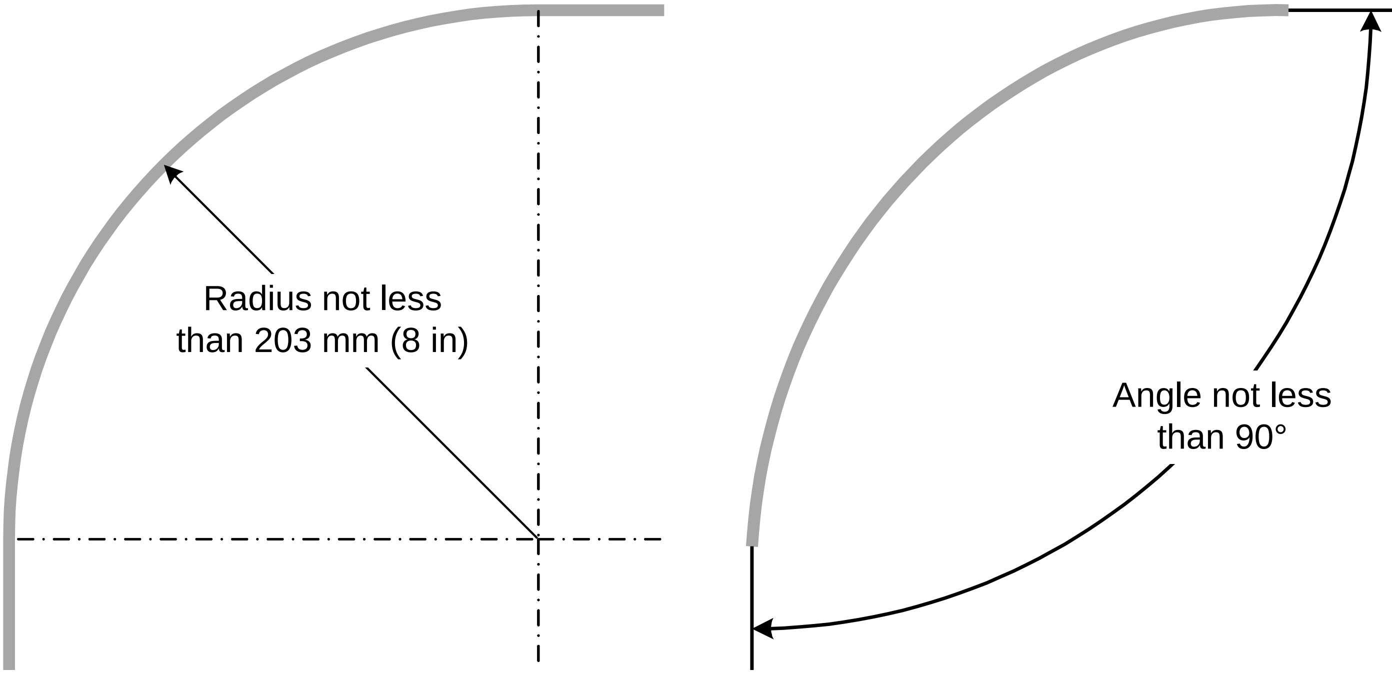
- The equipment must be in 'Zone B' (see Lightning protection zones on page 2-30).
- The AP must be grounded to the supporting structure.
- A surge suppression unit (600SSD) must be installed close to the SM.
- The distance between the SM and 600SSD should be kept to a minimum.
- The drop cable length 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 power 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 12). 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 12 Grounding cable minimum bend radius and angle



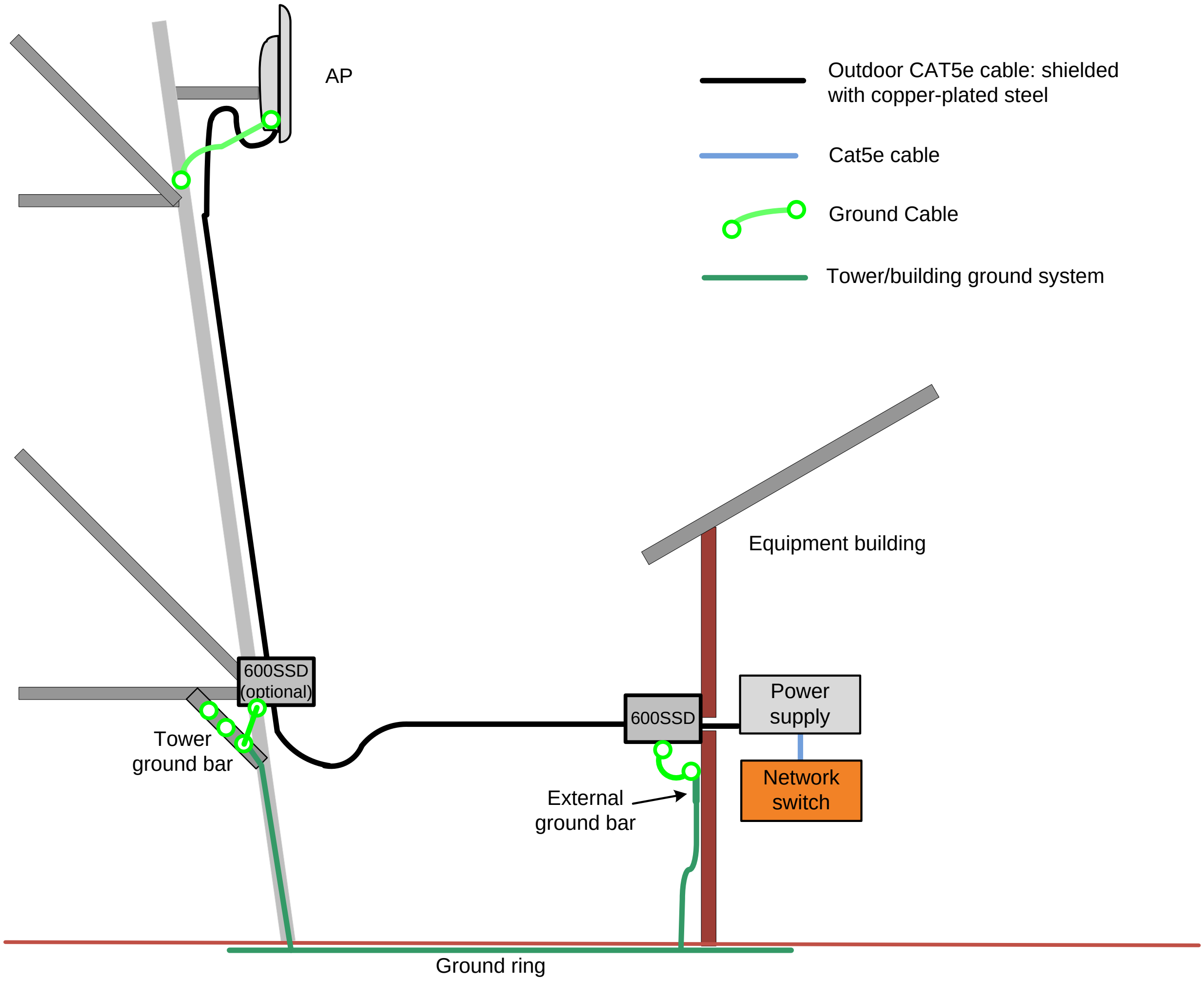
Protection requirements for a mast or tower installation

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.
- A grounding kit must be installed at the bottom of the tower, near the vertical to horizontal transition point. This grounding kit must be bonded to the tower or tower ground bus bar (TGB), if installed.

Schematic examples of mast or tower installations are shown in Figure 13.

Figure 13 Grounding and lightning protection on mast or tower



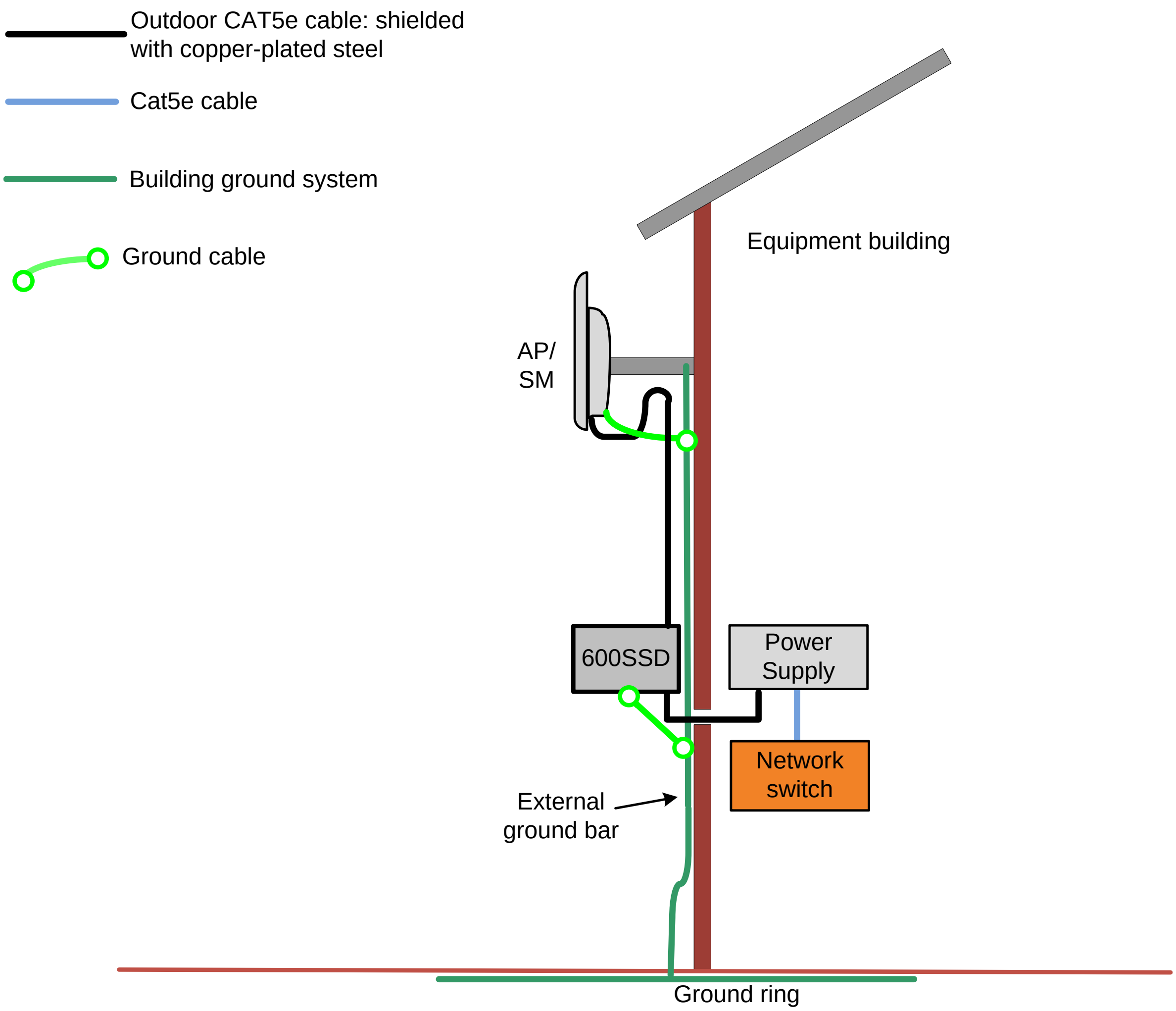
Protection requirements for a wall installation

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 14.

Figure 14 Grounding and lightning protection on wall

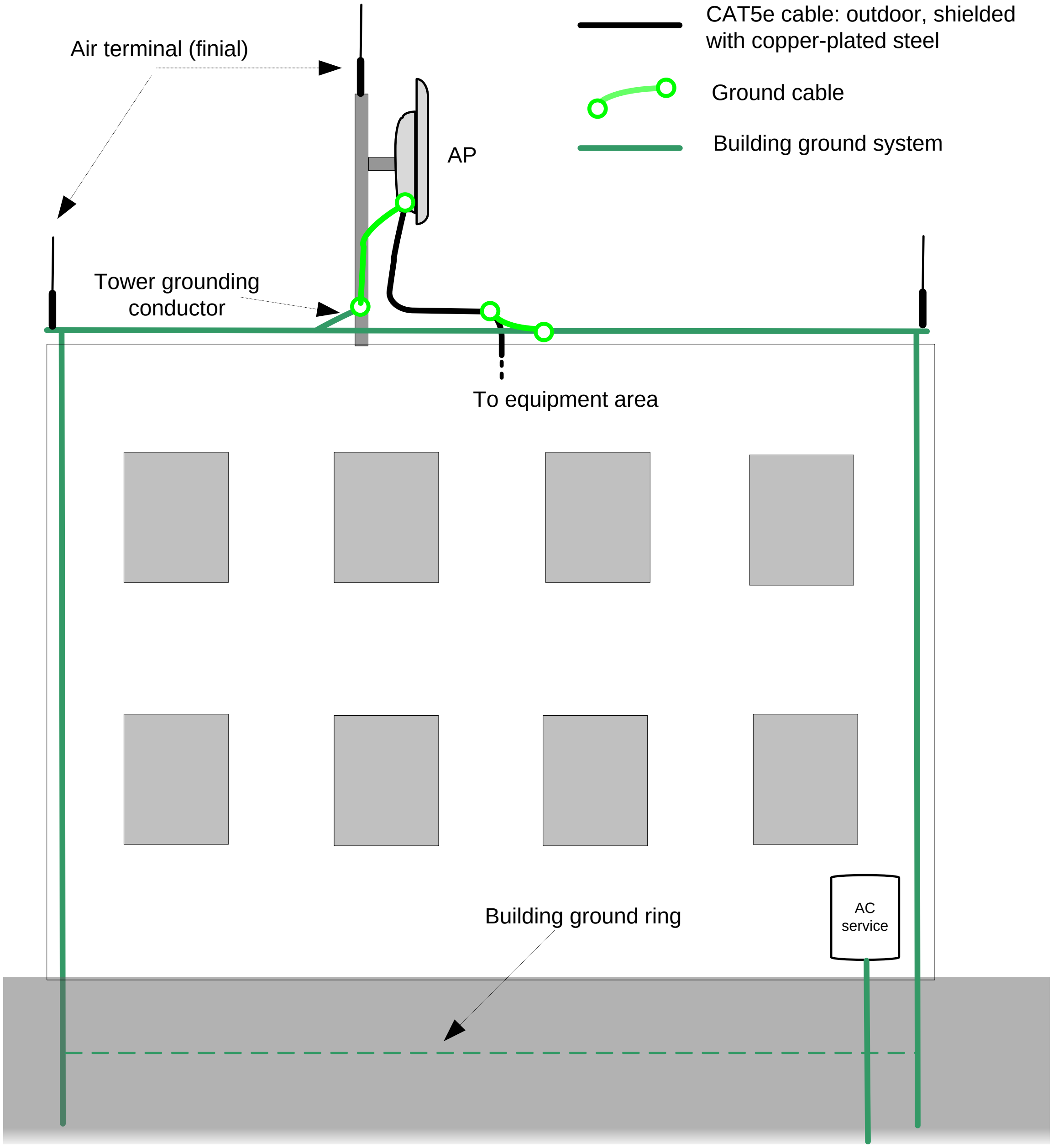


Protection requirements on a high rise building

If the AP is to be mounted on a high rise building, it is likely that cable entry is at roof level (Figure 15) and the equipment room is several floors below (Figure 16). 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 15 Grounding and lightning protection on building

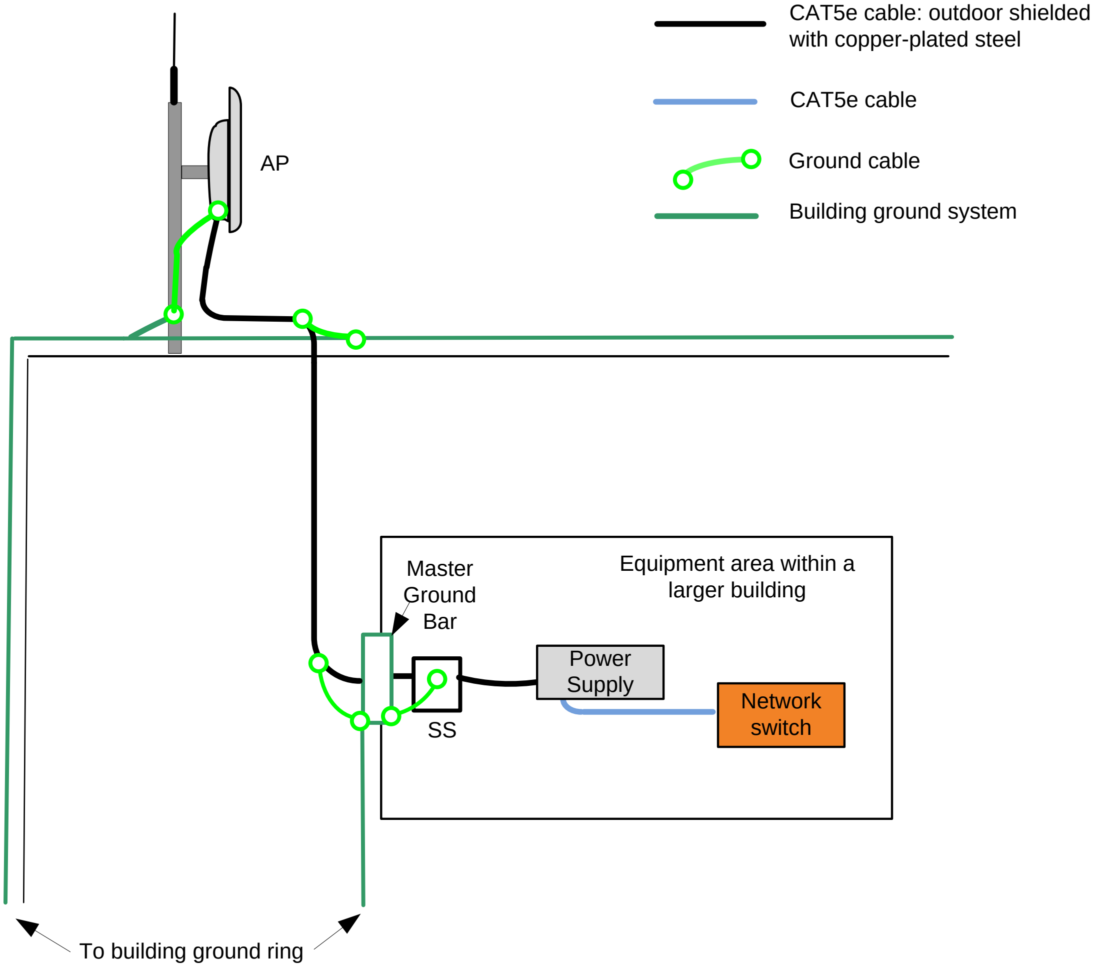


Protection inside a high rise building

The following protection requirements must be observed inside multi-story or high rise buildings (Figure 16):

- 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 16 Grounding and lightning protection inside high building



Configuration options for TDD synchronization

The PMP 450 system uses Time Division Duplexing (TDD) - one channel alternately transmits and receives - rather than using one channel for transmitting and a second channel for receiving. To accomplish TDD, the AP must provide sync to its SMs – it must keep them in sync. Furthermore, collocated APs must be synced together - an unsynchronized AP that transmits during the receive cycle of a collocated AP can prevent that second AP from being able to decode the signals from its SMs. In addition, across a geographical area, APs that can "hear" each other benefit from using a common sync to further reduce self-interference within the network.

GPS Synchronization

The Navigation Satellite Timing and Ranging (NAVSTAR) Global Positioning System (GPS) uses 24 satellites to relay information for precise derivation of position and time.

The cluster management module (CMM) contains a Cambium GPS Receiver. The CMM is a critical element in the operation of the system. At one AP cluster site or throughout an entire wireless system, the CMM provides a GPS timing pulse to each module, synchronizing the network transmission cycles.

The Oncore GPS Receiver tracks eight or more NAVSTAR satellites. The CMM uses the signal from at least four of these satellites to generate a one-second interval clock that has a rise time of 100 nsec. This clock directly synchronizes APs and which, in turn, synchronize the SMs in the network.

The Oncore GPS Receiver also provides

- the latitude and longitude of the GPS antenna (collocated with the CMM)
- the number of satellites that are being tracked
- the number of satellites that are available
- the date
- the time in Universal Coordinated Time (UCT)
- the altitude of the GPS antenna
- other information that can be used to diagnose network problems.

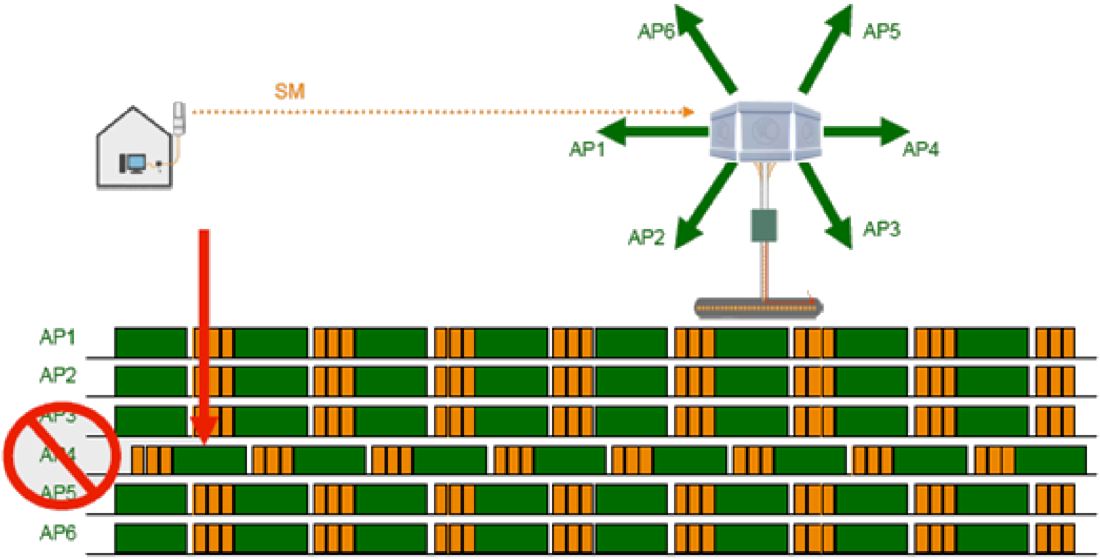
Alternative to GPS Sync

A link can operate without *GPS* sync, but cannot operate without sync. The alternative to GPS sync is to configure the AP in the link to generate a sync pulse to pass to the SM. Depending on the RF environment in which the link operates, this latter alternative may or may not be plausible.

For example, in Figure 17, AP4

- is not synchronized with any of the other APs.
- is transmitting nearby the other APs while they are expecting to receive SM transmissions from a maximum distance.

Figure 17 One unsynchronized AP in cluster



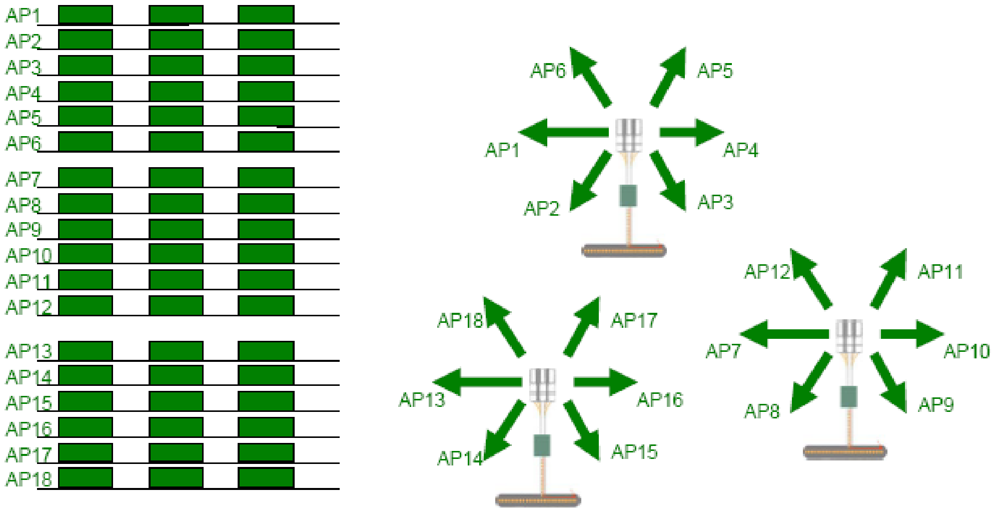
The result is self-interference. In this scenario, the self-interference can be avoided only by synchronizing the TDD transmit cycles of all APs that operate in the same frequency band.

An AP that is isolated by at least 5 miles (8 km) from any other equipment can generate and pass sync pulse without GPS timing and not risk that interference will result from the generated sync. In any other type of link, sync should be derived from GPS timing.

Advantage of GPS Sync

Although the embedded timing generation capability of the AP keeps a precise clock, no trigger exists to start the clock at the same moment in each AP of a cluster. So, the individual AP can synchronize communications between itself and registered SMs, but cannot synchronize itself with other modules, except by GPS timing (shown in Figure 18).

Figure 18 GPS timing throughout the network



Mounting the GPS receiver module on the equipment building

If mounting the GPS receiver on the equipment building, select a position on the wall that meets the following requirements:

- It must be below the roof height of the equipment building or below the height of any roof-mounted equipment (such as air conditioning plant).
- It must be below the lightning air terminals.
- It must not project more than 600mm (24 inches) from the wall of the building.

If these requirements cannot all be met, then the module must be mounted on a metal tower or mast.

Mounting the GPS receiver module on a metal tower or mast

If mounting the GPS receiver module on a metal tower or mast, select a position that meets the following requirements:

- It must not be mounted any higher than is necessary to receive an adequate signal from four GPS satellites.
- It must be protected by a nearby lightning air terminal that projects farther out from the tower than the GPS receiver module.
- It must meet all the requirements stated in Protection requirements for a mast or tower installation on page 2-32.

Data network planning

This section describes factors to be considered when planning PMP 450 data networks.

Understanding addresses

A basic understanding of Internet Protocol (IP) address and subnet mask concepts is required for engineering your IP network.

IP address

The IP address is a 32-bit binary number that has four parts (octets). This set of four octets has two segments, depending on the class of IP address. The first segment identifies the network. The second identifies the hosts or devices on the network. The subnet mask marks a boundary between these two sub-addresses.

Dynamic or static addressing

For any computer to communicate with a module, the computer must be configured to either

- use DHCP (Dynamic Host Configuration Protocol). In this case, when not connected to the network, the computer derives an IP address on the 169.254 network within two minutes.
- have an assigned static IP address (for example, 169.254.1.5) on the 169.254 network.

NOTE

If an IP address that is set in the module is not the 169.254.x.x network address, then the network operator must assign the computer a static IP address in the same subnet.

When a DHCP server is not found

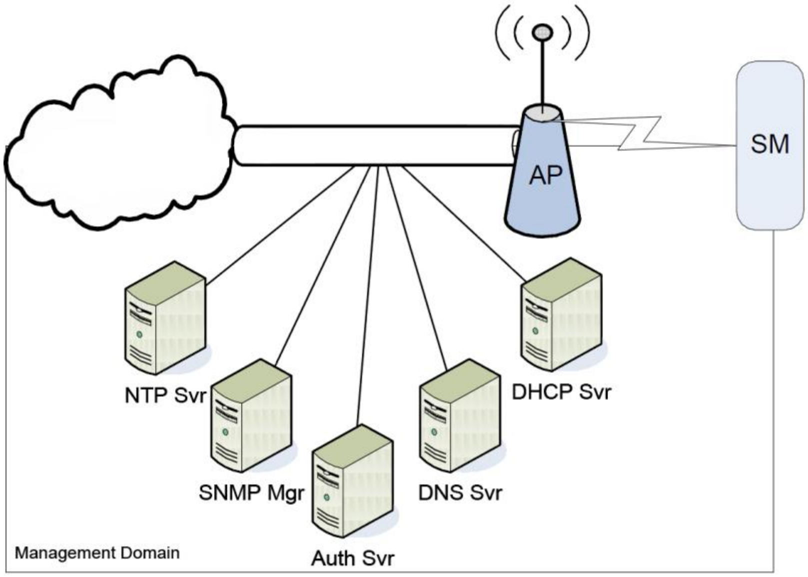
To operate on a network, a computer requires an IP address, a subnet mask, and possibly a gateway address. Either a DHCP server automatically assigns this configuration information to a computer on a network or an operator must input these items.

When a computer is brought on line and a DHCP server is not accessible (such as when the server is down or the computer is not plugged into the network), Microsoft and Apple operating systems default to an IP address of 169.254.x.x and a subnet mask of 255.255.0.0 (169.254/16, where /16 indicates that the first 16 bits of the address range are identical among all members of the subnet).

DNS Client

The DNS Client is used to resolve names of management servers within the operator's management domain (see Figure 19). This feature allows hostname configuration for NTP servers, Authorization Servers, DHCP relay servers, and SNMP trap servers. Operators may choose to either enter in the FQDN (Fully Qualified Domain Name) for the host name or to manually enter the IP addresses of the servers.

Figure 19 Cambium network management domain



Network Address Translation (NAT)

NAT, DHCP Server, DHCP Client, and DMZ in SM

The system provides NAT (network address translation) for SMs in the following combinations of NAT and DHCP (Dynamic Host Configuration Protocol):

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

NAT

NAT isolates devices connected to the Ethernet/wired side of an SM from being seen directly from the wireless side of the SM. With NAT enabled, the SM has an IP address for transport traffic (separate from its address for management), terminates transport traffic, and allows you to assign a range of IP addresses to devices that are connected to the Ethernet/wired side of the SM.

In the Cambium system, NAT supports many protocols, including HTTP, ICMP (Internet Control Message Protocols), and FTP (File Transfer Protocol). For virtual private network (VPN) implementation, L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) and PPTP (Point to Point Tunneling Protocol) are supported.

DHCP

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

In conjunction with the NAT features, each SM provides

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

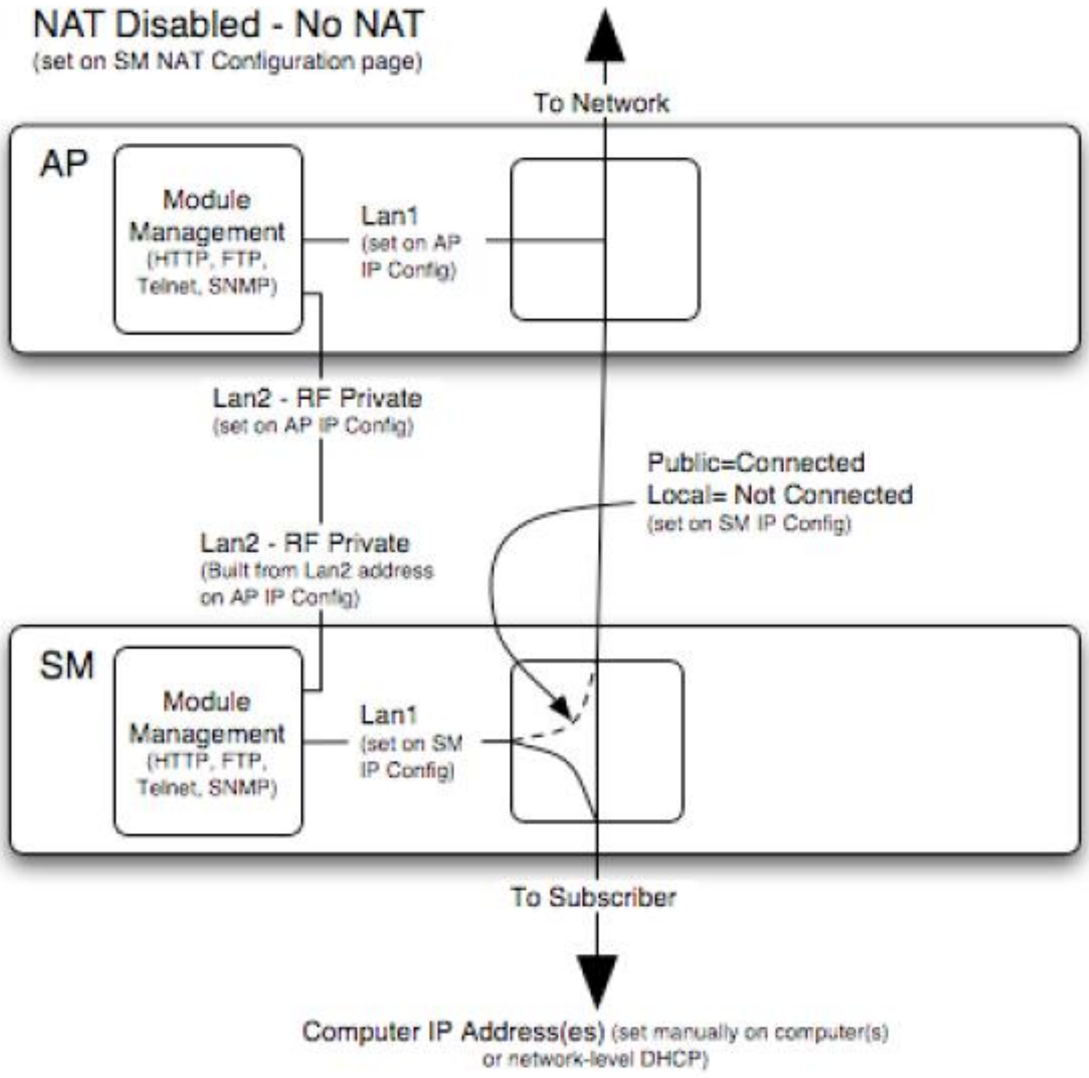
DMZ

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

NAT Disabled

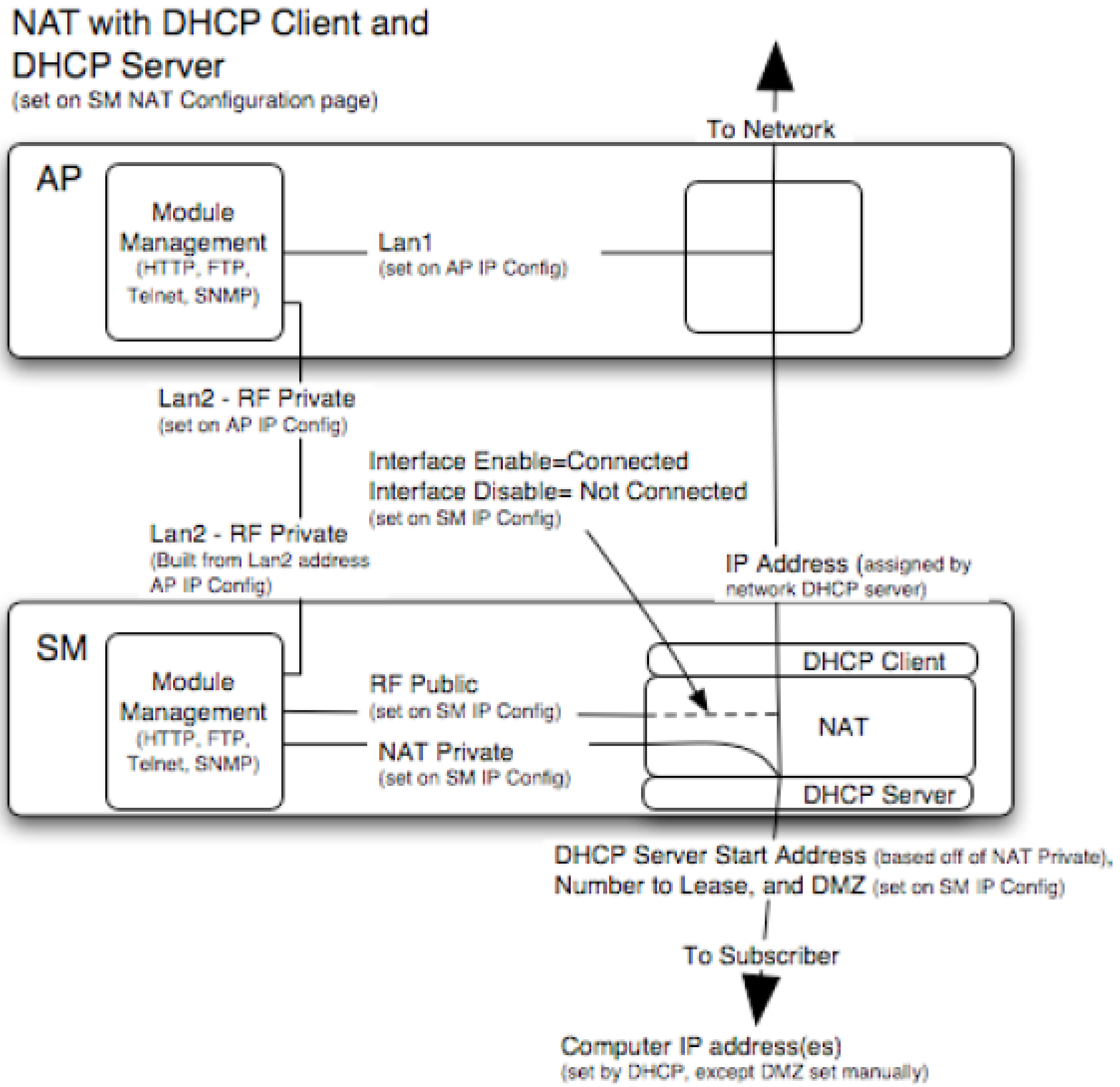
The NAT Disabled implementation is illustrated in Figure 20.

Figure 20 NAT disabled implementation


NAT Disabled - No NAT
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Public=Connected
Local= Not Connected
(set on SM IP Config)
Lan2 - RF Private (Built from Lan2 address on AP IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s) or network-level DHCP)

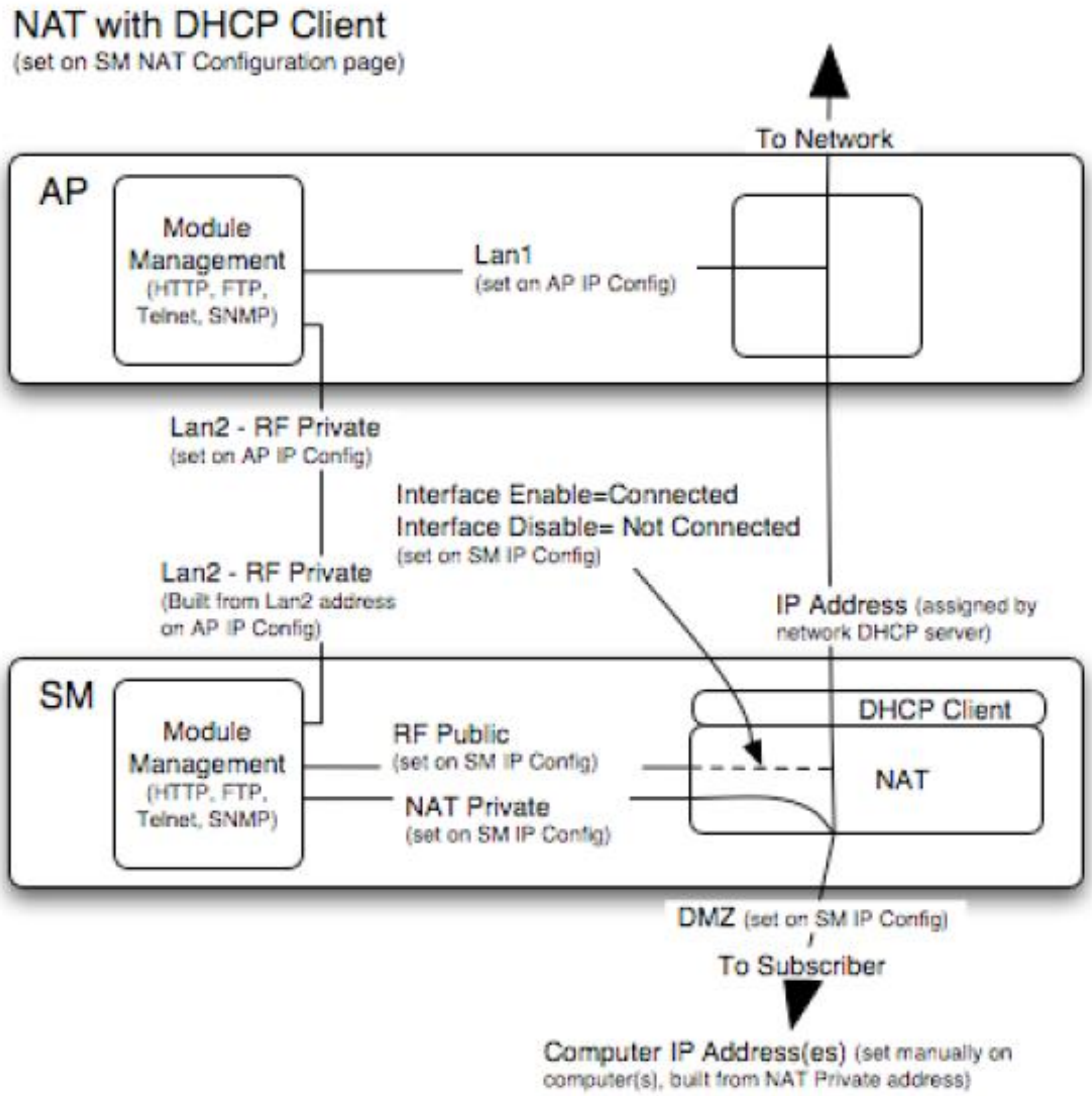
NAT with DHCP Client and DHCP Server

Figure 21 NAT with DHCP client and DHCP server implementation


NAT with DHCP Client and DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1 (set on AP IP Config)
Lan2 - RF Private (set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private (Built from Lan2 address AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public (set on SM IP Config)
NAT Private (set on SM IP Config)
DHCP Client
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private), Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es) (set by DHCP, except DMZ set manually)

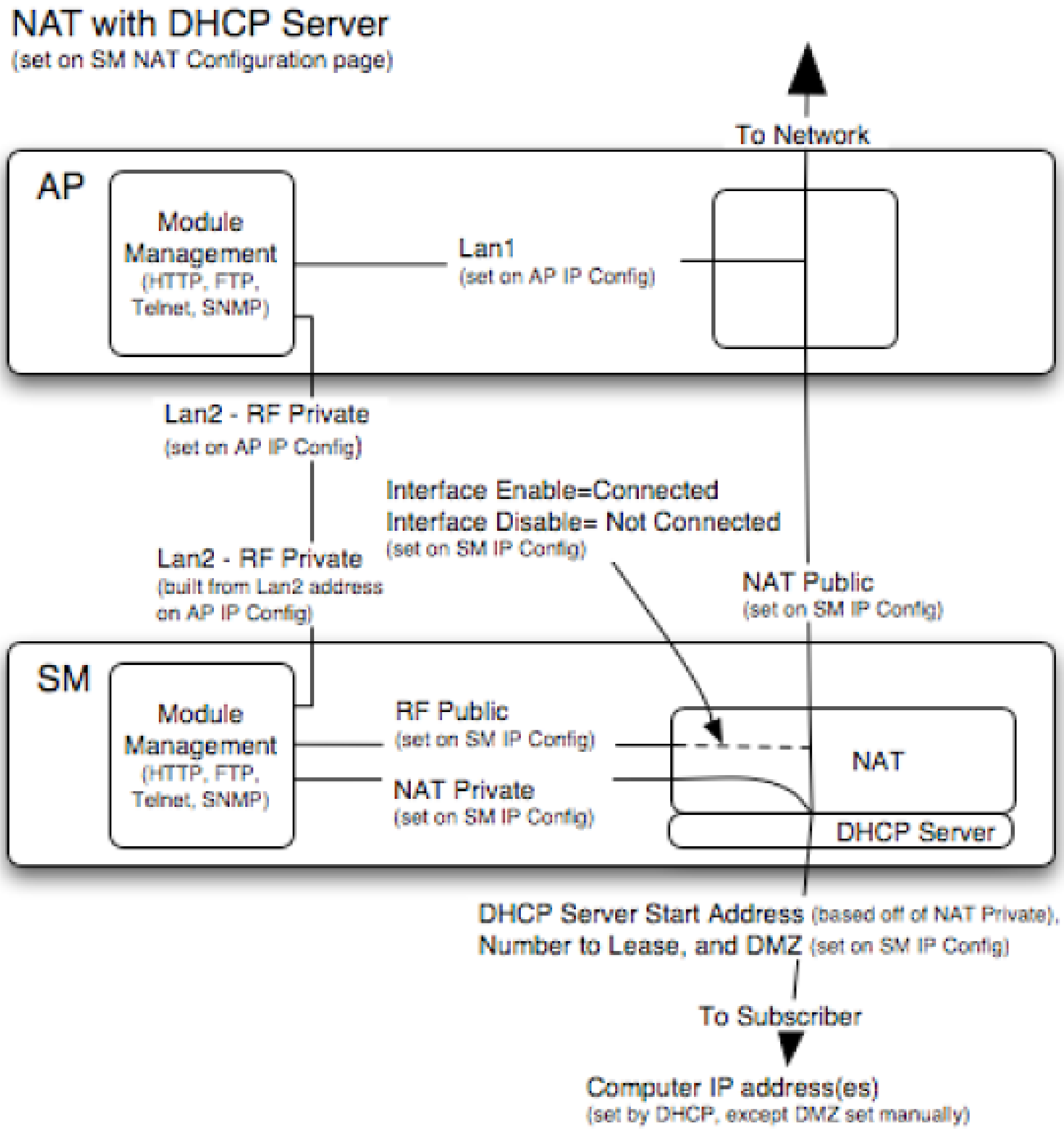
NAT with DHCP Client

Figure 22 NAT with DHCP client implementation


NAT with DHCP Client
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(Built from Lan2 address on AP IP Config)
IP Address (assigned by network DHCP server)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
DHCP Client
RF Public
(set on SM IP Config)
NAT
NAT Private
(set on SM IP Config)
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

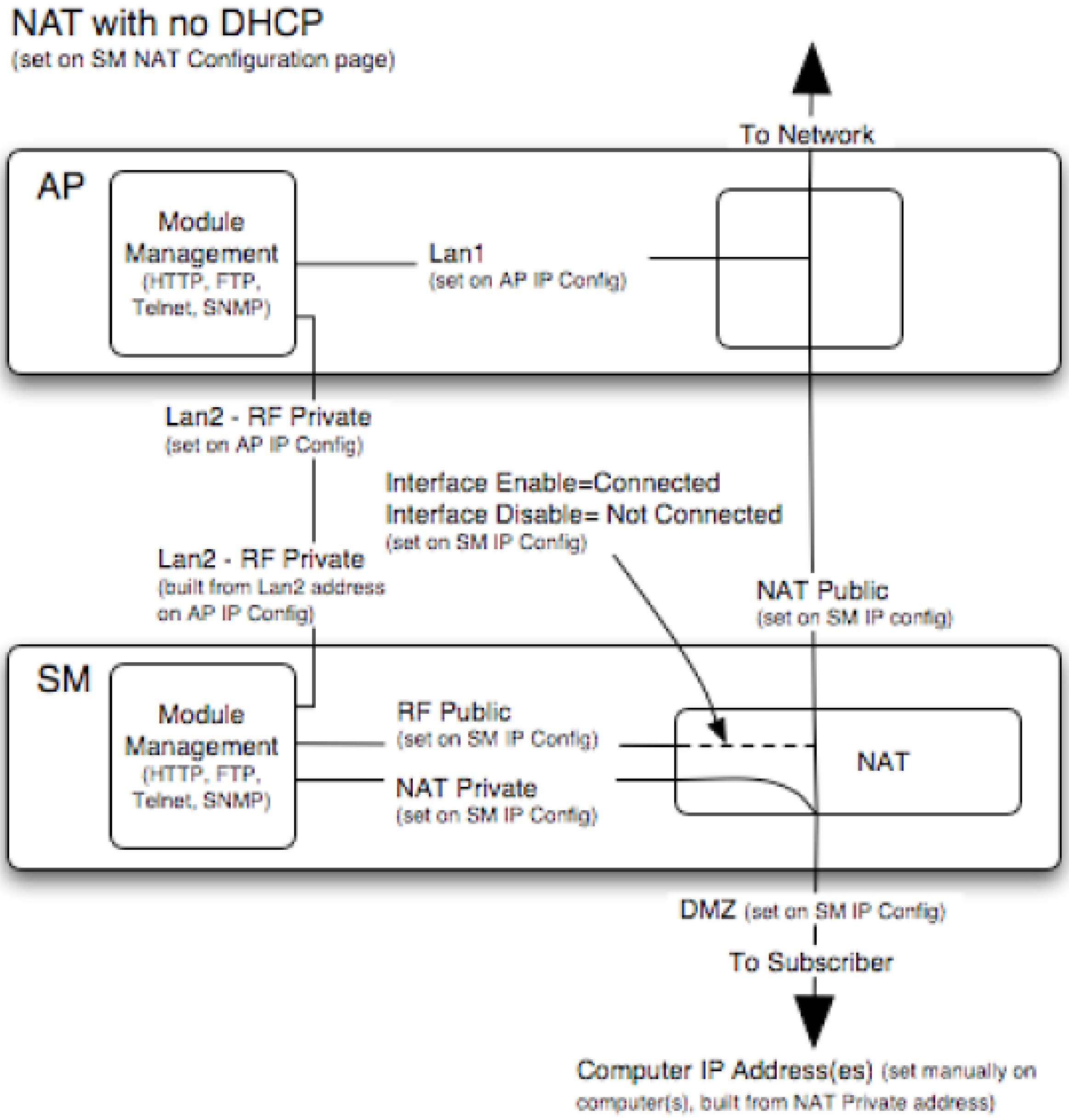
NAT with DHCP Server

Figure 23 NAT with DHCP server implementation


NAT with DHCP Server
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(built from Lan2 address on AP IP Config)
NAT Public
(set on SM IP Config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
NAT
DHCP Server
DHCP Server Start Address (based off of NAT Private), Number to Lease, and DMZ (set on SM IP Config)
To Subscriber
Computer IP address(es)
(set by DHCP, except DMZ set manually)

NAT without DHCP

Figure 24 NAT without DHCP implementation


NAT with no DHCP
(set on SM NAT Configuration page)
To Network
AP
Module Management (HTTP, FTP, Telnet, SNMP)
Lan1
(set on AP IP Config)
Lan2 - RF Private
(set on AP IP Config)
Interface Enable=Connected
Interface Disable= Not Connected
(set on SM IP Config)
Lan2 - RF Private
(built from Lan2 address on AP IP Config)
NAT Public
(set on SM IP config)
SM
Module Management (HTTP, FTP, Telnet, SNMP)
RF Public
(set on SM IP Config)
NAT Private
(set on SM IP Config)
NAT
DMZ (set on SM IP Config)
To Subscriber
Computer IP Address(es) (set manually on computer(s), built from NAT Private address)

NAT and VPNs

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

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

Developing an IP addressing scheme

Network elements are accessed through IP Version 4 (IPv4) addressing.
A proper IP addressing method is critical to the operation and security of a network.

Each module requires an IP address on the network. This IP address is for only management purposes. For security, you should either

- assign an unroutable IP address.
- assign a routable IP address only if a firewall is present to protect the module.

You will assign IP addresses to computers and network components by either *static* or *dynamic* IP addressing. You will also assign the appropriate subnet mask and network gateway to each module.

Address Resolution Protocol

As previously stated, the MAC address identifies a module in

- communications between modules.
- the data that modules store about each other.

The IP address is essential for data delivery through a router interface. Address Resolution Protocol (ARP) correlates MAC addresses to IP addresses.

For communications to outside the network segment, ARP reads the network gateway address of the router and translates it into the MAC address of the router. Then the communication is sent to MAC address (physical network interface card) of the router.

For each router between the sending module and the destination, this sequence applies. The ARP correlation is stored until the ARP cache times out.

Allocating subnets

The subnet mask is a 32-bit binary number that filters the IP address. Where a subnet mask contains a bit set to 1, the corresponding bit in the IP address is part of the network address.

Example IP address and subnet mask

In Figure 25 Example of IP address in Class B subnet the first 16 bits of the 32-bit IP address identify the network:

Figure 25 Example of IP address in Class B subnet

	Octet 1	Octet 2	Octet 3	Octet 4
IP address 169.254.1.1	10101001	11111110	00000001	00000001
Subnet mask 255.255.0.0	11111111	11111111	00000000	00000000

In this example, the network address is 169.254, and 2^{16} (65,536) hosts are addressable.

Selecting non-routable IP addresses

The factory default assignments for network elements are

- unique MAC address
- IP address of 169.254.1.1
- subnet mask of 255.255.0.0
- network gateway address of 169.254.0.0

For each radio and CMMmicro and CMM4, assign an IP address that is both consistent with the IP addressing plan for your network and cannot be accessed from the Internet. IP addresses within the following ranges are not routable from the Internet, regardless of whether a firewall is configured:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

You can also assign a subnet mask and network gateway for each CMMmicro and CMM4.

Translation bridging

Optionally, you can configure the AP to change the source MAC address in every packet it receives from its SMs to the MAC address of the SM that bridged the packet, before forwarding the packet toward the public network. If you do, then

- not more than 10 IP devices at any time are valid to send data to the AP from behind the SM.
- the AP populates the Translation Table tab of its Statistics web page, displaying the MAC address and IP address of all the valid connected devices.
- each entry in the Translation Table is associated with the number of minutes that have elapsed since the last packet transfer between the connected device and the SM.

- if 10 are connected, and another attempts to connect
  - and no Translation Table entry is older than 255 minutes, the attempt is ignored.
  - and an entry is older than 255 minutes, the oldest entry is removed and the attempt is successful.
- the **Send Untranslated ARP** parameter in the General tab of the Configuration page can be
  - disabled, so that the AP will overwrite the MAC address in Address Resolution Protocol (ARP) packets before forwarding them.
  - enabled, so that the AP will forward ARP packets regardless of whether it has overwritten the MAC address.

This is the **Translation Bridging** feature, which you can enable in the General tab of the Configuration web page in the AP. When this feature is disabled, the setting of the **Send Untranslated ARP** parameter has no effect, because all packets are forwarded untranslated (with the source MAC address intact).

See Address Resolution Protocol on Page 2-49.

Engineering VLANs

The radios support VLAN functionality as defined in the 802.1Q (*Virtual LANs*) specification, except for the following aspects of that specification:

- the following protocols:
  - Generic Attribute Registration Protocol (GARP) GARV
  - Spanning Tree Protocol (STP)
  - Multiple Spanning Tree Protocol (MSTP)
  - GARP Multicast Registration Protocol (GMRP)
- embedded source routing (ERIF) in the 802.1Q header
- multicast pruning
- flooding unknown unicast frames in the downlink

As an additional exception, the AP *does not* flood downward the unknown unicast frames to the SM.

A VLAN configuration in Layer 2 establishes a logical group within the network. Each computer in the VLAN, regardless of initial or eventual physical location, has access to the same data. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.

Special case VLAN numbers

This system handles special case VLAN numbers according to IEEE specifications:

Table 18 Special case VLAN IDs

VLAN Number	Purpose	Usage Constraint
0	These packets have 802.1p priority, but are otherwise handled as untagged.	Should not be used as a management VLAN.
1	Although not noted as special case by IEEE specifications, these packets identify traffic that was untagged upon ingress into the SM and should remain untagged upon egress. This policy is hard-coded in the AP.	Should not be used for system VLAN traffic.
4095	This VLAN is reserved for internal use.	Should not be used at all.

SM membership in VLANs

With the supported VLAN functionality, the radios determine bridge forwarding on the basis of not only the destination MAC address, but also the VLAN ID of the destination. This provides flexibility in how SMs are used:

- Each SM can be a member in its own VLAN.
- Each SM can be in its own broadcast domain, such that only the radios that are members of the VLAN can see broadcast and multicast traffic to and from the SM.
- The network operator can define a work group of SMs, regardless of the AP(s) to which they register.

PMP modules provide the VLAN frame filters that are described in Table 19.

Table 19 VLAN filters in point-to-multipoint modules

Where VLAN is active, if this parameter value is selected …	then a frame is discarded if…		because of this VLAN filter in the software:
	entering the bridge/ NAT switch through…		
	Ethernet…	TCP/IP…	
any combination of VLAN parameter settings	with a VID not in the membership table		Ingress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Ingress

Allow Frame Types: **Tagged Frames Only**	with no 802.1Q tag		Only Tagged
Allow Frame Types: **Untagged Frames Only**	with an 802.1Q tag, regardless of VID		Only Untagged
Local SM Management: **Disable** in the SM, or **All Local SM Management:** **Disable** in the AP	with an 802.1Q tag and a VID in the membership table		Local SM Management
	leaving **the bridge/ NAT switch through…**		
	Ethernet…	**TCP/IP…**	
any combination of VLAN parameter settings	with a VID not in the membership table		Egress
any combination of VLAN parameter settings		with a VID not in the membership table	Local Egress

Priority on VLANs (802.1p)

The radios can prioritize traffic based on the eight priorities described in the IEEE 802.1p specification. When the high-priority channel is enabled on an SM, regardless of whether VLAN is enabled on the AP for the sector, packets received with a priority of 4 through 7 in the 802.1p field are forwarded onto the high-priority channel.

Operators may configure priority precedence as 802.1p Then Diffserv (Default) or Diffserv Then 802.1p. Since these priority precedence configurations are independent between the AP and SM, this setting must be configured on both the AP and the SM to ensure that the precedence is adhered to by both sides of the link.

VLAN settings can also cause the module to convert received non-VLAN packets into VLAN packets. In this case, the 802.1p priority in packets leaving the module is set to the priority established by the DiffServ configuration.

If you enable VLAN, *immediately* monitor traffic to ensure that the results are as desired. For example, high-priority traffic may block low-priority.

Q-in-Q DVLAN (Double-VLAN) Tagging (802.1ad)

PMP modules can be configured with 802.1ad Q-in-Q DVLAN (Double-VLAN) tagging which is a way for an operator to put an 802.1Q VLAN inside of an 802.1ad VLAN. A nested VLAN, which is the original 802.1Q tag and a new second 802.1ad tag, allows for bridging of VLAN traffic across a network and segregates the broadcast domains of 802.1Q VLANs. Q-in-Q can be used with PPPoE and/or NAT.

The 802.1ad standard defines the S-VLAN as the Service Provider VLAN and the C-VLAN as the customer VLAN. The radio software does 2 layer Q-in-Q whereby the C-VLAN is the 802.1Q tag and the S-VLAN is the second layer Q tag as shown in Table 20.

Table 20 Q-in-Q Ethernet frame

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

The 802.1ad S-VLAN is the outer VLAN that is configurable on the Configuration => VLAN web page of the AP. The Q-in-Q EtherType parameter is configured with a default EtherType of 0x88a8 in addition to four alternate EtherType's that can be configured to aid in interoperability with existing networks that use a different EtherType than the default.

The C-VLAN is the inner VLAN tag, which is the same as 802.1Q. As a top level concept, this operates on the outermost tag at any given time, either "pushing" a tag on or "popping" a tag off. This means packets will at most transition from an 802.1Q frame to an 801.ad frame (with a tag "pushed" on) or an untagged 802.1 frame (with the tag "popped" off. Similarly, for an 802.1ad frame, this can only transition from an 802.1ad frame to an 802.1Q frame (with the tag "popped" off) since the radio software only supports 2 levels of tags.

Security planning

This section describes how to plan for PMP 450 networks to operate in secure mode.

Isolating APs from the Internet

Ensure that the IP addresses of the APs in your network

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

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

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

Managing module access by passwords

Adding a user for access to a module

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

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

⚠ CAUTION

If you use Wireless Manager or BAM (Bandwidth and Authentication Manager), do not delete the root account from any module. If you use an NMS that communicates with modules through SNMP, do not delete the root account from any module unless you first can confirm that the NMS does not rely on the root account for access to the modules.

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

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

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

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

Table 21 Identity-based user account permissions - AP

Menu Option	**Menu Tab**	**ADMIN**	**INSTALLER**	**TECH**
Home	General Status	🟥	🟩	🟪
	Session Status	🟥	🟩	🟪
	Remote Subscribers	🟥	🟩	🟪
	Event Log	🟥	🟩	🟪
	Engineering Event Log			
	Network Interface	🟥	🟩	🟪
	Layer2 Neighbors	🟥	🟩	
	ADI Registers			
Configuration	General	🟥	🟩	🟪
	IP	🟥	🟩	🟪
	Radio	🟥	🟩	🟪
	SNMP	🟥	🟩	🟪
	Quality of Service (QoS)	🟥	🟩	🟪
	Security	🟥	🟩	
	Time	🟥	🟩	
	VLAN	🟥	🟩	
	VLAN Membership	🟥	🟩	
	DiffServ	🟥	🟩	
	Protocol Filtering	🟥	🟩	
	Port Configuration	🟥	🟩	
	Syslog	🟥	🟩	

	Unit Settings	🟥	🟩	
Statistics	Scheduler	🟥		
	NI Buffer			
	SM Registration Failures	🟥		
	Bridge Control Block	🟥		
	Bridging Table	🟥	🟩	🟪
	Ethernet	🟥		
	Socket			
	Radio	🟥		
	VLAN	🟥		
	Data VC	🟥		
	Throughput	🟥		
	Filter	🟥		
	HTTP Proxy			
	SNMP Proxy			
	Web GUI Engine			
	ARP	🟥	🟩	🟪
	Overload	🟥		
	DHCP Relay	🟥		
	Pass Through Statistics	🟥		
	DNS Statistics	🟥		
	HTTP Tunnel Statistics			
	Syslog Statistics			
Tools	Link Capacity Test	🟥	🟩	🟪
	Combo Frame Calculator	🟥	🟩	🟪
	OFDM Frame Calculator	🟥	🟩	🟪
	Packet Capture Configuration			
	Packet Dump			
	Stale Buffer Dump			
	NiBuffers Dump			
	Subscriber Configuration	🟥		
	Feature Key Information			
	Program Feature Keys			
	Temperature History			
	DFS FPGA Long Pulse State History			
	DFS FPGA Short Pulse State History			
	DFS RSSI History			
	Link Status	🟥	🟩	🟪
	Remote Spectrum Analyzer	🟥	🟩	🟪
	Sessions	🟥		

	DNS Test	🟥	🟩	🟪
Engineering	Engineer Configuration			
	Board Status			
	Burnflash			
Logs	AP Auto Update Logs			
	AP Sessions	🟥		
	AP Authentication State Machine Log	🟥		
	AP Authorization State Machine Log	🟥		
	Link Test Log			
	Top Level RF State Machine			
	RF GPS State Machine			
	RF Sync State Machine			
	RF Calibration			
	NiBuf Monitor Log			
	Web Server Event Log			
	Regulatory Log			
	EAP Radius Log	🟥		
Accounts	User Authentication And Access Tracking	🟥	🟩	
	Change User Password	🟥	🟩	🟪
	Add User	🟥		
	Delete User	🟥		
Quick Start	Quick Start	🟥	🟩	🟪
	Region Settings	🟥	🟩	🟪
	Radio Carrier Frequency	🟥	🟩	🟪
	Synchronization	🟥	🟩	🟪
	LAN IP Address	🟥	🟩	🟪
	Review and Save Configuration	🟥	🟩	🟪
Copyright	Copyright Notices	🟥	🟩	🟪
Logoff		🟥	🟩	🟪

Table 22 Identity-based user account permissions - SM

Menu	**Menu Tab**	**ADMIN**	**INSTALLER**	**TECH**
Home	General Status	🟥	🟩	🟪
	Event Log	🟥	🟩	🟪
	Engineering Event Log			
	Network Interface	🟥	🟩	🟪
	Layer2 Neighbors	🟥	🟩	

	ADI Registers			
Configuration	General	🟥	🟩	🟪
	IP	🟥	🟩	🟪
	Radio	🟥	🟩	🟪
	SNMP	🟥	🟩	🟪
	Quality of Service (QoS)	🟥	🟩	🟪
	Security	🟥	🟩	
	VLAN	🟥	🟩	
	VLAN Membership	🟥	🟩	
	DiffServ	🟥	🟩	
	Protocol Filtering	🟥	🟩	
	Port Configuration	🟥	🟩	
	NAT	🟥	🟩	
	PPPoE	🟥	🟩	
	NAT Port Mapping	🟥	🟩	
	Syslog	🟥	🟩	
	Unit Settings	🟥	🟩	
Statistics	Scheduler	🟥		
	NI Buffer			
	Bridge Control Block	🟥		
	Bridging Table	🟥	🟩	🟪
	Translation Table	🟥	🟩	🟪
	Ethernet	🟥		
	Socket			
	Radio	🟥		
	VLAN	🟥		
	Data VC	🟥		
	Filter	🟥		
	NAT Stats	🟥		
	NAT DHCP	🟥		
	Web GUI Engine			
	ARP	🟥	🟩	🟪
	Overload	🟥		
	PPPoE Statistics	🟥		
	Peer Statistics	🟥		
	DNS Statistics	🟥		
	HTTP Tunnel Statistics			
	Syslog Statistics	🟥		
Tools	Spectrum Analyzer	🟥	🟩	🟪
	Alignment	🟥	🟩	🟪

	Link Capacity Test	🟥	🟩	🟪
	AP Evaluation	🟥	🟩	🟪
	Combo Frame Calculator	🟥	🟩	🟪
	OFDM Frame Calculator	🟥	🟩	🟪
	BER Results	🟥	🟩	🟪
	Packet Capture Configuration			
	Packet Dump			
	Stale Buffer Dump			
	NiBuffers Dump			
	BER Results			
	Feature Key Information			
	Loopback Test (Factory)			
	Program Feature Keys			
	Temperature History			
	DFS FPGA Long Pulse State History			
	DFS FPGA Short Pulse State History			
	DFS RSSI History			
	Alignment Tool	🟥	🟩	🟪
	Link Status	🟥	🟩	🟪
	DNS Test	🟥	🟩	🟪
Engineering	Engineer Configuration			
	Board Status			
	Burnflash			
Logs	NAT Table	🟥		
	SM Communication Center			
	SM AutoUpdate			
	Link Test Log			
	Top Level RF State Machine			
	RF GPS State Machine			
	RF Sync State Machine			
	RF Scanning			
	RF Calibration			
	NiBuf Monitor Log			
	NAT DHCP Event			
	NAT DHCP Client State Machine			
	NAT DHCP Server State Machine			
	SM Session	🟥		
	SM Authentication	🟥		
	SM Authorization	🟥		
	SM Sync			

	Web Server Event Log			
	PPPoE Session Log	🟥		
	EAP Radius Log	🟥		
Accounts	User Authentication and Access Tracking	🟥	🟩	
	Change User Password	🟥	🟩	🟪
	Add User	🟥		
	Delete User	🟥		
PDA	Quick Status	🟥	🟩	🟪
	Spectrum Results (PDA)	🟥	🟩	🟪
	Information	🟥	🟩	🟪
	AP Evaluation	🟥	🟩	🟪
	AIM	🟥	🟩	🟪
Copyright	Copyright Notices	🟥	🟩	🟪
Logoff		🟥	🟩	🟪

Filtering protocols and ports

You can filter (block) specified protocols and ports from leaving the AP and SM and entering the network. This protects the network from both intended and inadvertent packet loading or probing by network users. By keeping the specified protocols or ports off the network, this feature also provides a level of protection to users from each other.

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

Port Filtering with NAT Enabled

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

- To block a subscriber from using FTP, you can filter Ports 20 and 21 (the FTP ports) for both the TCP and UDP protocols.
- To block a subscriber from access to SNMP, you can filter Ports 161 and 162 (the SNMP ports) for both the TCP and UDP protocols.
  NOTE: In only the SNMP case, filtering occurs before the packet interacts with the protocol stack.

Protocol and Port Filtering with NAT Disabled

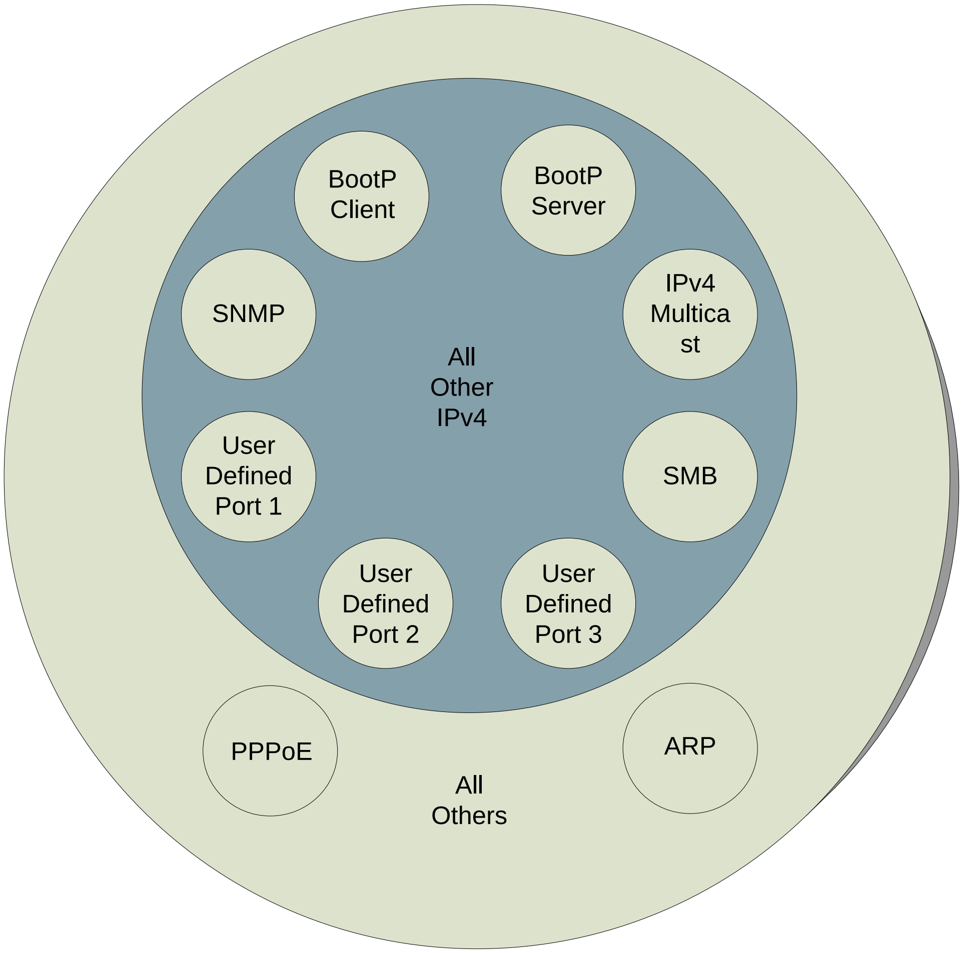
Where NAT is disabled on the SM, you can filter both protocols and the three user-defined ports. Using the check boxes on the interface, you can either

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

You can allow or block any of the following protocols:

- PPPoE (Point to Point Protocol over Ethernet)
- Any or all of the following IPv4 (Internet Protocol version 4) protocols:
    - SMB (Network Neighborhood)
    - SNMP
    - Up to 3 user-defined ports
    - All other IPv4 traffic (see Figure 26)
    - Uplink Broadcast
    - ARP (Address Resolution Protocol)
    - All others (see Figure 26)

Figure 26 Categorical protocol filtering



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

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

The ports that are filtered as a result of protocol selections in the Protocol Filtering tab of the SM are listed in Table 23.

Table 23 Ports filtered per protocol selections

Protocol Selected	**Port Filtered (Blocked)**

SMB	Destination Ports 137 TCP and UDP, 138 UDP, 139 TCP, 445 TCP
SNMP	Destination Ports 161 TCP and UDP, 162 TCP and UDP
Bootp Client	Source Port 68 UDP
Bootp Server	Source Port 67 UDP

Port Lockdown

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

Table 24 Device default port numbers

Port	Usage	Port Usage	Device
21	FTP	Listen Port	AP, SM
80	HTTP	Listen Port	AP, SM
1812	Standard RADIUS port	Destination Port	AP
1813	Standard RADIUS accounting port	Destination Port	AP, SM
161	SNMP port	Listen Port	AP, SM
162	SNMP trap port	Destination Port	AP, SM
514	Syslog	Destination Port	AP, SM

Isolating SMs

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

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

- **Disable SM Isolation** (the default selection). This allows full communication between SMs.
- **Block SM Packets from being forwarded**. This prevents both multicast/broadcast and unicast SM-to-SM communication.
- **Block and Forward SM Packets to Backbone**. This not only prevents multicast/broadcast and unicast SM-to-SM communication but also sends the packets, which otherwise would have been handled SM to SM, through the Ethernet port of the AP.

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

Filtering management through Ethernet

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

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

Allowing management from only specified IP addresses

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

If you select

- **IP Access Filtering Disabled**, then management access is allowed from any IP address, even if the **Allowed Source IP *1 to 3*** parameters are populated.
- **IP Access Filtering Enabled**, and specify at least one address in the **Allowed Source IP *1 to 3*** parameter, then management access is limited to the specified address(es).

Configuring management IP by DHCP

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

In the SM, this parameter is settable

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

Planning for airlink security

Cambium fixed wireless broadband IP systems employ the following form of encryption for security of the wireless link:

- DES–Data Encryption Standard, an over-the-air link option that uses secret 56-bit keys and 8 parity bits.

Planning for RF Telnet Access Control

The RF Telnet Access feature restricts Telnet access to the AP from a device situated below a network SM (downstream from the AP). This is a security enhancement to restrict RF-interface sourced AP access specifically to the LAN1 IP address and LAN2 IP address (Radio Private Address, typically 192.168.101.[LUID]). This restriction disallows unauthorized users from running Telnet commands on the AP that can change AP configuration or modifying network-critical components such as routing and ARP tables.

Planning for RADIUS integration

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

RADIUS Functions

RADIUS protocol support provides the following functions:

- **SM Authentication** allows only known SMs onto the network (blocking "rogue" SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to "rogue" APs). RADIUS authentication is used for SMs, but is not used for APs. Cambium modules support EAP-TTLS and EAP-MSCHAPv2 authentication methods.
- **SM Authorization** configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when an SM registers to an AP.
- **SM Accounting** provides support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP.
- **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed IP** allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).

Planning for SNMP security

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

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

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 25 lists PMP 450 components.

Table 25 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 3: Legal information

This chapter provides legal notices including software license agreements.

⚠ CAUTION

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

The following topics are described in this chapter:

- Cambium Networks end user license agreement on page 3-73
- Hardware warranty on page 3-79
- Limit of liability on page 3-80

Cambium Networks end user license agreement

Acceptance of this agreement

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

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

Definitions

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

Grant of license

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

Conditions of use

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

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.

3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.

4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

Title and restrictions

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

Confidentiality

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

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

Right to use Cambium's name

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

Transfer

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

Updates

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

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

Maintenance

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

Disclaimer

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

Limitation of liability

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

U.S. government

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

Term of license

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

Governing law

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

Assignment

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

Survival of provisions

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

Entire agreement

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

Third party software

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

Hardware warranty

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

Limit of liability

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

Chapter 4: 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 4-82 contains specifications of the AP, SM and other equipment required for PMP 450 installations.
- Wireless specifications on page 4-87 contains specifications of the PMP 450 wireless interface, including RF bands, channel width and link loss.
- Data network specifications on page 4-89 contains specifications of the PMP 450 Ethernet interface.
- Compliance with safety standards on page 4-90 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 4-95 describes how the PMP 450 complies with the radio regulations that are in force in various countries.
- Notifications on page 4-99 contains notifications made to regulatory bodies for the PMP 450.
- Data throughput tables on page 4-103 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 26. These specifications apply to all PMP 450 product variants.

Table 26 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")
Maximum Power Consumption	18 W

Category	Specification
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 26 and **Error! Reference source not found.**. These specifications apply to all PMP 450 product variants.

Figure 27 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)
Protocols Used	IPv4, UDP, TCP, IP, ICMP, Telnet, SNMP, HTTP, FTP

Category	Specification
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	55º azimuth, 55º 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	
Wind Loading	190 km/hour (118 mi/hour)
Environmental	IP55

Category	**Specification**
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 27 lists the wireless specifications that apply to all PMP 450 variants.

Table 27 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 28 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 29.

Table 29 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 4-103
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 30.

Table 30 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 31 lists the EMC specification type approvals that have been granted for PMP 450.

Table 31 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 4-91) is:

10 W/m^2 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 32 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 32:

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 32 Power compliance margins

Freq. Band	Antenna	Variable			*d* (calculated)	Recommended Separation Distance	Power Compliance Margin
		P	**G**	**S**			
5.8 GHz OFDM	Integrated SM, 9 dBi patch	0.158 W (22 dBm)	7.9 (9 dB)	10 W/m^2 or 1 mW/cm^2	10 cm	20 cm (8 in)	40.27
	Integrated SM, 9 dBi patch with 9 dBi Cassegrain LENS	0.158 W (22 dBm)	39.8 (16 dB)	10 W/m^2 or 1 mW/cm^2	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/m^2 or 1 mW/cm^2	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/m^2 or 1 mW/cm^2	25.1 cm	50 cm (20 in)	39.77

NOTE

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

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

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

NOTE

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

Compliance with radio regulations

This section describes how the PMP 450 complies with the radio regulations that are 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 31 lists the radio specification type approvals that have been granted for PMP 450 frequency variants.

Table 33 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 34 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 34 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 35 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 36 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 28).

Figure 28 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

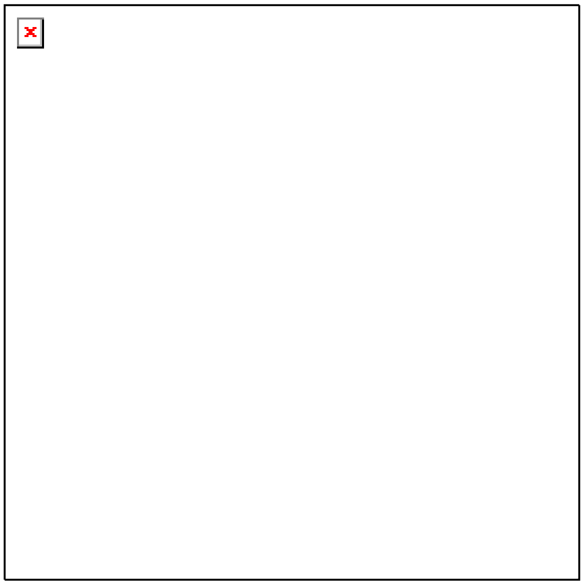
The PMP 450 is a Class 2 device as it operates on frequencies that are not harmonized across the EU. Currently the product may only be operated in the UK, Eire (IRL), Germany, Norway and Denmark. However, the regulatory situation in Europe is changing and the radio spectrum may become available in other 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 29).

Figure 29 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 37 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)			

Appendix A: Glossary

Table 38 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.

Term	Definition
Activate	To provide feature capability to a module, but not to *enable* (turn on) the feature in the module. See also Enable.
Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See http://www.faqs.org/rfcs/rfc826.html.
Aggregate Throughput	The sum of the throughputs in the uplink and the downlink.
AP	Access Point Module. One module that distributes network or Internet services to 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.

Term	Definition
Burst	Preset amount limit of data that may be continuously transferred.
C/I Ratio	Ratio of intended signal (carrier) to unintended signal (interference) received.
Canopy	A trademark of 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. 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.