



USER GUIDE

ePMP (802.11n)

System Release 4.6



Reservation of Rights

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 recommends reviewing the Cambium Networks website for the latest changes and updates to products. 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

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”).

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Contents

- Contents** **3**
- About This User Guide** **11**
 - Problems and warranty 11
 - Repair and service 11
 - Warranty 11
 - Security advice 12
 - Warnings, cautions, and notes 12
 - Caring for the environment 13
 - In EU countries 13
 - Disposal of Cambium equipment 13
 - Disposal of surplus packaging 13
- Chapter 1: Product Description** **14**
 - Overview of ePMP 14
 - Purpose 14
 - Key features 14
 - Typical installation equipment 15
 - Wireless operation 16
 - Time division duplexing 16
 - OFDM and channel bandwidth 16
 - Adaptive modulation 16
 - MIMO 17
 - Radar avoidance 17
 - Encryption 17
 - Country codes 17
 - Smart Beamforming (ePMP 2000 series) 18
 - PMP networks 19
 - Further reading on wireless operation 19
 - System management 19

Management agent	20
Web server	20
Web pages	21
Identity-based user accounts	21
SNMP	22
Network Time Protocol (NTP)	22
cnMaestro™	22
Software upgrade	22
Further reading on system management	22
Chapter 2: System Hardware	23
Installation and Safety	23
Site installation	24
Grounding and lightning protection	24
Lightning protection zones	26
ePMP 2000	27
ePMP 2000 Access Point with intelligent filtering and sync	27
ePMP 2000 Access Point with Intelligent Filtering and Sync description	28
ePMP 2000 Access Point with Intelligent Filtering and Sync part numbers	28
ePMP 2000 Access Point with Intelligent Filtering and Sync mounting bracket	30
ePMP 2000 Access Point with Intelligent Filtering and Sync interfaces	30
ePMP 2000 Access Point with Intelligent Filtering and Sync LEDs	31
ePMP 2000 Access Point with Intelligent Filtering and Sync specifications	32
ePMP 2000 Access Point with Intelligent Filtering and Sync heater	33
ePMP 2000 Access Point with Intelligent Filtering and Sync - external antenna location	33
ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading	33
ePMP 2000 Access Point with Intelligent Filtering and Sync software packages	34
ePMP 2000 Access Point with Intelligent Filtering and Sync, antennas and antenna cabling	35
Antenna requirements	35
FCC and IC approved antennas	35
ePMP 1000	36

ePMP 1000 Connectorized Radio with Sync	36
ePMP 1000 Connectorized Radio with Sync description	36
ePMP 1000 Connectorized Radio with Sync part numbers	37
ePMP 1000 Connectorized Radio with Sync mounting bracket	38
ePMP 1000 Connectorized Radio with Sync interfaces	38
ePMP 1000 Connectorized Radio with Sync LEDs	39
ePMP 1000 Connectorized Radio with Sync specifications	40
ePMP 1000 Connectorized Radio with Sync heater	41
ePMP 1000 Connectorized Radio with Sync and external antenna location	41
ePMP 1000 Connectorized Radio with Sync wind loading	41
ePMP 1000 Connectorized Radio with Sync software packages	42
ePMP 1000 Connectorized Radio with Sync, antennas, and antenna cabling	42
ePMP 1000 Antenna requirements	43
ePMP 1000 FCC and IC approved antennas	43
ePMP 1000 Integrated Radio	43
ePMP 1000 Integrated Radio description	44
ePMP 1000 Integrated Radio part numbers	44
ePMP 1000 Integrated Radio mounting bracket	45
ePMP 1000 Integrated Radio interfaces	45
ePMP 1000 Integrated Radio LEDs	46
ePMP 1000 Integrated Radio specifications	47
ePMP 1000 Integrated Radio heater	48
ePMP 1000 Integrated Radio wind loading	49
ePMP 1000 Integrated Radio software packages	50
ePMP 1000 Connectorized Radio	50
ePMP 1000 Connectorized Radio description	50
ePMP 1000 Connectorized Radio part numbers	51
ePMP 1000 Connectorized Radio mounting bracket	51
ePMP 1000 Connectorized Radio Interfaces	52
ePMP 1000 Connectorized Radio LEDs	53

ePMP 1000 Connectorized Radio specifications	54
ePMP 1000 Connectorized Radio heater	55
ePMP 1000 Connectorized Radio and external antenna location	55
ePMP 1000 Connectorized Radio wind loading	55
Connectorized Radio software packages	56
ePMP 1000 Connectorized Radio antennas and antenna cabling	56
ePMP 1000 Antenna requirements	57
ePMP 1000 FCC and IC approved antennas	57
Force 130	57
Force 130 description	58
Force 130 part numbers	58
Force 130 mounting	59
Force 130 interfaces	60
Force 130 LEDs	61
Force 130 specifications	62
Force 130 software packages	63
Force 180	63
Force 180 description	64
Force 180 part numbers	64
Force 180 mounting bracket	65
Force 180 interfaces	65
Force 180 LEDs	66
Force 180 specifications	67
Force 180 heater	67
Force 180 wind loading	68
Force 180 software packages	69
Force 190	69
Force 190 description	69
Force 190 part numbers	70
Force 190 mounting bracket	70

Force 190 interfaces	71
Force 190 LEDs	72
Force 190 specifications	73
Force 190 heater	74
Force 190 wind loading	74
Force 190 software packages	75
Force 200	75
Force 200 description	75
Force 200 part numbers	76
Force 200 mounting bracket	77
Force 200 interfaces	78
Force 200 LEDs	79
Force 200 specifications	79
Force 200 heater	80
Force 200 wind loading	80
Force 200 software packages	81
Force 200L	81
Force 200L description	82
Force 200L part numbers	82
Power supply	83
Force 200L mounting bracket	84
Force 200L interfaces	84
Force 200L LEDs	85
Force 200L specifications	87
Force 200L Heater	87
Force 200L wind loading	87
Force 200L software packages	88
Chapter 3: Power Supply	89
ePMP 2000 Series Power Supply	89
Power supply description	89

Power supply part numbers	89
Power supply interfaces	89
Power supply specifications	90
Power supply location	90
ePMP 1000 Series Power Supply (includes Force 180, Force 190, and Force 200)	91
Power supply description	91
Power supply part numbers	91
Power supply interfaces	91
Power supply specifications	92
Power supply location	94
Chapter 4: Ethernet Cabling	95
Ethernet standards and cable lengths	95
Outdoor Cat5e cable	95
Cambium Industrial Cable	95
Surge suppression unit	96
Gigabit Ethernet Surge Suppressor	96
Chapter 5: System Planning	98
Radio spectrum planning	98
General wireless specifications	98
Regulatory limits	100
Conforming to the limits	100
Available spectrum	100
Channel bandwidth	101
Avoidance of weather radars	101
Link planning	101
Range and obstacles	102
Path loss	102
Adaptive modulation	102
Planning for connectorized units	103
Calculating maximum power level for connectorized units	103

Data network planning	104
Ethernet interfaces	104
Management VLAN	105
Quality of service for bridged Ethernet traffic	105
Chapter 6: Configuration	106
Preparing for configuration	106
Safety precautions	106
Regulatory compliance	106
Connecting to the unit	106
Configuring the management PC	107
Connecting to the PC and powering up	108
Using the web interface	108
Logging into the web interface	109
Layout of the web interface	110
ePMP Device Configuration Parameters - Default Values	118
Configuring connectorized radios using the Quick Start menu	121
Configuring SM units using the Quick Start menu	124
Using the AP menu options	128
AP Configure menu	129
AP Monitor menu	156
AP Tools menu	173
Using the SM menu options	190
SM Configuration menu	190
SM Monitor menu	232
SM Tools menu	253
Radius Server	265
Installing Free-radius on Ubuntu 12.04 LTS	265
Configuring Free-radius server	265
Configuring radius parameters on AP	267
Configuring radius parameters on SM	268

Configuring MIR profiles	268
Creating certificate for Radius server and SM device	270
Vendor-Specific Attribute (VSA) Reference	275
Chapter 7: Operation and Troubleshooting	280
General Planning for Troubleshooting	280
General fault isolation process	281
Questions to help isolate the problem	281
Upgrading device software	282
Upgrading on-board GPS chip firmware	284
GPS Chip and Software Reference	285
Testing hardware	285
Checking the power supply LED	285
Power LED is off	286
Ethernet LED is off	286
Troubleshooting the radio link	287
Module has lost or does not establish radio connectivity	287
Link is unreliable or does not achieve data rates required	288
Module Has Lost or Does Not Gain GPS Synchronization	288
Using the device external reset button	289
Resetting ePMP to factory defaults by power cycling	290
Recovery of flash-corrupted ePMP devices	291
Flexible License Generation Procedure	292
Enabling AP Flexible License Management	296
Glossary	298

About This User Guide

This guide describes the planning, installation, configuration, and operation of the Cambium ePMP Series of point-to-multipoint wireless Ethernet systems. It is intended for use by the system designer, system installer, and system administrator.

For radio network design, see:

- [Product description](#)
- [System hardware](#)
- [System planning](#)
- [Legal and reference information](#)

For system configuration, monitoring, and fault finding, see:

- [Configuration](#)
- [Operation and Troubleshooting](#)

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: https://support.cambiumnetworks.com/
3	Ask for assistance from the Cambium product supplier.
4	Gather information from affected units, such as any available diagnostic downloads.
5	Escalate the problem by emailing or telephoning support: http://www.cambiumnetworks.com/support/contact-support

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

Do not open the radio housing for repair or diagnostics; there are no serviceable parts within the housing.

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.

Cambium Networks ePMP equipment is shipped with default web management interface login credentials. It is highly recommended that these usernames and passwords are modified prior to system installation.

Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and 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. For disposal instructions, see <https://support.cambiumnetworks.com>

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 ePMP product. It describes the function of the product, the main product variants, and typical installation. It also describes the main hardware components.

The following topics are described in this chapter:

- The key features, typical uses, product variants, and components of the ePMP are explained in [Overview of ePMP](#).
- How the ePMP wireless link is operated, including modulation modes, power control, and security is described under [Wireless operation](#).
- The ePMP management system, including the web interface, installation, configuration, alerts, and upgrades is described in [System management](#).

Overview of ePMP

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

Purpose

Cambium ePMP Series products are designed for Ethernet bridging over point-to-multipoint microwave links in the unlicensed 2.4 GHz, 2.5 GHz (Brazil only), 5 GHz, and 6.4 GHz bands. Users must ensure that the ePMP Series complies with local operating regulations.

The ePMP Series acts as a transparent bridge between two segments of the operator and customers' networks. In this sense, it can be treated as a virtual wired connection between the Access Point and the Subscriber Module. The ePMP Series forwards 802.3 Ethernet packets destined for the other part of the network and filters packets it does not need to forward.

Key features

The ePMP system is a high-performance wireless bridge for Ethernet traffic with a maximum UDP throughput of 200+ Mbps (40 MHz Channel Bandwidth). It is capable of operating in Line-of-Sight (LoS) and near-LoS conditions. Its maximum LoS range is 13 mi (20 MHz channel bandwidth) or 9 mi (40 MHz channel bandwidth).

Utilizing GPS sync, the ePMP is an ideal fit for networks that require capacity and reliability for superior QoS in remote and underserved areas. The integrated PTP and PMP solution features an efficient GPS synchronized operational mode that permits highly scalable frequency reuse.

ePMP operates in the unlicensed 2.4 GHz, 2.5 GHz (Brazil only), 5 GHz, and 6.4 GHz bands and supports a channel bandwidth of up to 40 MHz. It is available with an integrated antenna or in a connectorized version for use with an external antenna.

The wireless link is primarily TDD-based. System Release 1.2.3 added a Flexible Frame Ratio option which provides improved latency and throughput under unsynchronized operational mode.

From a network point-of-view, the ePMP wireless link is a transparent Layer 2 bridge. It offers limited switching capability to support a primary and a secondary (future release) Ethernet port on the Subscriber Module.

ePMP supports Quality of Service (QoS) classification capability and supports three traffic priorities. Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

System Release 1.3.4 adds support for RADIUS EAP-TTLS authentication and VSA support for MIR.

When deployed with a sector antenna, the ePMP 1000 GPS Sync Radio can be configured as a GPS synchronized Access Point serving ePMP Integrated Radios configured as Subscriber Modules. When deployed with a high gain point-to-point antenna, the ePMP GPS Sync Radio can be configured to be a GPS Synchronized Backhaul Master, forming a PTP link with another ePMP Radio module.

Powered by Hypure™ technology, ePMP 2000 features Smart Beamforming. This powerful addition to your network creates narrow, targeted beams to each subscriber, rather than relying on a traditional wide beam, blocking out multiple sources of interference to keep performance high.

ePMP 2000 also includes Intelligent Filtering, working automatically to clean up the signals received by the access point as well as keep its own transmissions clean. This helps not just that single access point reach optimum performance, but the whole tower too.

A summary of the main ePMP characteristics is listed under [Table 1](#).

Table 1: Main characteristics of the ePMP Series

Characteristic	Value
Topology	PMP or PTP
Wireless link condition	LoS, near LoS
Scheduler	TDD (Fixed or Flexible Ratios), ePTP, Standard Wi-Fi
Connectivity	Ethernet
Operating frequencies	ePMP 2000 Unlicensed bands, 5 GHz
	ePMP 1000 Unlicensed bands, 2.4 GHz, 2.5 GHz, 5 GHz, 6.4 GHz
Channel bandwidth	5 MHz, 10 MHz, 20 MHz, or 40 MHz
Data rate	200+ Mbps

Typical installation equipment

The ePMP is a solution consisting of integrated or connectorized outdoor units, indoor power supply units/LAN injectors, cabling, and surge suppression equipment.

The main hardware components of an ePMP installation are as follows:

- **ePMP 2000 Access Point with Intelligent Filtering and Sync or Connectorized Radio with GPS Sync (ePMP 1000):** A connectorized outdoor transceiver unit containing all the radio, networking, and surge suppression electronics.
- **ePMP 2000 Access Point with Intelligent Sync Power Supply or GPS Sync Connectorized Radio (ePMP 1000) Power Supply:** An indoor power supply module providing Power-over-Ethernet (PoE) supply and 1000/100/10BASE-TX to the Access Point.

- ePMP 2000 Access Point with Intelligent Sync or GPS Sync Connectorized Radio (ePMP 1000) Radio Cabling and lightning protection: Shielded Cat5e cables, grounding cables, and connectors.
- **Integrated Radio:** An integrated-antenna outdoor transceiver unit containing all the radio, networking, antenna, and surge suppression electronics.
- **Integrated or Un-sync Connectorized Radio:** A connectorized outdoor transceiver unit containing all the radio, networking, and surge suppression electronics.
- **Integrated Radio Power Supply:** An indoor power supply module providing Power-over-Ethernet (PoE) supply and 100/10BASE-TX to the Subscriber Module.
- Integrated Radio Cabling and lightning protection: Shielded Cat5e cables and connectors.

For more information about these components, including interfaces, specifications, and Cambium part numbers, see [System hardware](#).

Wireless operation

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

Time division duplexing

TDD cycle

ePMP links operate using Time Division Duplexing (TDD). The links employ a TDD cycle in which the APs determines which SMs may transmit and when based on the configured downlink/uplink ratio (duty cycle). Three fixed Downlink/Uplink frame ratios are available – 75/25, 50/50, and 30/70. A flexible frame ratio is available as a fourth option where the AP dynamically determines the downlink and uplink ratio based on data demand in each direction.

OFDM and channel bandwidth

The ePMP series transmits using Orthogonal Frequency Division Multiplexing (OFDM). This wideband signal consists of many equally spaced sub-carriers. Although each subcarrier is modulated at a low rate using conventional modulation schemes, the resultant data rate from all the sub-carriers is high.

The channel bandwidth of the OFDM signal is 5 MHz, 10 MHz, 20 MHz, or 40 MHz, based on operator configuration.

Each channel is offset in center frequency from its neighboring channel by 5 MHz.

Adaptive modulation

The ePMP series can transport data over the wireless link using a number of different modulation modes ranging from 64-QAM to QPSK. For a given channel bandwidth and TDD frame structure, each modulation mode transports data at a fixed rate. Also, the receiver requires a given signal-to-noise ratio to successfully demodulate a given modulation mode. Although the more complex modulations such as 64-QAM will transport data at a much higher rate than the less complex modulation modes, the receiver requires a much higher signal-to-noise ratio.

The ePMP series provides an adaptive modulation scheme where the receiver constantly monitors the quality of the received signal and notifies the far end of the link of the optimum modulation mode with which to transmit. In this way, optimum capacity is achieved at all times.

MIMO

Multiple-Input Multiple-Output (MIMO) technique protects against fading and increases the probability of a received decoded signal being usable.

The ePMP transmits two signals on the same radio frequency, one of which is 90 degrees offset from the other.

Radar avoidance

In regions where the protection of radars is part of the local regulations, the ePMP must detect interference from radar-like systems and avoid co-channel operation with these systems.

To meet this requirement, the ePMP implements the following features:

- The equipment can only transmit on available channels, of which there are none at initial power-up. The radar detection algorithm will always scan a usable channel for 60 seconds for radar interference before making the channel an available channel.
- This compulsory channel scan will mean that there is at least 60 seconds service outage every time radar is detected and that the installation time is extended by at least 60 seconds even if there is found to be no radar on the channel

There is a secondary requirement for bands requiring radar avoidance. Regulators have mandated that products provide a uniform loading of the spectrum across all devices. In general, this prevents operation with fixed frequency allocations. However:

- ETSI regulations do allow frequency planning of networks (as that has the same effect of spreading the load across the spectrum).
- The FCC does allow channels to be avoided if there is actual interference on them.



Note

When operating in a region that requires DFS, ensure that the AP is configured with alternate frequencies and that the SM is configured to scan for these frequencies to avoid long outages.

Encryption

The ePMP supports optional encryption for data transmitted over the wireless link. The encryption algorithm used is the Advanced Encryption Standard (AES) with a 128-bit key size. AES is a symmetric encryption algorithm approved by U.S. Government organizations (and others) to protect sensitive information.

Country codes

Some aspects of the wireless operation are controlled, enforced, or restricted according to a country code. ePMP country codes represent individual countries (for example Denmark) or regulatory regions (for example FCC or ETSI).

Country codes affect the following aspects of wireless operation:

- Maximum transmit power
- Radar avoidance

- Frequency range



Caution

To avoid possible enforcement action by the country regulator, always operate links in accordance with local regulations

Smart Beamforming (ePMP 2000 series)

- ePMP 2000 Smart Beamforming drastically reduces the effects of on-channel interference. The System learns the locations of each served Subscriber Module and forms a narrow beam towards the desired Subscriber Module while that radio is transmitting in the uplink. This reduces the gain on the uplink for on-channel interferers that are transmitting at an azimuth angle different than the Subscriber Module, delivering performance gains never before seen.



Smart antenna key advantages:

- Eliminate Uplink Interference: Smart Beamforming delivers dramatic performance improvements when dealing with strong co-channel uplink interference, maximizing network performance.
- Consistent Performance in High Interference: By mitigating significant sources of interference, packet loss and retransmissions are kept to a minimum, keeping your network applications working at their best.
- Improvement in Uplink and Downlink Performance: By eliminating packet loss and retransmissions resulting from co-channel uplink interference, TCP retransmissions are greatly reduced. Other applications also show significant performance benefits.
- Intelligent Filtering (ePMP 2000 Series)
- ePMP 2000 Intelligent Filtering improves both receive and transmit performance. It protects the

network from off-channel interferers with a filter that dynamically moves around the channel. On the transmit side, it protects the RF environment by reducing off-channel transmission noise.

PMP networks

Using frequency planning

Frequency planning is the exercise of assigning operating channels to PMP units to minimize RF interference between links. Frequency planning must consider interference from any PMP unit to any other PMP unit in the network. Low levels of interference normally allow for stable operation and high link capacity.

The frequency planning task is made more straightforward by using the following techniques:

- Using several different channels
- Separating units located on the same mast
- Configuring a 5 MHz guard band between adjacent sector operating band edges.

For help with planning networks, see [System planning](#).

Further reading on wireless operation

For information on planning wireless operation, see:

- The regulatory restrictions that affect radio spectrum usages, such as frequency range and radar avoidance are described under [Radio spectrum planning](#).
- The factors to be taken into account when planning links such as range, path loss, and data throughput are described under [Link planning](#).
- The safety specifications against which the ePMP has been tested are listed under [Compliance with safety standards](#). It also describes how to keep RF exposure within safe limits.
- How ePMP complies with the radio regulations that are enforced in various countries is explained in [Compliance with radio regulations](#).
- Compliance with the radio regulations that are enforced in various regions is explained in [Table 1](#) through [Table 2](#).
- Tables and graphs to support the calculation of the data rate capacity that can be provided by ePMP configurations are available at [Data throughput tables](#).

For more information on configuring and operating the wireless link, see:

- The configuration parameters of the ePMP devices are described under [Configuration](#).
- Post-installation procedures and troubleshooting tips are explained under [Operation and Troubleshooting](#).

System management

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

Management agent

ePMP 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:

- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Simple Network Management Protocol (SNMP)
- Network Time Protocol (NTP)
- System logging (Syslog)
- Cambium Network Services Server (CNSS) software
- Dynamic Host Configuration Protocol (DHCP)

Web server

The ePMP management agent contains a web server. The web server supports access via the HTTP and HTTPS interfaces.

Web-based management offers a convenient way to manage the ePMP 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 the installation of ePMP, and the majority of ePMP configuration management tasks.

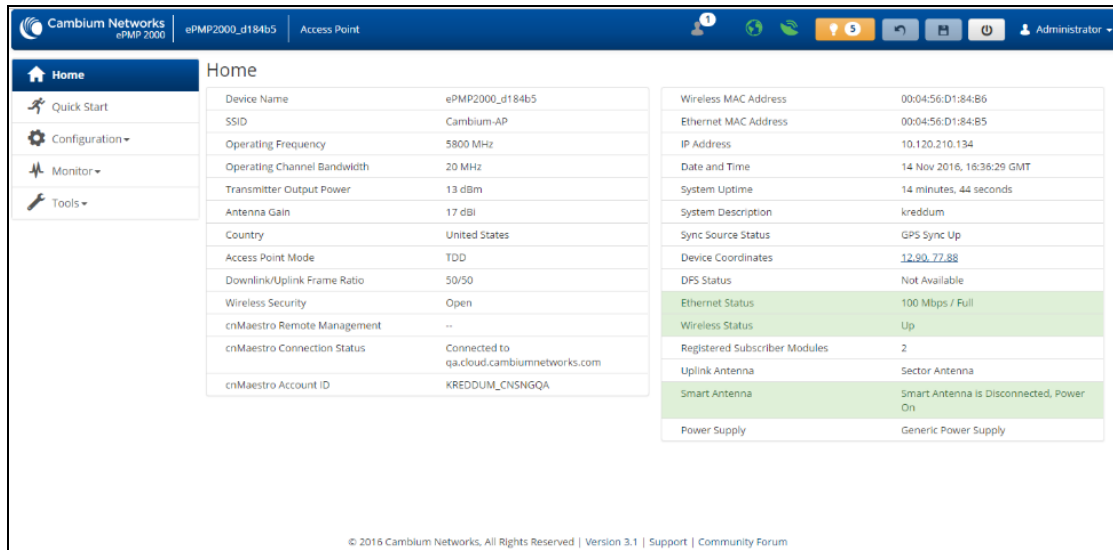
Figure 1: ePMP 1000 AP web-based management screenshot

The screenshot displays the web-based management interface for a Cambium Networks ePMP 1000 AP. The interface is organized into a navigation sidebar on the left and a main content area. The sidebar includes links for Home, Quick Start, Configuration, Monitor, and Tools. The main content area is titled 'Home' and displays system information for the device 'ePMP1000_cf8ed'. This information is presented in two columns of key-value pairs. The left column lists device details such as SSID (Cambium-AP), operating frequency (5700 MHz), channel (40 MHz), power (7 dBm), antenna gain (15 dBi), country (Other), access point mode (TDD), frame ratio (75/25), security (WPA2), and connection status (Connected to cloud.cambiumnetworks.com). The right column lists network and system details including MAC addresses, IP address (192.168.2.200), date and time, uptime (1 minute, 22 seconds), and system description (GP5 Sync Up). A status table at the bottom right highlights the 'Ethernet Status' as '1000 Mbps / Full' and 'Wireless Status' as 'Up'. The interface also shows a 'Registered Subscriber Modules' count of 1. The footer contains copyright information for Cambium Networks, 2016.

Device Name	ePMP1000_cf8ed
SSID	Cambium-AP
Operating Frequency	5700 MHz
Operating Channel Bandwidth	40 MHz
Transmitter Output Power	7 dBm
Antenna Gain	15 dBi
Country	Other
Access Point Mode	TDD
Downlink/Uplink Frame Ratio	75/25
Wireless Security	WPA2
cnMaestro Remote Management	--
cnMaestro Connection Status	Connected to cloud.cambiumnetworks.com
cnMaestro Account ID	MARTIN_GRAY

Wireless MAC Address	00:04:56:C6:F8:EE
Ethernet MAC Address	00:04:56:C6:F8:ED
IP Address	192.168.2.200
Date and Time	01 Sep 2015, 00:01:18 GMT
System Uptime	1 minute, 22 seconds
System Description	--
Sync Source Status	GP5 Sync Up
Device Coordinates	--
Ethernet Status	1000 Mbps / Full
Wireless Status	Up
Registered Subscriber Modules	1

Figure 2: ePMP 2000 AP web-based management screenshot



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 and Subscriber Module web-pages:

- **Dashboard:** The Dashboard web-page reports the general device status, session status, remote subscriber status, event log information, and network interface status.
- **Configure:** 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, protocol filtering, and unit settings.
- **Monitor:** The Monitor web-page reports detailed operating statistics for the radio link and network, and reports system log information.
- **Tools:** The tools web-page offers useful tools for device installation, configuration, and operation including software upgrade, backup/restore, spectrum analyzer, throughput test, ping test, and traceroute.
- **Quick Start:** The Quick Start web-page provides quick access to requisite parameters for radio link establishment and network access.

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** (default username/password "admin"), who has full read and write permission.
- **INSTALLER** (default username/password "installer"), who has permission to read and write parameters applicable to unit installation and monitoring.

- HOME (default username/password “home”), who has permission only to access pertinent information for support purposes
- READONLY (default username/password “readonly”), who has permission to only view the Monitor page.

SNMP

The management agent supports fault and performance management using an SNMP interface. The management agent is compatible with SNMP v2c using one Management Information Base (MIB) file which is available for download from the Cambium Networks Support website (<https://support.cambiumnetworks.com/files/epmp>).

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.

ePMP devices may receive NTP data from a CMM3 or CMM4 module or an NTP server configured in the system’s management network.

The Time Zone option is configurable on the AP’s **Configure > System** page and may be used to offset the received NTP time to match the operator’s local time zone.

cnMaestro™

cnMaestro is a cloud-based or on-site platform designed to monitor, configure, operate, upgrade, manage and monitor ePMP systems. For more information, see the [cnMaestro website](#).

Software upgrade

Software upgrades may be issued via the radio web interface (**Tools > Software Upgrade**) or via CNSS (Cambium Networks Services Server). For Software upgrades, see

<https://support.cambiumnetworks.com/files/epmp>.

Further reading on system management

For more information on system management, see:

- [AP system page](#)
- [SM System page](#)
- [Operation and Troubleshooting](#)

Chapter 2: System Hardware

This chapter describes the site planning and hardware components of an ePMP link.

The following topics are described in this chapter:

- Factors to be considered when planning the proposed network are described under [Installation and Safety](#).
- The ePMP 2000 Access Point with Intelligent Filtering and Sync module hardware, part numbers, mounting equipment, and specifications are described under [ePMP 2000 Access Point with Intelligent Filtering and Sync](#).
- The ePMP 1000 Connectorized with Sync module hardware, part numbers, mounting equipment, and specifications are described under [ePMP 1000 Connectorized Radio with Sync](#).
- The ePMP 1000 Integrated hardware, part numbers, mounting equipment, and specifications are described under [ePMP 1000 Integrated Radio](#) (ePMP 1000).
- The ePMP 1000 Connectorized hardware, part numbers, mounting equipment, and specifications are described under [ePMP 1000 Connectorized Radio](#) (ePMP 1000).
- The Force 130 hardware, part numbers, mounting equipment, and specifications are described under [Force 130](#).
- The Force 180 hardware, part numbers, mounting equipment, and specifications are described under [Force 130](#).
- The Force 190 hardware, part numbers, mounting equipment, and specifications are described under [Force 190](#).
- The Force 200 hardware, part numbers, mounting equipment, and specifications are described under [Force 200](#).
- The Force 200L hardware, part numbers, mounting equipment, and specifications are described under [Force 200L](#).
- The power supply hardware, part numbers, and specifications are described under [ePMP 1000 Series Power Supply \(includes Force 180, Force 190, and Force 200\)](#).
- The AP sector antenna (including optional Smart Antenna) part numbers are described under [ePMP 2000 Access Point with Intelligent Filtering and Sync, antennas and antenna cabling](#) (ePMP 2000) [ePMP 1000 Connectorized Radio with Sync software packages](#) (ePMP 1000).
- Cable standards and lengths are described under [Ethernet cabling](#).
- Surge suppression requirements and recommendations are described under [Surge suppression unit](#).

Installation and Safety

Conduct a site survey to ensure that the proposed AP and SM sites meet the requirements defined in this section.

Site installation

An ePMP site typically consists of a high supporting structure such as a mast, tower, or building for the AP or SM.

There is only one Ethernet interface, a copper Cat5e connection from the AP or SM to the AP/SM power supply, and network terminating equipment. If a 1000BASE-TX (Gigabit) Ethernet connection is required at the AP, ensure that power supply N000900L001B (ePMP 1000) or N000000L034A (ePMP 2000) is utilized.

Grounding and lightning protection

Structures, equipment, and people must be protected against power surges (typically caused by lightning) by conducting the surge current to the ground via a separate preferential solid path. The actual degree of protection required depends on local conditions and applicable local regulations. To adequately protect an ePMP installation, both ground bonding and transient voltage surge suppression are required.



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.

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.



Note

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.

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.

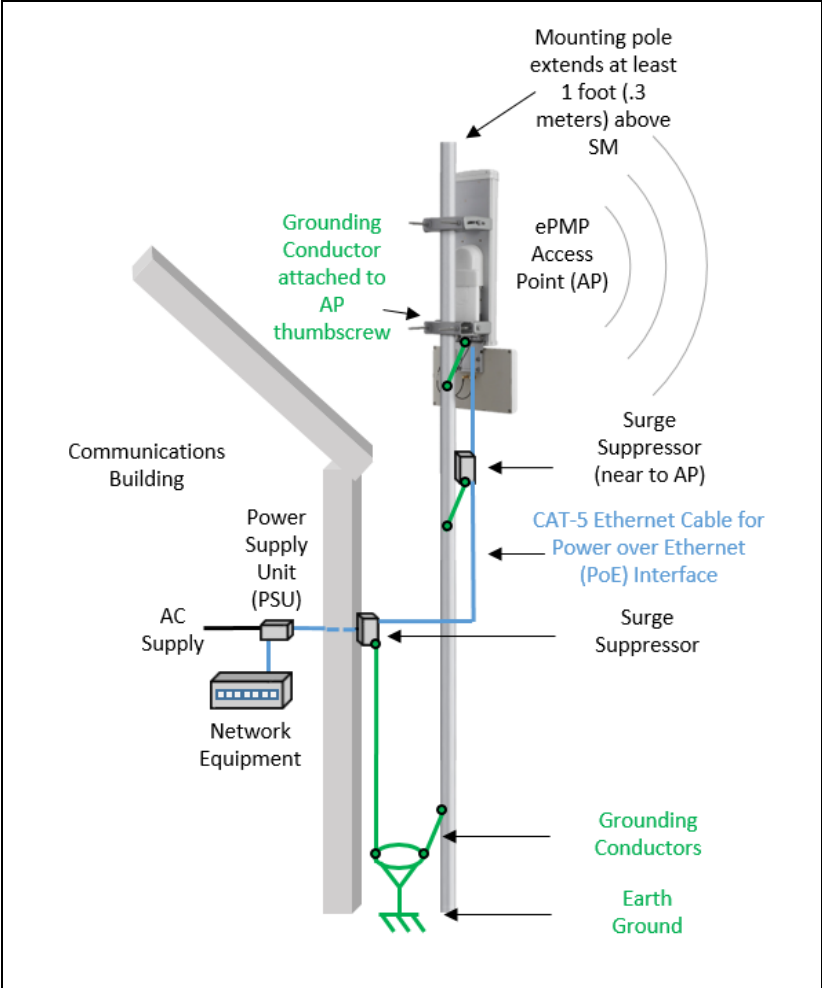


Figure 3: AP Cabling Diagram

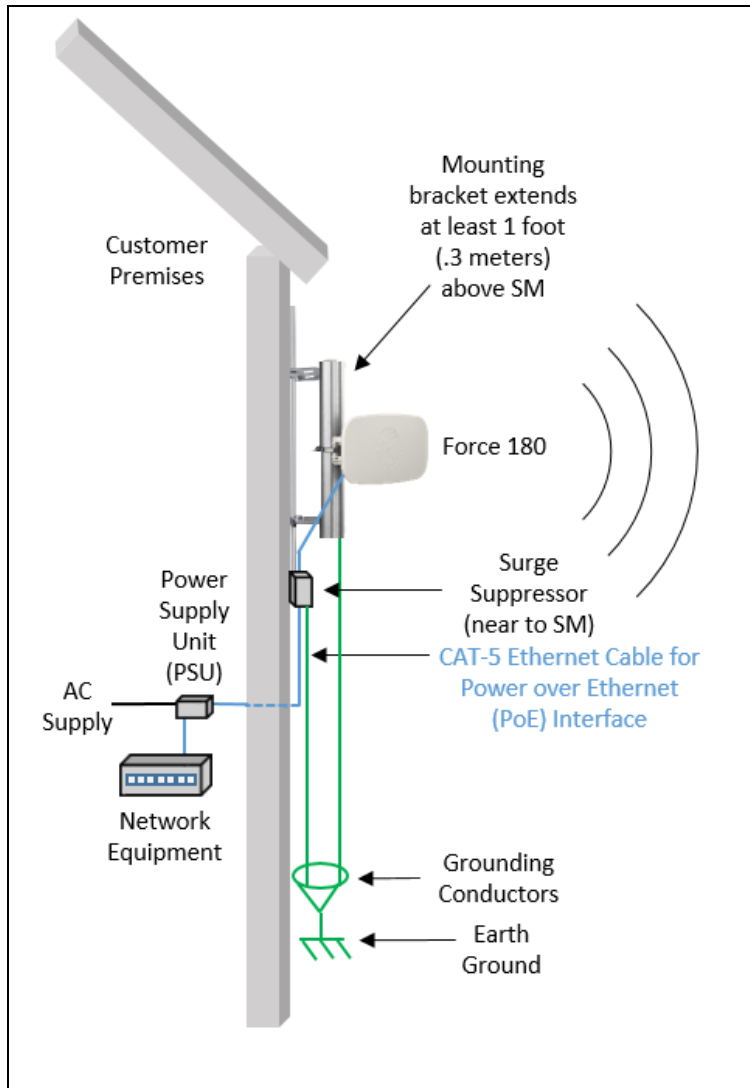


Figure 4: SM Cabling Diagram

Lightning protection zones

Use the rolling sphere method (Figure 5) 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.

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.

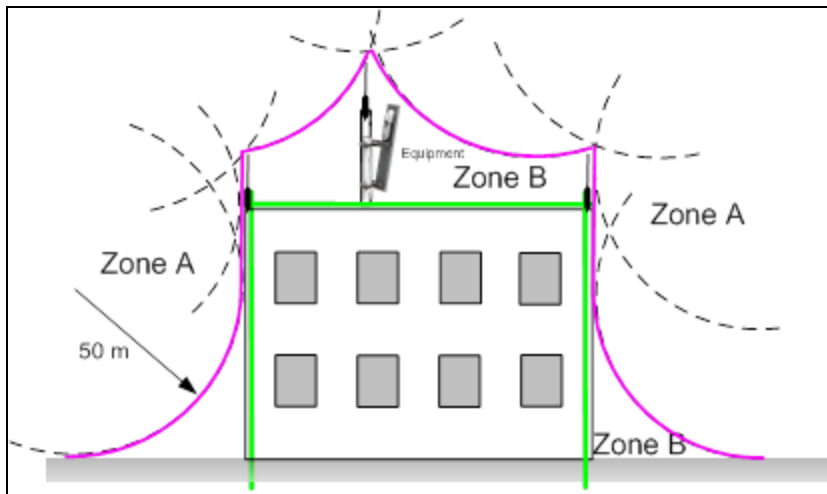


Figure 5: Rolling sphere method to determine the lightning protection zones



Warning

Do not mount equipment in Zone A which can put the equipment, structures, and life at risk.

ePMP 2000

ePMP 2000 Access Point with intelligent filtering and sync

For details of the ePMP 2000 Access Point with Intelligent Filtering and Sync connectorized hardware, see:

- [ePMP 2000 Access Point with Intelligent Filtering and Sync description](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync part numbers](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync mounting bracket](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync interfaces](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync LEDs](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync LEDs](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync heater](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync - external antenna location](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading](#)
- [ePMP 2000 Access Point with Intelligent Filtering and Sync, antennas and antenna cabling](#)

ePMP 2000 Access Point with Intelligent Filtering and Sync description

The ePMP 2000 Access Point with Intelligent Filtering and Sync device is a self-contained transceiver unit that houses both radio and networking electronics. The connectorized unit is designed to work with externally mounted antennas that have high gains to cope with difficult radio conditions. The unit is designed with female RP-SMA 50Ω antenna connections located at the top of the unit and female RP-SMA 50Ω DC-coupled for connection to the optional Smart Antenna (detected upon connection/power on).



Note

To select antennas, RF cables, and connectors for connectorized units, see [ePMP 2000 Access Point with Intelligent Filtering and Sync, antennas and antenna cabling](#).



Figure 6: ePMP 2000 Series Access Point with Intelligent Filtering and Sync

ePMP 2000 Access Point with Intelligent Filtering and Sync part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 1](#) includes the following items:

- 1 x connectorized unit
- 1 x power supply 1000/100/10BASE-TX LAN injector

The GPS-capable parts listed in [Table 1](#) also ship with a GPS antenna.

Table 2: ePMP 2000 Access Point with Intelligent Filtering and Sync part numbers

Cambium description	Cambium part number
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (EU)	C050900A033A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (FCC)	C058900A132A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (no cord)	C050900A031A

Cambium description	Cambium part number
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (EU cord)	C050900A231A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (US cord)	C050900A131A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (EU) (UK cord)	C050900A333A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (UK cord)	C050900A331A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (India cord)	C050900A431A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (China cord)	C050900A531A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW) (Brazil cord)	C050900A631A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW)(Argentina cord)	C050900A731A
ePMP 2000: 5 GHz AP with Intelligent Filtering and Sync (ROW)(ANZ cord)	C050900A831A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (EU)	C050900L033A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (FCC)	C058900L132A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (no cord)	C050900L031A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (EU cord)	C050900L231A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (US cord)	C050900L131A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (EU) (UK cord)	C050900L333A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (UK cord)	C050900L331A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (India cord)	C050900L431A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (China cord)	C050900L531A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW) (Brazil cord)	C050900L631A
ePMP 2000: 5 GHz AP Lite with Intelligent Filtering and Sync (ROW)(Argentina cord)	C050900L731A
ePMP 2000 AP Lite License Key - Upgrade Lite (10 SM) to Full (120 SM)	C050900S2KLA

Table 3: Access Point with Intelligent Filtering and Sync accessory part numbers

Cambium description	Cambium part number
Power supply, 30W, 56V - Gbps support	N000000L034

ePMP 2000 Access Point with Intelligent Filtering and Sync mounting bracket

The ePMP 2000 Access Point with Intelligent Filtering and Sync is designed to be attached to the new Cambium ePMP sector antenna. The new Cambium ePMP sector antenna contains all of the mounting brackets, antenna cabling, and GPS antenna mounting for device installation.



Figure 7: ePMP 2000 Access Point with Intelligent Filtering and Sync mounted to ePMP sector antenna

ePMP 2000 Access Point with Intelligent Filtering and Sync interfaces

The ePMP 2000 Access Point with Intelligent Filtering and Sync interfaces are illustrated in [Figure 1](#) and described in [Table 1](#).

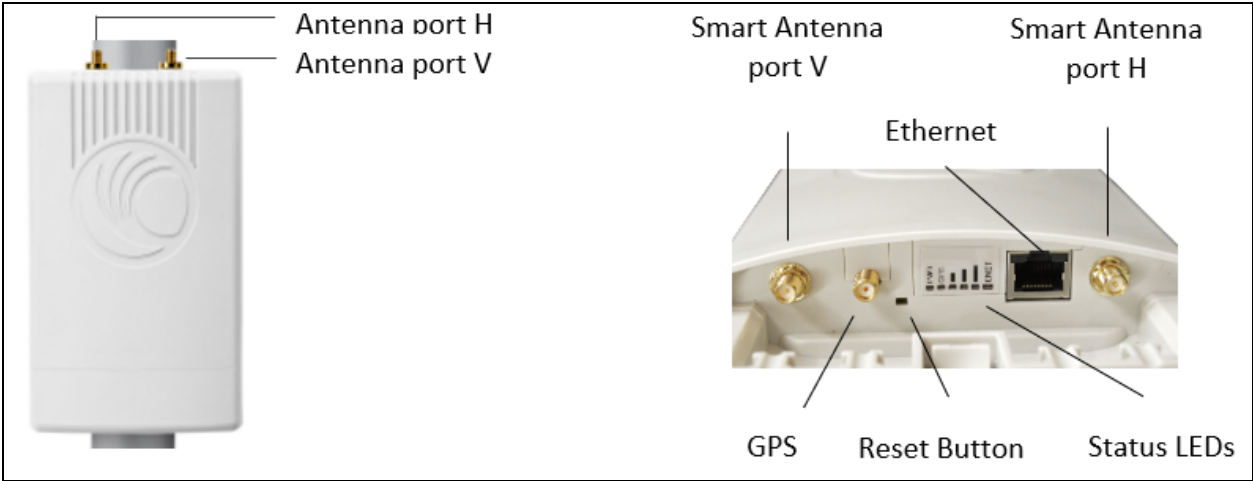

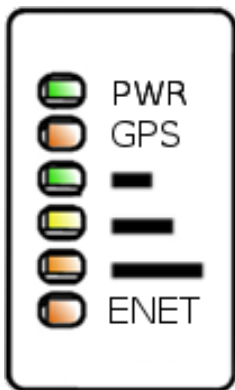


Figure 8: Connectorized Radio with Sync interfaces

Table 4: ePMP 2000 Access Point with Intelligent Filtering and Sync interfaces

Name	Connector	Interface	Description
Antenna port H	RP-SMA, female	Antenna, H polarization	To/from H polarized antenna port
Antenna port V	RP-SMA, female	Antenna, V polarization	To/from V polarized antenna port
Smart Antenna port H	RP-SMA, female	Smart Antenna, H polarization	To/from H polarized Smart Antenna port
Smart Antenna port V	RP-SMA, female	Smart Antenna, V polarization	To/from V polarized Smart Antenna port
Ethernet	RJ45	PoE input	802.3at-compliant.  Note A non-802.3at-compliant power supply may also be used to power the device. The power supply must supply at least 20 Watts.
		10/100/1000BASE-TX Ethernet	Management and data
GPS	SMA, female	Antenna, GPS	To/from GPS antenna
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button .

ePMP 2000 Access Point with Intelligent Filtering and Sync LEDs



LED	Function
POWER	<p>Green: Power is applied to the device</p> <p>Unlit: No power is applied to the device or improper power source</p>
GPS SYNC	<p>Orange: AP has acquired a 1PPS GPS synchronization pulse either from the internal GPS module and antenna or from a connected CMM</p> <p>Unlit: 1PPS GPS not acquired, or Synchronization Source set to Internal (AP operates without sync)</p>
<p>■</p> <p>■ ■</p> <p>■ ■ ■</p>	<p>No LEDs lit: Three or fewer satellites tracked</p> <p>One LED lit: Four or five satellites tracked</p> <p>Two LEDs lit: Six or seven satellites tracked</p> <p>All LEDs lit: Eight or more satellites are tracked</p>
ETH	<p>Once lit, blinking indicates Ethernet activity:</p> <p>Red: 10BASE-TX link</p> <p>Green: 100BASE-TX link</p> <p>Orange: 1000BASE-TX link</p> <p>Unlit: No Ethernet link established</p>

ePMP 2000 Access Point with Intelligent Filtering and Sync specifications

The ePMP 2000 Access Point with Intelligent Filtering and Sync connectorized module conforms to the specifications listed in [Table 1](#) and [Table 2](#).

The connectorized module meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of Access Point with Intelligent Filtering and Sync specifications, see the [ePMP 2000 website](#).

Table 5: ePMP 2000 Access Point with Intelligent Filtering and Sync physical specifications

Category	Specification
Dimensions (H x W x D)	Radio: 22.2 x 12.4 x 4.5 cm (8.75 x 4.9 x 1.75 in) without brackets
Weight	.7 kg (1.5 lbs) without brackets

Table 6: ePMP 2000 Access Point with Intelligent Filtering and Sync environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)

Category	Specification
Wind loading	118 mph (190 kph) maximum. See ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading for a full description.
Humidity	95% condensing
Environmental	IP55

ePMP 2000 Access Point with Intelligent Filtering and Sync heater

At startup, if the ePMP 2000 Access Point with Intelligent Filtering and Sync module temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in [Table 1](#).

Table 7: ePMP 2000 Access Point with Intelligent Filtering and Sync startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C) H	20 minutes
-4° F (-20° C)	6 minutes
14° F (-10° C)	2 minutes, 30 seconds

ePMP 2000 Access Point with Intelligent Filtering and Sync - external antenna location

Find a location for the device and external antenna that meets the following requirements:

- The equipment is high enough to achieve the best radio path.
- People can be kept a safe distance away from the equipment when it is radiating. The safe separation distances are defined in [Calculated distances and power compliance margins](#).
- The equipment is lower than the top of the supporting structure (tower, mast, or building) or its lightning air terminal.
- The location is not subject to excessive wind loading. For more information, see [ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading](#).

ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading

Ensure that the device and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics are available from national meteorological offices.

The device and its mounting bracket are capable of withstanding wind speeds of up to 190 kph (118 mph).

Wind blowing on the device will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of the device. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

$$\text{Force (in pounds)} = 0.0042 Av^2$$

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in [Table 1](#) and [Table 2](#).

Table 8: ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Connectorized with Sector Antenna	0.09	8.5 Kg	15 Kg	23.5 Kg	33.9 Kg	46.1 Kg

Table 9: ePMP 2000 Access Point with Intelligent Filtering and Sync wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Connectorized with Sector Antenna	1	26.9 lb	42 lb	60.1 lb	82.32 lb	107.5 lb

ePMP 2000 Access Point with Intelligent Filtering and Sync software packages

ePMP 2000 Access Point with Intelligent Filtering and Sync devices may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP connectorized radios are named:

- ePMP-GPS_Synced-[Version].tar.gz

ePMP 2000 Access Point with Intelligent Filtering and Sync, antennas and antenna cabling

ePMP 2000 Access Point with Intelligent Filtering and Sync devices require external antennas connected using RF cables (included with Cambium ePMP sector antennas). For details of the antennas and accessories required for a connectorized ePMP installation, see:

- [ePMP 2000 Access Point with Intelligent Filtering and Sync, antennas and antenna cabling](#)
- [Antenna requirements](#)

Antenna requirements

For ePMP 2000 Access Point with Intelligent Filtering and Sync units operating in the USA or Canada 5 GHz bands, choose external antennas from those listed in [Antenna requirement](#). For installations in other countries, the listed antennas are advisory, not mandatory.

FCC and IC approved antennas

For ePMP 2000 Access Point with Intelligent Filtering and Sync units operating in the USA or Canada, choose external antennas from [Table 1](#). These are approved by the FCC for use with the product and are constrained by the following limits:

- 5 GHz – 18 dBi gain



Caution

Using other than approved antennas may cause measurements higher than reported for certification.

This radio transmitter (IC certification number 109W-0005) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (Numéro de certification IC 109W-0005) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Table 10: ePMP 2000 Allowed antennas for installation in USA/Canada

Cambium part number	Antenna Type	Gain (dBi)
C050900D021A	5 GHz Sector Antenna – 90/120 degree	18
C050900D020A	Smart Antenna (complimentary to Sector Antenna, does not replace Sector Antenna)	-

ePMP 1000

ePMP 1000 Connectorized Radio with Sync

For details of the ePMP connectorized hardware, see:

- [ePMP 1000 Connectorized Radio with Sync description](#)
- [ePMP 1000 Connectorized Radio with Sync part numbers](#)
- [ePMP 1000 Connectorized Radio with Sync interfaces](#)
- [ePMP 1000 Connectorized Radio with Sync specifications](#)
- [ePMP 1000 Connectorized Radio with Sync and external antenna location](#)
- [ePMP 1000 Connectorized Radio with Sync wind loading](#)
- [ePMP 1000 Connectorized Radio with Sync software packages](#)

ePMP 1000 Connectorized Radio with Sync description

The connectorized ePMP device is a self-contained transceiver unit that houses both radio and networking electronics. The connectorized unit is designed to work with externally mounted antennas that have high gains. Connectorized units can cope with more difficult radio conditions. The unit is designed with female RP-SMA 50Ω antenna connections located at the top of the unit. An ePMP connectorized unit may function as an Access Point (AP) or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology.

An overview of ePMP 1000 Connectorized Radio with Sync is shown in [Figure 9](#).



Figure 9: ePMP 1000 Series Connectorized Radio with Sync



Note

To select antennas, RF cables, and connectors for connectorized units, see [ePMP 1000 Connectorized Radio with Sync software packages](#).

ePMP 1000 Connectorized Radio with Sync part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 11](#) includes the following items:

- 1 x connectorized unit
- 1 x power supply 1000/100/10BASE-TX LAN injector

The GPS-capable parts listed in [Table 12](#) also ship with a GPS antenna.

Table 11: ePMP 1000 Connectorized Radio with Sync part numbers

Cambium description	Cambium part number
ePMP GPS, Conn - 2.4 GHz - US power cord	C024900A011A
ePMP GPS, Conn - 2.5 GHz - no power cord - Brazil only	C025900A611A
ePMP GPS, Conn - 5 GHz - no power cord - ROW version	C050900A011A
ePMP GPS, Conn - 5 GHz - no power cord - EU version	C050900A013A
ePMP GPS, Conn - 5 GHz - US power cord - FCC version	C058900A112A
ePMP GPS, Conn - 6.4 GHz - no power cord - ROW version	C060900A211A
GPS Sync AP License Key - ePMP 1000 GPS Sync AP License Key - Upgrade Lite (10 SM) to Full (120 SM)	C050900S200A

Table 12: ePMP 1000 Connectorized Radio with Sync accessory part numbers

Cambium description	Cambium part number
ePMP Power Supply for GPS Radio - no cord (spare)	N000900L001B
ePMP Power Supply for non-GPS Radio - no cord (spare)	N000900L002A

ePMP 1000 Connectorized Radio with Sync mounting bracket

The connectorized unit is designed to be attached to a Cambium ePMP sector antenna (see [Table 19](#)). The Cambium ePMP sector antenna contains all of the mounting brackets, antenna cabling, and GPS antenna mounting for device installation.

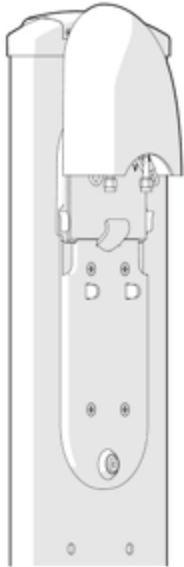


Figure 10: ePMP 1000 Connectorized Radio with Sync sector antenna

ePMP 1000 Connectorized Radio with Sync interfaces

The connectorized radios with sync interfaces are illustrated in [Figure 11](#) and described in [Table 13](#).

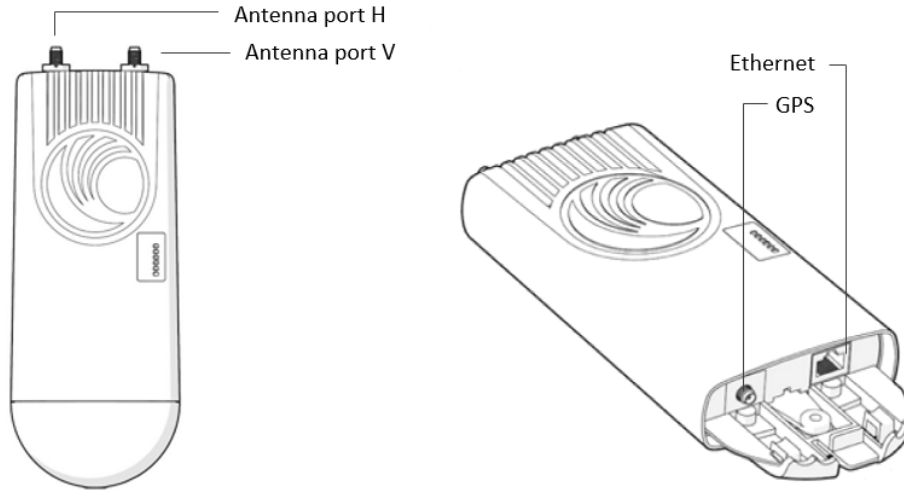
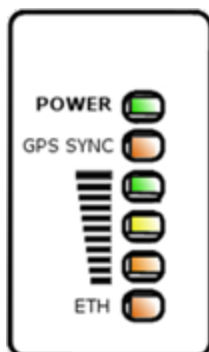



Figure 11: ePMP 1000 Connectorized Radio with Sync interfaces

Table 13: ePMP 1000 Connectorized Radio with Sync interfaces

Name	Connector	Interface	Description
Antenna port H	RP-SMA, female	Antenna, H polarization	To/from H polarized antenna port
Antenna port V	RP-SMA, female	Antenna, V polarization	To/from V polarized antenna port
Ethernet	RJ45	PoE input	802.3af PoE Standard, as well as Proprietary power over Ethernet (PoE), twisted pair (for powering via CMM3/CMM4)
		10/100/1000BASE-TX Ethernet	Management and data
GPS	SMA, female	Antenna, GPS	To/from GPS antenna
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button.

ePMP 1000 Connectorized Radio with Sync LEDs



LED	Function
POWER	<p>Green: Power is applied to the device</p> <p>Unlit: No power is applied to the device or improper power source</p>
GPS SYNC	<p>Orange: AP has acquired a 1PPS GPS synchronization pulse either from the internal GPS module and antenna or from a connected CMM</p> <p>Unlit: 1PPS GPS not acquired, or Synchronization Source set to Internal (AP operates without sync)</p>
	<p>No LEDs lit: Three or fewer satellites tracked</p> <p>One LED lit (bottom): Four or five satellites tracked</p> <p>Two LEDs lit (bottom two): Six or seven satellites tracked</p> <p>All LEDs lit: Eight or more satellites are tracked</p>
ETH	<p>Once lit, blinking indicates Ethernet activity</p> <p>Red: 10BASE-TX link</p> <p>Green: 100BASE-TX link</p> <p>Orange: 1000BASE-TX link</p> <p>Unlit: No Ethernet link established</p>

ePMP 1000 Connectorized Radio with Sync specifications

The ePMP connectorized module conforms to the specifications listed in [Table 14](#) and [Table 15](#).

The connectorized module meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of connectorized radio with sync specifications, see the [ePMP 1000 website](#).

Table 14: ePMP 1000 Connectorized Radio with Sync physical specifications

Category	Specification
Dimensions (H x W x D)	<p>Radio: 227 x 88 x 33 mm (8.9" x 3.5" x 1.3")</p> <p>Antenna: 529 x 124 x 53 mm (20.8" x 4.9" x 2.1")</p>
Weight	<p>0.521 kg (1.15 lbs) without antenna</p> <p>4.5 kg (10 lbs) with antenna</p>

Table 15: ePMP 1000 Connectorized Radio with Sync environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)
Wind loading	118 mph (190 kph) maximum. See ePMP 1000 Connectorized Radio with Sync and external antenna location for a full description.
Humidity	95% condensing
Environmental	IP55

ePMP 1000 Connectorized Radio with Sync heater

At startup, if the ePMP connectorized module temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated, and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in [Table 16](#).

Table 16: ePMP 1000 Connectorized Radio with Sync startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C) H	20 minutes
-4° F (-20° C)	6 minutes
14° F (-10° C)	2 minutes, 30 seconds

ePMP 1000 Connectorized Radio with Sync and external antenna location

Find a location for the device and external antenna that meets the following requirements:

- The equipment is high enough to achieve the best radio path.
- People can be kept a safe distance away from the equipment when it is radiating. The safe separation distances are defined in [Calculated distances and power compliance margins](#).
- The equipment is lower than the top of the supporting structure (tower, mast, or building) or its lightning air terminal.
- The location is not subject to excessive wind loading. For more information, see ePMP 1000 Connectorized Radio with Sync wind loading.

ePMP 1000 Connectorized Radio with Sync wind loading

Ensure that the device and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics are available from national meteorological offices.

The device and its mounting bracket are capable of withstanding wind speeds of up to 190 Kph (118 mph).

Wind blowing on the device will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of the device. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

$$\text{Force (in pounds)} = 0.0042Av^2$$

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in [Table 1](#) and [Table 2](#).

Table 17: ePMP 1000 Connectorized Radio with Sync wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Connectorized	0.13	12.2 Kg	21.7 Kg	34 Kg	49 Kg	66.6 Kg

Table 18: ePMP 1000 Connectorized Radio with Sync wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Connectorized	1.39	37.4 lb	58.4 lb	84.1 lb	114.4 lb	131.4 lb

ePMP 1000 Connectorized Radio with Sync software packages

Connectorized radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP connectorized radios are named:

- ePMP-GPS_Synced-[Version].tar.gz

ePMP 1000 Connectorized Radio with Sync, antennas, and antenna cabling

Connectorized modules require external antennas connected using RF cable (included with Cambium ePMP sector antennas). For details of the antennas and accessories required for a connectorized ePMP

installation, see:

- [ePMP 1000 Antenna requirements](#)
- [ePMP 1000 FCC and IC approved antennas](#)

ePMP 1000 Antenna requirements

For connectorized units operating in the USA or Canada with 2.4 GHz, 5.2 GHz, 5.4 GHz, or 5.8 GHz bands, choose external antennas from those listed in [ePMP 1000 FCC and IC approved antennas](#). For installations in other countries, the listed antennas are advisory, not mandatory.

ePMP 1000 FCC and IC approved antennas

For connectorized units operating in the USA or Canada, choose external antennas from [Table 19](#). These are approved by the FCC for use with the product and are constrained by the following limits:

- 5 GHz - 15 dBi gain
- 2.4 GHz - 15 dBi gain



Caution

Using other than approved antennas may cause measurements higher than reported for certification.

This radio transmitter (IC certification number 109W-0005) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (Numéro de certification IC 109W-0005) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Table 19: ePMP 1000 Allowed antennas for installation in USA/Canada

Cambium part number	Antenna Type	Gain (dBi)
C050900D021A	5 GHz Sector Antenna - 90/120 degree	18
C050900D003A	5 GHz Sector Antenna - 90 degree	15
C050900D002A	5 GHz Sector Antenna - 120 degree	15
C024900D004A	2.4 GHz Sector Antenna - 90 /120 degree	15

ePMP 1000 Integrated Radio

For details of the ePMP 1000 integrated hardware, see:

- [ePMP 1000 Integrated Radio description](#)
- [ePMP 1000 Integrated Radio part numbers](#)

- [ePMP 1000 Integrated Radio mounting bracket](#)
- [ePMP 1000 Integrated Radio interfaces](#)
- [ePMP 1000 Integrated Radio specifications](#)
- [ePMP 1000 Integrated Radio heater](#)
- [ePMP 1000 Integrated Radio wind loading](#)
- [ePMP 1000 Integrated Radio software packages](#)

ePMP 1000 Integrated Radio description

The integrated ePMP 1000 module is a self-contained transceiver unit that houses both radio and networking electronics. An ePMP 1000 integrated unit may function as an Access Point (AP) or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology.

An overview of ePMP 1000 Integrated Radio is shown in [Figure 12](#).



Figure 12: *ePMP 1000 Series Integrated Radio*

ePMP 1000 Integrated Radio part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 20](#) includes the following items:

- 1 x integrated module (with mounting bracket)
- 1 x metal mounting strap
- 1 x Power supply

Table 20: ePMP 1000 Integrated Radio part numbers

Cambium description	Cambium part number
ePMP Integrated - 5 GHz - no power cord - ROW version	C050900C031A
ePMP Integrated - 5 GHz - EU power cord - EU version	C050900P033A
ePMP Integrated - 5 GHz - US power cord - FCC version	C058900C132A
ePMP Integrated - 2.4 GHz - US power cord	C024900C031A

Table 21: ePMP 1000 Integrated Radio accessory part numbers

Cambium description	Cambium part number
ePMP Power Supply for non-GPS Radio - no cord (spare)	N000900L002A

ePMP 1000 Integrated Radio mounting bracket

The ePMP 1000 integrated module is designed to be pole-mounted using the mounting strap and bracket provided in the box with the radio.

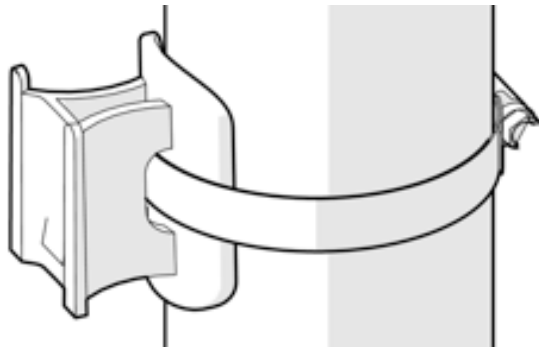


Figure 13: Integrated module mounting bracket

ePMP 1000 Integrated Radio interfaces

The integrated module interfaces are illustrated in [Figure 14](#) and described in [Table 22](#).

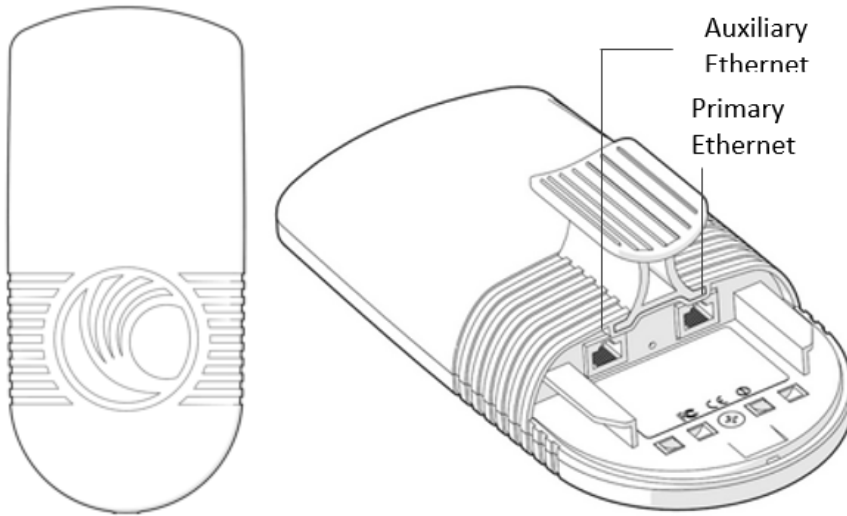
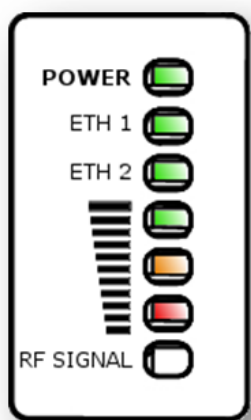



Figure 14: ePMP 1000 Integrated Radio interfaces




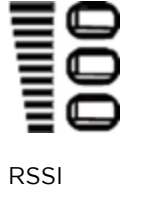
Table 22: ePMP 1000 Integrated Radio interfaces

Port name	Connector	Interface	Description
Primary Ethernet	RJ45	PoE input	Proprietary power over Ethernet (PoE) twisted pair (for powering via CMM3/CMM4)
		10/100BASE-TX Ethernet	Management and data
Auxiliary Ethernet (future release)	RJ45	Cambium proprietary PoE output, data bridging	Proprietary 30V PoE output for auxiliary devices (not 802.3af standard PoE)

ePMP 1000 Integrated Radio LEDs



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH 1	Main/Primary Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100BASE-TX link
ETH 2	Auxiliary/Secondary Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100BASE-TX link
	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning Radio registered: LEDs light to indicate the RSSI level at the device.

			
RSSI > -60 dBm	-70 dBm < RSSI ≤ -60 dBm	-80 dBm < RSSI ≤ -70 dBm	RSSI ≤ -80 dBm

ePMP 1000 Integrated Radio specifications

The ePMP integrated module conforms to the specifications listed in [Table 23](#) and [Table 24](#).

The integrated device meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of integrated radio specifications, see the [ePMP 1000 website](#).

Table 23: ePMP 1000 Integrated Radio physical specifications

Category	Specification
Dimensions (H x W x D)	Radio: 29.1 x 14.5 x 8.3 cm (11.4 x 5.7 x 3.3 in)
Weight	0.49 kg (1.1 lbs)

Table 24: ePMP 1000 Integrated Radio environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (131°F)
Wind loading	90 mph (145 kph) maximum. See ePMP 1000 Integrated Radio heater for a full description.
Humidity	95% condensing
Environmental	IP55

ePMP 1000 Integrated Radio heater

Upon power-on, if the ePMP integrated module device temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the integrated module continues its startup sequence.

The effect on integrated module startup time at various temperatures is defined in [Table 25](#).

Table 25: ePMP 1000 Integrated module startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C)	4 minutes
-4° F (-20° C)	2 minutes
14° F (-10° C)	1 minute, 30 seconds

ePMP 1000 Integrated Radio wind loading

Ensure that the integrated module and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics must be available from national meteorological offices.

The integrated module and its mounting bracket are capable of withstanding wind speeds of up to 145 Kph (90 mph).

Wind blowing on the integrated module will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of the integrated module. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

$$\text{Force (in pounds)} = 0.0042Av^2$$

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

Applying these formulae to the ePMP integrated module at different wind speeds, the resulting wind loadings are shown in [Table 26](#) and [Table 27](#).

Table 26: ePMP 1000 Integrated Radio wind loading (Kg)

Type of ePMP module	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Integrated	0.042	4 Kg	7 Kg	11 Kg	15.8 Kg	21.6 Kg

Table 27: ePMP 1000 Integrated Radio wind loading (lb)

Type of ePMP module	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Integrated	0.45	12.1 lb	18.9 lb	27.2 lb	37 lb	42.5 lb

ePMP 1000 Integrated Radio software packages

Integrated radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP integrated radios are named:

- ePMP-NonGPS_Synced-[Version].tar.gz

ePMP 1000 Connectorized Radio

For details of the ePMP 1000 connectorized hardware, see:

- [ePMP 1000 Connectorized Radio description](#)
- [ePMP 1000 Connectorized Radio part numbers](#)
- [ePMP 1000 Connectorized Radio Interfaces](#)
- [ePMP 1000 Connectorized Radio specifications](#)
- [ePMP 1000 Connectorized Radio and external antenna location](#)
- [ePMP 1000 Connectorized Radio wind loading](#)
- [Connectorized Radio software packages](#)
- [ePMP 1000 Connectorized Radio antennas and antenna cabling](#)

ePMP 1000 Connectorized Radio description

The connectorized ePMP 1000 device is a self-contained transceiver unit that houses both radio and networking electronics. The connectorized unit is designed to work with externally mounted antennas that have high gains. Connectorized units can cope with more difficult radio conditions. The unit is designed with female RP-SMA 50Ω antenna connections located at the top of the unit. An ePMP 1000 connectorized unit may function as an Access Point (AP) or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology.

An overview of ePMP 1000 Series Connectorized Radio is shown in [Figure 15](#).



Figure 15: ePMP 1000 Series Connectorized Radio



Note

To select antennas, RF cables, and connectors for connectorized units, see [ePMP 1000 Connectorized Radio antennas and antenna cabling](#).

ePMP 1000 Connectorized Radio part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in Table 28 includes the following items:

- One connectorized unit
- One power supply 100/10BASE-TX LAN injector

Table 28: ePMP 1000 Connectorized Radio part numbers

Cambium description	Cambium part number
ePMP Conn - 2.4 GHz - US power cord	C024900A021A
ePMP Conn - 2.5 GHz - no power cord - Brazil only	C025900A611A
ePMP Conn - 5 GHz - no power cord - ROW version	C050900A021A
ePMP Conn - 5 GHz - EU power cord - EU version	C050900A023A
ePMP Conn - 5 GHz - US power cord - FCC version	C058900A122A
ePMP Conn - 6.4 GHz - no power cord - ROW version	C060900A221A

Table 29: ePMP 1000 Connectorized Radio accessory part numbers

Cambium description	Cambium part number
ePMP Power Supply for non-GPS Radio - no cord (spare)	N000900L002A

ePMP 1000 Connectorized Radio mounting bracket

The ePMP 1000 Connectorized unit is designed to be attached to a Cambium ePMP sector antenna or with a non-Cambium antenna.

An overview of connectorized radio sector antenna is shown in Figure 16.

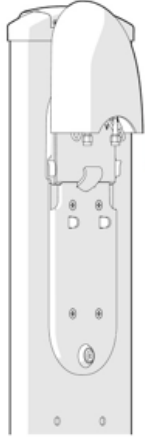


Figure 16: Connectorized radio sector antenna

ePMP 1000 Connectorized Radio Interfaces

The connectorized radio with interfaces is illustrated in Figure 17 and described in Table 30.

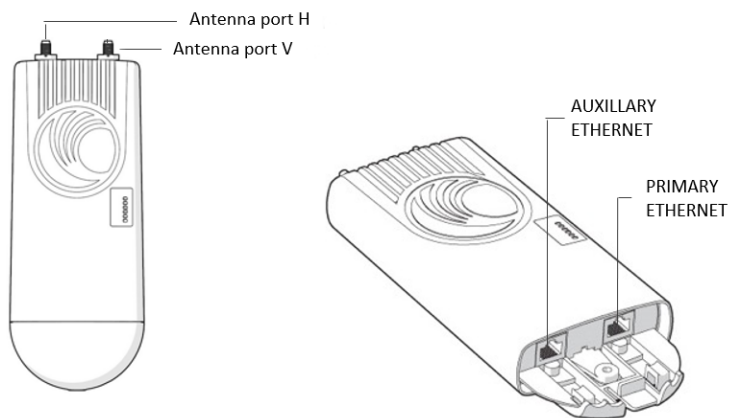
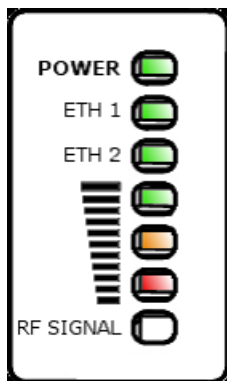


Figure 17: Connectorized radio interfaces


Table 30: ePMP 1000 Connectorized radio interfaces

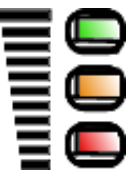



Name	Connector	Interface	Description
Antenna port H	RP-SMA, female	Antenna, H polarization	To/from H polarized antenna port
Antenna port V	RP-SMA, female	Antenna, V polarization	To/from V polarized antenna port
Primary Ethernet	RJ45	PoE input	Proprietary power over Ethernet (PoE) twisted pair (for powering via CMM3/CMM4)
		10/100BASE-TX Ethernet	Management and data
Auxiliary Ethernet (future release)	RJ45	Cambium propriety PoE output, data bridging	Propriety 30V PoE output for auxiliary devices (not 802.3af standards Poe)
Reset Button	Physical button	N/A	For resetting the radio and for resetting the radio back to its factory default configuration, see Using the device external reset button.

ePMP 1000 Connectorized Radio LEDs



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH 1	Main/Primary Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100BASE-TX link
ETH 2	Auxiliary/Secondary Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100BASE-TX link

LED	Function
	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning Radio registered: LEDs light to indicate the RSSI level at the device.
	Reserved for future release

			
RSSI > -60 dBm	-70 dBm < RSSI ≤ -60 dBm	-80 dBm < RSSI ≤ -70 dBm	RSSI ≤ -80 dBm

ePMP 1000 Connectorized Radio specifications

The ePMP connectorized radio conforms to the specifications listed in [Table 31](#) and [Table 32](#).

The connectorized module meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of connectorized radio specifications, see the [ePMP 1000 website](#).

Table 31: ePMP 1000 Connectorized radio physical specifications

Category	Specification
Dimensions (H x W x D)	Radio: 227 x 88 x 33 mm (8.9" x 3.5" x 1.3") Antenna: 529 x 124 x 53 mm (20.8" x 4.9" x 2.1")
Weight	0.521 kg (1.15 lbs) without antenna 4.5 kg (10 lbs) with antenna

Table 32: ePMP 1000 Connectorized radio environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)

Category	Specification
Wind loading	118 mph (190 kph) maximum. See ePMP 1000 Connectorized Radio wind loading for a full description.
Humidity	95% condensing
Environmental	IP55

ePMP 1000 Connectorized Radio heater

On startup, if the ePMP 1000 Connectorized radio temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not transfer heat to the device until the startup completes. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in [Table 33](#).

Table 33: ePMP 1000 Connectorized radio startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C) H	20 minutes
-4° F (-20° C)	6 minutes
14° F (-10° C)	2 minutes, 30 seconds

ePMP 1000 Connectorized Radio and external antenna location

Find a location for the device and external antenna that meets the following requirements:

- The equipment is high enough to achieve the best radio path.
- People are a safe distance away from the equipment when it is radiating. The safe separation distances are defined in [Calculated distances and power compliance margins](#).
- The equipment is lower than the top of the supporting structure (tower, mast, or building) or its lightning air terminal.
- The location is not subjected to excessive wind loading. For more information, see [ePMP 1000 Connectorized Radio wind loading](#).

ePMP 1000 Connectorized Radio wind loading

Ensure that the device and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics must be available from national meteorological offices.

The device and its mounting bracket are capable of withstanding wind speeds of up to 190 kph (118 mph).

Wind speeds on the device subjects the mounting structure to significant lateral force. The magnitude of the force depends on both the wind strength and surface area of the device. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

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

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in [Table 34](#) and [Table 35](#).

Table 34: ePMP 1000 Connectorized radio wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Connectorized	0.13	12.2 Kg	21.7 Kg	34 Kg	49 Kg	66.6 Kg

Table 35: ePMP 1000 Connectorized radio wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Connectorized	1.39	37.4 lb	58.4 lb	84.1 lb	114.4 lb	131.4 lb

Connectorized Radio software packages

Connectorized radio may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP 1000 Un-synced connectorized radio are named:

- ePMP-NonGPS_Synced-[Version].tar.gz

ePMP 1000 Connectorized Radio antennas and antenna cabling

Connectorized radio requires external antennas connected using RF cable (included with Cambium ePMP sector antennas). For details of the antennas and accessories required for a connectorized ePMP installation, see:

- [ePMP 1000 Antenna requirements](#)
- [ePMP 1000 FCC and IC approved antennas](#)

ePMP 1000 Antenna requirements

For connectorized units operating in the USA or Canada with 2.4 GHz, 5.4 GHz, or 5.8 GHz bands, choose external antennas from those listed in [ePMP 1000 FCC and IC approved antennas](#). For installations in other countries, the listed antennas are advisory, not mandatory.

ePMP 1000 FCC and IC approved antennas

For connectorized units operating in the USA or Canada, choose external antennas from [Table 36](#). These are approved by the FCC for use with the product and are constrained by the following limits:

- 5 GHz - 15 dBi gain
- 2.4 GHz - 15 dBi gain



Caution

Using other than approved antennas may cause measurements higher than reported for certification.

This radio transmitter (IC certification number 109W-0005) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

- Le présent émetteur radio (Numéro de certification IC 109W-0005) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Table 36: ePMP 1000 allowed antennas for installation in USA/Canada - 5 GHz

Cambium part number	Antenna Type	Gain (dBi)
C050900D003A	5 GHz Sector Antenna - 90 degree	15
C050900D002A	5 GHz Sector Antenna - 120 degree	15
C024900D004A	2.4 GHz Sector Antenna - 90 /120 degree	15

Force 130

For details of the ePMP Force 130 hardware, see:

- [Force 130 description](#)
- [Force 130 part numbers](#)
- [Force 130 mounting](#)
- [Force 130 interfaces](#)

- [Force 180 LEDs](#)
- [Force 130 specifications](#)
- [Force 130 software packages](#)

Force 130 description

The Force 130 integrated module available in both 5 GHz and 2.4 GHz is a self-contained transceiver unit that houses both radio and networking electronics. An ePMP Force 130 unit may function as an AP or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology. It is typically deployed as an SM in a PMP system.

An overview of Force 130 is shown in [Figure 18](#).



Figure 18: ePMP Series Force 130

Force 130 part numbers

Choose the correct regional variant, one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 37](#) includes the following items:

- 1 x Force 130 module (with mounting bracket)
- 2 x plastic mounting strap
- Power supply

Table 37: Force 130 part numbers

Cambium description	Cambium part number
ePMP 2.4 GHz Force 130 SM (ROW) (no cord)	C024900C603A
ePMP 2.4 GHz Force 130 SM (ROW) (US cord)	C024900C604A
ePMP 2.4 GHz Force 130 SM (ROW) (EU cord)	C024900C605A

Cambium description	Cambium part number
ePMP 2.4 GHz Force 130 SM (ROW) (UK cord)	C024900C606A
ePMP 2.4 GHz Force 130 SM (ROW) (India cord)	C024900C607A
ePMP 2.4 GHz Force 130 SM (ROW) (China cord)	C024900C609A
ePMP 2.4 GHz Force 130 SM (ROW) (Brazil cord)	C024900C610A
ePMP 2.4 GHz Force 130 SM (ROW) (Argentina cord)	C024900C611A
ePMP 2.4 GHz Force 130 SM (ROW) (ANZ cord)	C024900C612A
ePMP 2.4 GHz Force 130 SM (ROW) (South Africa cord)	C024900C613A
ePMP 2.4 GHz Force 130 SM (ROW) (No PSU)	C024900C614A
ePMP 5 GHz Force 130 SM (ROW) (ANZ cord)	C050900C513A
ePMP 5 GHz Force 130 SM (EU) (EU cord)	C050900C502A
ePMP 5 GHz Force 130 SM (EU) (UK cord)	C050900C503A
ePMP 5 GHz Force 130 SM (ROW) (no cord)	C050900C504A
ePMP 5 GHz Force 130 SM (ROW) (US cord)	C050900C505A
ePMP 5 GHz Force 130 SM (ROW) (EU cord)	C050900C506A
ePMP 5 GHz Force 130 SM (ROW) (UK cord)	C050900C507A
ePMP 5 GHz Force 130 SM (ROW) (India cord)	C050900C508A
ePMP 5 GHz Force 130 SM (India) (India cord)	C050900C509A
ePMP 5 GHz Force 130 SM (ROW) (China cord)	C050900C510A
ePMP 5 GHz Force 130 SM (ROW) (Brazil cord)	C050900C511A
ePMP 5 GHz Force 130 SM (ROW) (Argentina cord)	C050900C512A
ePMP 5 GHz Force 130 SM (ROW) (ANZ cord)	C050900C513A
ePMP 5 GHz Force 130 SM (ROW) (South Africa cord)	C050900C514A
ePMP 5 GHz Force 130 SM (ROW) (No PSU)	C050900C515A

Force 130 mounting

The Force 130 module is designed to be pole-mounted using the mounting straps provided in the box with the radio. Force 130 module mounting steps are shown in [Figure 19](#).

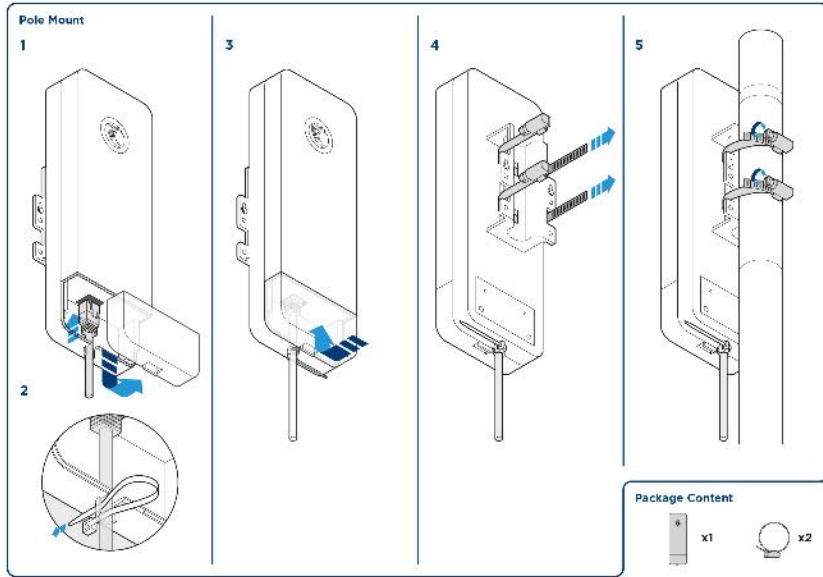


Figure 19: Force 130 module mounting

Force 130 interfaces

The Force 130 module interfaces are illustrated in Figure 20 and described in Table 38.

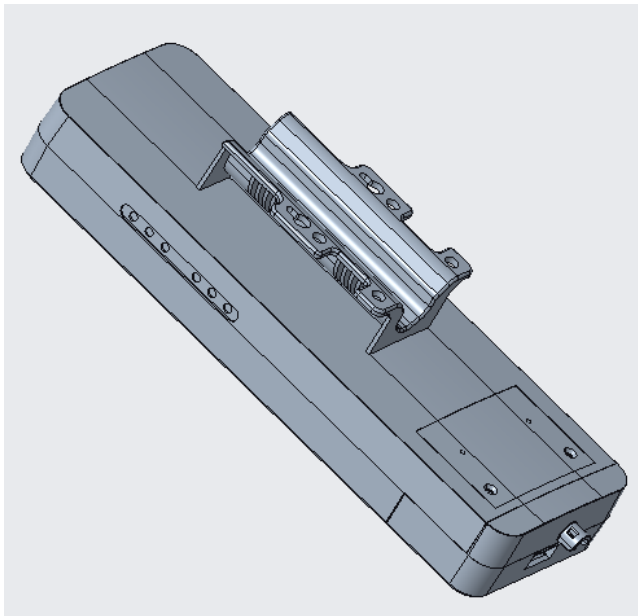
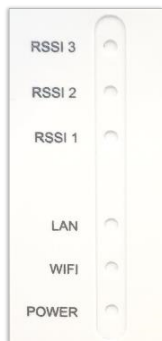



Figure 20: Force 130 interfaces

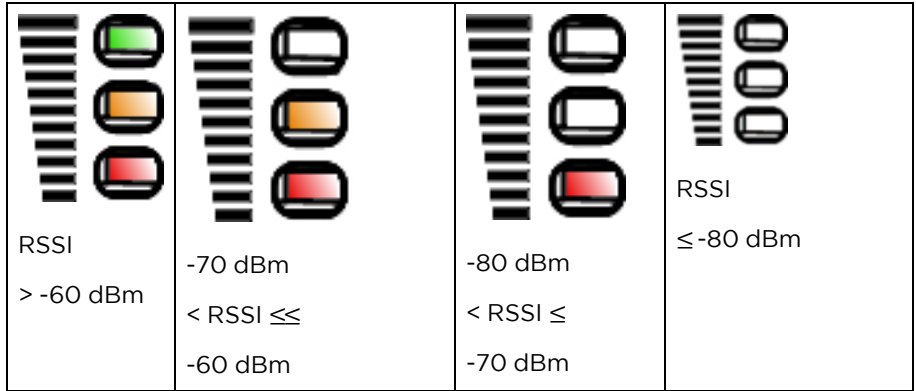
Table 38: Force 130 interfaces

Port name	Connector	Interface	Description
Ethernet	RJ45	24V PoE input	10/100BASE-T
		100BASE-TX Ethernet	Management and data
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button .

Force 130 LEDs



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
WiFi	XXX
LAN	XXX
 RF SIGNAL	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning Radio registered: LEDs light to indicate the RSSI level at the device.



Force 130 specifications

The Force 130 module conforms to the specifications listed in [Table 44](#) and [Table 45](#).

The device meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of Force 130 specifications, see [Force 130 website](#).

Table 39: Force 130 physical and environmental specifications

Category	Specification
Dimensions (H x W x D)	235 x 77 x 58 mm
Weight	0.35 kg (0.88 lbs)
Surge Suppression	1 Joule Integrated
Environment	IP55
Temperature	-30°C to +55°C (-22°F to +122°F)
Power consumption	8 W Maximum, 5 W Typical
Input Voltage	24 V; uses standard passive PoE injectors at 24V. Not compatible with 29V supplies

Table 40: Force 130 Performance and Security specifications

Category	Specification
ARQ	Yes
Nominal Receive Sensitivity (w/FEC) @20 MHz Channel	MCS0 -88 dBm to MCS15 = -70 dBm at MCS7 for 20 MHz
Nominal Receive Sensitivity (w/FEC) @40 MHz Channel	MCS0 = -86 dBm to MCS15 = -68 dBm at MCS7 for 40 MHz
Modulation Levels (Adaptive)	MCS0 (BPSK) to MCS15 (64QAM 5/6)
Quality of Service	Three-level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Address, Broadcast, Multicast, and Station Priority
Transmit Power Range	+3 to 31 dBm (combined, to regional EIRP limit) (1 dB interval)
Antenna Gain	12 dBi
Security Encryption	128-bit AES (CCMP mode)

Table 41: Force 130 Antenna specifications

Category	Specification
Frequency Range	2402 - 2472 MHz
Antenna Type	Flat pane
Peak Gain	12 dBi
3dB Beamwidth-Azimuth	45 degrees
3dB Beamwidth-Elevation	15 degrees

Force 130 software packages

Force 130 radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP Force 130 are named:

- ePMP-NonGPS_Synced-[version].tar.gz

Force 180

For details of the ePMP Force 180 hardware, see:

- [Force 180 description](#)
- [Force 180 part numbers](#)
- [Force 180 mounting bracket](#)

- [Force 180 interfaces](#)
- [Force 180 LEDs](#)
- [Force 180 specifications](#)
- [Force 180 heater](#)
- [Force 180 wind loading](#)
- [Force 180 software packages](#)

Force 180 description

The Force 180 integrated module is a self-contained transceiver unit that houses both radio and networking electronics. An ePMP Force 180 unit may function as an AP or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology. It is typically deployed as an SM in a PMP system.

An overview of ePMP Series Force 180 is shown in [Figure 21](#).



Figure 21: ePMP Series Force 180

Force 180 part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 42](#) includes the following items:

- 1 x Force 180 module (with mounting bracket)
- 1 x metal mounting strap
- 1 x Power supply

Table 42: Force 180 part numbers

Cambium description	Cambium part number
ePMP 5 GHz Force 180 Integrated Radio (FCC) (US cord)	C058900C072A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (no cord)	C050900C071A
ePMP 5 GHz Force 180 Integrated Radio (EU) (EU cord)	C050900C073A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (US cord)	C050900C171A

Cambium description	Cambium part number
ePMP 5 GHz Force 180 Integrated Radio (ROW) (EU cord)	C050900C271A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (UK cord)	C050900C371A
ePMP 5 GHz Force 180 Integrated Radio (EU) (UK cord)	C050900C373A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (India cord)	C050900C471A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (China cord)	C050900C571A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (Brazil cord)	C050900C671A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (Argentina cord)	C050900C771A
ePMP 5 GHz Force 180 Integrated Radio (ROW) (ANZ cord)	C050900C871A
ePMP 2.4 GHz Force 180 Integrated Radio (ROW) (no cord)	C060900C271A

Force 180 mounting bracket

The Force 180 module is designed to be pole-mounted using the mounting strap and bracket provided in the box with the radio. Force 180 module mounting bracket is shown in [Figure 22](#).

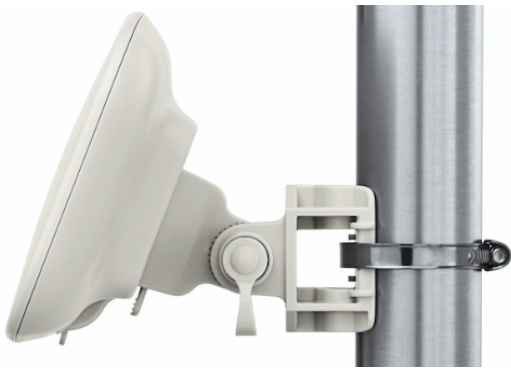


Figure 22: Force 180 module mounting bracket

Force 180 interfaces

The Force 180 module interfaces are illustrated in [Figure 23](#) and described in [Table 43](#).

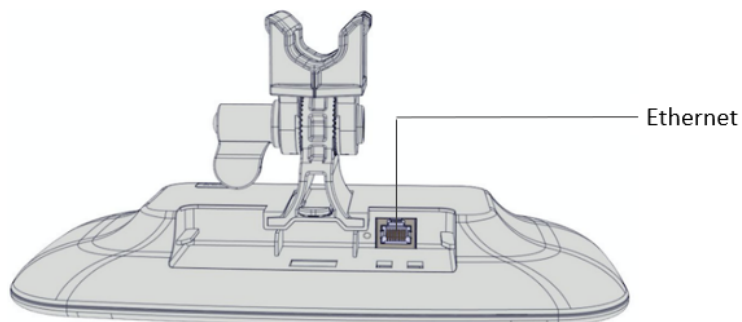



Figure 23: Force 180 interfaces

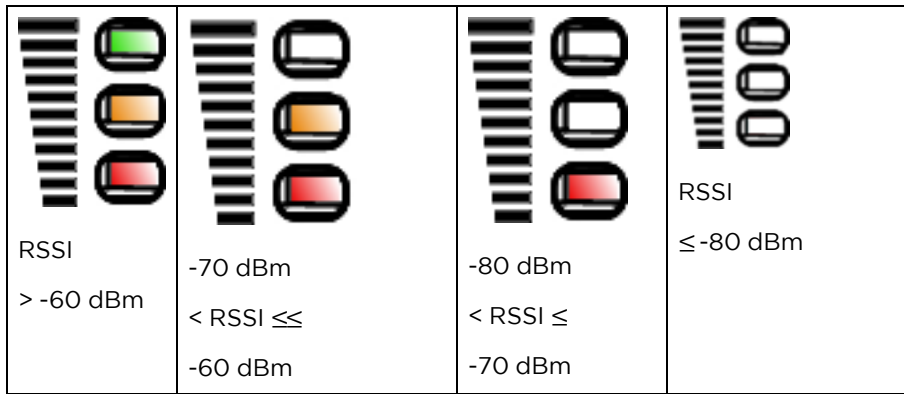
Table 43: Force 180 interfaces

Port name	Connector	Interface	Description
Ethernet	RJ45	PoE input	10/100/1000BASE-T, Compatible with Cambium PoE pinouts (V+ = 7 & 8, Return = 4 & 5) and Standard PoE pinouts (V+ = 4 & 5, Return = 7 & 8)
		10/100/1000BASE-TX Ethernet	Management and data
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button .

Force 180 LEDs



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH	Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100/1000BASE-TX link
 RF SIGNAL	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning Radio registered: LEDs light to indicate the RSSI level at the device.



Force 180 specifications

The Force 180 module conforms to the specifications listed in [Table 44](#) and [Table 45](#).

The device meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of Force 180 specifications, see the [ePMP 1000 website](#).

Table 44: Force 180 physical specifications

Category	Specification
Dimensions (H x W x D)	Radio: 12.5 x 25.1 x 11.9 cm (4.9 x 9.9 x 4.7 in) – with mounting bracket attached Radio: 12.5 x 25.1 x 4 cm (4.9 x 9.9 x 1.6 in) – without mounting bracket attached
Weight	0.50 kg (1.1 lbs)

Table 45: Force 180 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to $+60^{\circ}\text{C}$ (140°F)
Wind loading	90 mph (145 kph) maximum. See Force 180 wind loading for a full description.
Humidity	95% condensing
Environmental	IP55

Force 180 heater

Upon power-on, if the ePMP Force 180 device temperature is at or below 32°F (0°C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32°F (0°C), the heater is deactivated and the integrated module continues its startup sequence.

The effect on Force 200 startup time at various temperatures is defined in [Table 46](#).

Table 46: Force 180 startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C)	4 minutes
-4° F (-20° C)	2 minutes
14° F (-10° C)	1 minute, 30 seconds

Force 180 wind loading

Ensure that the Force 180 and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics must be available from national meteorological offices.

The Force 180 and its mounting bracket are capable of withstanding wind speeds of up to 145 Kph (90 mph).

Wind blowing on the Force 180 will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of Force 180. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

$$\text{Force (in pounds)} = 0.0042Av^2$$

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

Applying these formulae to the ePMP Force 180 at different wind speeds, the resulting wind loadings are shown in [Table 47](#) and [Table 48](#).

Table 47: Force 180 wind loading (Kg)

Type of ePMP module	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Force 180	0.031	3 Kg	5.2 Kg	8.2 Kg	11.8 Kg	16 Kg

Table 48: Force 180 wind loading (lb)

Type of ePMP module	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Force 180	0.33	9 lb	14.1 lb	20.3 lb	27.7 lb	31.8 lb

Force 180 software packages

Force 180 radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP Force 180 are named:

- ePMP-NonGPS_Synced-[Version].tar.gz

Force 190

For details of the ePMP Force 190 hardware, see:

- [Force 190 description](#)
- [Force 190 part numbers](#)
- [Force 190 mounting bracket](#)
- [Force 190 mounting bracket](#)
- [Force 190 LEDs](#)
- [Force 190 specifications](#)
- [Force 190 specifications](#)
- [Force 190 heater](#)
- [Force 190 software packages](#)

Force 190 description

The Force 190 integrated dish is a self-contained transceiver unit that houses both radio, parabolic dish, and networking electronics. An ePMP Force 190 unit may function as an Access Point (AP) or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology. It is typically deployed as an SM in a PMP system and either Master or Slave in a PTP system.

An overview of ePMP Series Force 190 is shown in [Figure 24](#)



Figure 24: ePMP Series Force 190

Force 190 part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 49](#) includes the following items for the Force 190 Radio Assembly.

- 1 x Power Cord (if applicable)
- 1 x Power Supply
- 1 x Side Reflector Panels (Qty. 2)
- 1 x Top Reflector Panel
- 1 x Bottom Reflector Panel
- 1 x Rear Housing
- 1 x Pole Mounting Bracket
- 1 x Pole Clamp

Table 49: Force 190 part numbers

Cambium description	Cambium part number
ePMP Force 190 5 GHz Subscriber Module (FCC) (US Cord)	C058900C082A
ePMP Force 190 5 GHz Subscriber Module (EU) (EU Cord)	C050900C083A
ePMP Force 190 5 GHz Subscriber Module (EU) (UK Cord)	C050900C873A
ePMP Force 190 5 GHz Subscriber Module (RoW) (No Cord)	C050900C081A
ePMP Force 190 5 GHz Subscriber Module (RoW) (US Cord)	C050900C181A
ePMP Force 190 5 GHz Subscriber Module (RoW) (EU Cord)	C050900C281A
ePMP Force 190 5 GHz Subscriber Module (RoW) (India Cord)	C050900C481A
ePMP Force 190 5 GHz Subscriber Module (RoW) (China Cord)	C050900C581A
ePMP Force 190 5 GHz Subscriber Module (RoW) (Brazil Cord)	C050900C681A
ePMP Force 190 5 GHz Subscriber Module (RoW) (Type-N Plug Cord)	C050900C781A
ePMP Force 190 5 GHz Subscriber Module (RoW) (ANZ Cord)	C050900C881A
ePMP Force 190 5 GHz Subscriber Module (RoW) (No PSU)	C050900C981A

Force 190 mounting bracket

The Force 190 module is designed to be pole-mounted using the mounting bracket and clamp assembly provided in the box with the radio. Force 190 mounting is shown in [Figure 25](#) and [Figure 26](#).



Figure 25: Force 190 mounting bracket (clamp insertion)

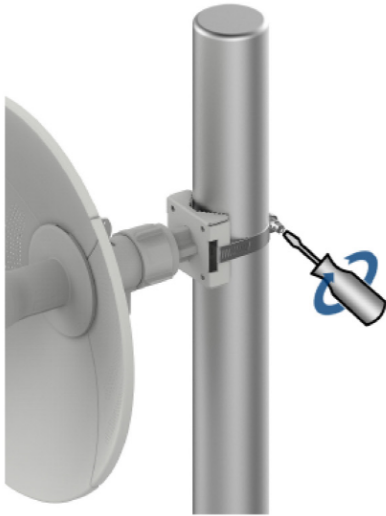


Figure 26: Force 190 mounting bracket (clamp securing)

Force 190 interfaces

The Force 190 module interfaces are illustrated in [Figure 27](#) and described in [Table 50](#).



Figure 27: Force 190 interfaces


Table 50: Force 190 interfaces





Port name	Connector	Interface	Description
Ethernet	RJ45	PoE input	10/100/1000BASE-T, Compatible with Cambium PoE pinouts (V+ = 7 & 8, Return = 4 & 5) and Standard PoE pinouts (V+ = 4 & 5, Return = 7 & 8)
		10/100BASE-TX Ethernet	Management and data
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button .

Force 190 LEDs



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH	Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100/1000BASE-TX link

LED	Function
	<p>Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning</p> <p>Radio registered: LEDs light to indicate the RSSI level at the device.</p>

 <p>RSSI > -60 dBm</p>	 <p>-70 dBm < RSSI ≤ -60 dBm</p>	 <p>-80 dBm < RSSI < -70 dBm</p>	 <p>RSSI ≤ -80 dBm</p>
--	--	---	---

Force 190 specifications

The Force 190 module conforms to the specifications listed in [Table 51](#) and [Table 52](#).

The device meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of Force 190 specifications, see the [ePMP 1000 website](#).

Table 51: Force 190 physical specifications

Category	Specification
Dimensions (Dia x Depth)	35 x 28 cm (13.5 x 11.2 in)
Weight	1.0 kg (2.2 lbs)

Table 52: Force 190 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (140°F) - with radome attached maximum temperature is +47°C (116°F)
Wind loading	70 mph (125 kph) maximum. See Force 190 heater for a full description.
Humidity	95% condensing
Environmental	IP55

Force 190 heater

Upon power-on, if the ePMP Force 190 device temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the Force 190 module continues its startup sequence.

The effect on Force 190 startup time at various temperatures is defined in [Table 53](#).

Table 53: Force 190 startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C)	4 minutes
-4° F (-20° C)	2 minutes
14° F (-10° C)	1 minute, 30 seconds

Force 190 wind loading

Ensure that the Force 190 and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics must be available from national meteorological offices.

The Force 190 and its mounting bracket are capable of withstanding wind speeds of up to 125 Kph (70 mph).

Wind blowing on the Force 190 will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of the integrated module. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

$$\text{Force (in pounds)} = 0.0042Av^2$$

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

Applying these formulae to the ePMP Force 200 at different wind speeds, the resulting wind loadings are shown in [Table 54](#) and [Table 55](#).

Table 54: Force 190 wind loading (Kg)

Type of ePMP module	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Force 190	0.12	2.8 Kg	7.8 Kg	15.3 Kg	25.4 Kg	37.9 Kg

Table 55: Force 190 wind loading (lb)

Type of ePMP module	Largest surface area (square feet)	Wind speed (miles per hour)				
		30	50	70	90	110
Force 190	1.05	4 lb	11 lb	21.6 lb	35.7 lb	53.4 lb

Force 190 software packages

Force 190 radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP Force 190 are named:

- ePMP-NonGPS_Synced-[Version].tar.gz

Force 200

For details of the ePMP Force 200 hardware, see:

- [Force 200 description](#)
- [Force 200 part numbers](#)
- [Force 200 mounting bracket](#)
- [Force 200 interfaces](#)
- [Force 200 LEDs](#)
- [Force 200 specifications](#)
- [Force 200 heater](#)
- [Force 200L wind loading](#)
- [Force 200 software packages](#)

Force 200 description

The Force 200 integrated dish is a self-contained transceiver unit that houses both radio, parabolic dish, and networking electronics. An ePMP Force 200 unit may function as an AP or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology. It is typically deployed as an SM in a PMP system and either Master or Slave in a PTP system.

An overview of ePMP Series Force 200 is shown in [Figure 28](#) and [Figure 29](#).



Figure 28: ePMP Series Force 200



Figure 29: ePMP Series Force 200 (with optional radome – sold separately)

Force 200 part numbers

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 56](#) includes the following items for the Force 200:

- 1 x Radio Assembly
- 1 x Power Cord (if applicable)
- 1 x Power Supply
- 1 x Dish
- 1 x Pole Bracket Assembly
- 1 x 200 Pole Clamp Assembly
- 4 x M6 Bolts

Table 56: Force 200 part numbers

Cambium description	Cambium part number
ePMP 5 GHz Force 200AR5-25 High Gain Radio (FCC) (US cord)	C058900C062A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (no cord)	C050900C061A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (EU) (EU cord)	C050900C063A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (US cord)	C050900C161A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (EU cord)	C050900C261A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (UK cord)	C050900C361A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (EU) (UK cord)	C050900C363A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (India cord)	C050900C461A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (China/ANZ cord)	C050900C561A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (Brazil cord)	C050900C661A
ePMP 5 GHz Force 200AR5-25 High Gain Radio (ROW) (Argentina cord)	C050900C761A
ePMP 2.4 GHz Force 200AR2-25 High Gain Radio (US cord)	C024900C161A
ePMP 2.4 GHz Force 200AR2-25 High Gain Radio (EU cord)	C024900C261A
ePMP Force 200 Radome	N000900L021A

Force 200 mounting bracket

The Force 200 module is designed to be pole-mounted using the mounting bracket and clamp assembly provided in the box with the radio.

An overview of Force 200 mounting bracket is shown in [Figure 30](#) and [Figure 31](#).



Figure 30: Force 200 mounting bracket (side)



Figure 31: Force 200 mounting bracket (back)

Force 200 interfaces

The Force 200 module interfaces are illustrated in Figure 32 and described in Table 57.

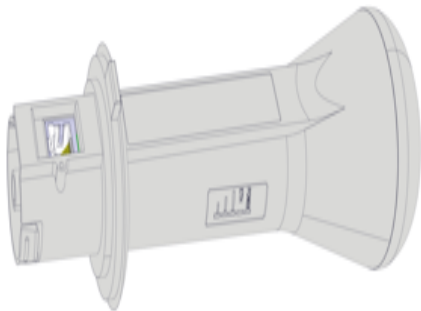


Figure 32: Force 200 interfaces


Table 57: Force 200 interfaces





Port name	Connector	Interface	Description
Ethernet	RJ45	PoE input	10/100/1000BASE-T, Compatible with Cambium PoE pinouts (V+ = 7 & 8, Return = 4 & 5) and Standard PoE pinouts (V+ = 4 & 5, Return = 7 & 8)
		10/100/1000BASE-TX Ethernet	Management and data

Port name	Connector	Interface	Description
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button .

Force 200 LEDs



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH	Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100/1000BASE-TX link
 RF SIGNAL	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning Radio registered: LEDs light to indicate the RSSI level at the device.

			
RSSI > -60 dBm	-70 dBm < RSSI ≤ -60 dBm	-80 dBm < RSSI ≤ -70 dBm	RSSI ≤ -80 dBm

Force 200 specifications

The Force 200 module conforms to the specifications listed in [Table 58](#) and [Table 59](#).

The device meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

For a full listing of Force 200 specifications, see the [ePMP 1000 website](#).

Table 58: Force 200 physical specifications

Category	Specification
Dimensions (Dia x Depth)	47 x 28 cm (18.5 x 11.2 in)
Weight	2.4 GHz: 2.8 kg (6.2 lbs) 5 GHz: 2.3 kg (5.1 lbs)

Table 59: Force 200 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (140°F) – with radome attached maximum temperature is +47°C (116°F)
Wind loading	90 mph (145 kph) maximum. See Force 200 heater for a full description.
Humidity	95% condensing
Environmental	IP55

Force 200 heater

Upon power-on, if the ePMP Force 200 device temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the Force 200 module continues its startup sequence.

The effect on Force 200 startup time at various temperatures is defined in [Table 60](#).

Table 60: Force 200 startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C)	4 minutes
-4° F (-20° C)	2 minutes
14° F (-10° C)	1 minute, 30 seconds

Force 200 wind loading

Ensure that the Force 200 and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics must be available from national meteorological offices.

The Force 200 and its mounting bracket are capable of withstanding wind speeds of up to 145 Kph (90 mph).

Wind blowing on the Force 200 will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of the integrated module. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

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

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

Applying these formulae to the ePMP Force 200 at different wind speeds, the resulting wind loadings are shown in [Table 61](#) and [Table 62](#).

Table 61: Force 200 wind loading (Kg)

Type of ePMP module	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Force 200	0.13	12.3 Kg	22 Kg	34.4 Kg	49.5 Kg	67.4 Kg

Table 62: Force 200 wind loading (lb)

Type of ePMP module	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Force 200	1.44	38.7 lb	60.4 lb	87 lb	118 lb	136 lb

Force 200 software packages

Force 200 radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP Force 200 are named:

- ePMP-NonGPS_Synced-[Version].tar.gz

Force 200L

For details of the ePMP Force 200L hardware, see:

- [Force 200L description](#)
- [Force 200L part numbers](#)
- [Power supply](#)
- [Force 200L LEDs](#)
- [Force 200L specifications](#)

- [Force 200 specifications](#)
- [Force 200L software packages](#)

Force 200L description

The Force 200L is a 25 dBi integrated dish is a self-contained transceiver unit that houses both radio, parabolic dish, and networking electronics. An ePMP Force 200L unit may function as an Access Point (AP) or a Subscriber Module (SM) in a Point-To-Multipoint (PMP) or a Point-To-Point (PTP) network topology. It is typically deployed as an SM in a PMP system and either Master or Slave in a PTP system.

An overview of ePMP Series Force 200L is shown in [Figure 33](#) and [Figure 34](#).



Figure 33: ePMP Series Force 200L



Figure 34: ePMP Series Force 200L (with optional radome - sold separately)

Force 200L part numbers

Choose the correct regional variant: one is for use in regions where one is for use in ETSI countries (EU), and one is for non-FCC/IC/ETSI-restricted regions (RoW).

Each of the parts listed in [Table 63](#) includes the following items:

- 1 x Radio/feedhorn

- 1 x dish
- 1 x mounting bracket and straps
- 1 x PoE power supply
- 1 x country-specific line cord
- 1 x Regulatory leaflet

Table 63: Force 200L part numbers

Cambium description	Cambium part number
ePMP 5 GHz Force 200L SM (ROW) (no cord)	C050900C091A
ePMP 5 GHz Force 200L SM (ROW) (US cord)	C050900C191A
ePMP 5 GHz Force 200L SM (ROW) (EU cord)	C050900C291A
ePMP 5 GHz Force 200L SM (EU) (EU cord)	C050910C293A
ePMP 5 GHz Force 200L SM (ROW) (UK cord)	C050910C391A
ePMP 5 GHz Force 200L SM (EU) (UK cord)	C050910C393A
ePMP 5 GHz Force 200L SM (ROW) (India cord)	C050910C491A
ePMP 5 GHz Force 200L SM (India) (India Cord)	C050910C492A
ePMP 5 GHz Force 200L SM (ROW) (China cord)	C050910C591A
ePMP 5 GHz Force 200L SM (ROW) (Brazil cord)	C050910C691A
ePMP 5 GHz Force 200L SM (ROW) (Argentina cord)	C050910M791A
ePMP 5 GHz Force 200L SM (ROW) (ANZ cord)	C050910C891A
ePMP 5 GHz Force 200L SM (ROW) (South Africa cord)	C050910C991A
ePMP 5 GHz Force 200L SM (ROW) (No PSU)	C050910CZ91A

Power supply

The power supply and respective partnumbers are described in [Table 64](#).

Table 64: Force 200L power supply

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015

Cambium description	Cambium part number
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

Force 200L mounting bracket

The Force 200L module is designed to be pole-mounted using the mounting bracket and clamp assembly provided in the box with the radio.

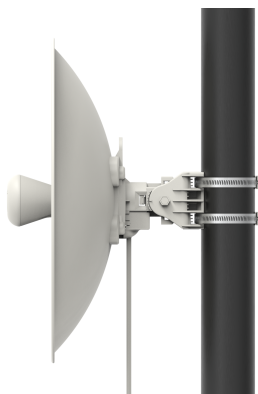


Figure 35: Force 200L mounting bracket (side)

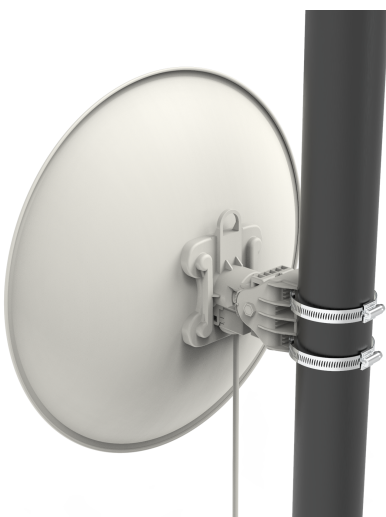


Figure 36: Force 200L mounting bracket (back)

Force 200L interfaces

The Force 200L module interfaces are illustrated in [Figure 37](#) and described in [Table 65](#).




Figure 37: Force 200L interfaces





Table 65: Force 200L interfaces

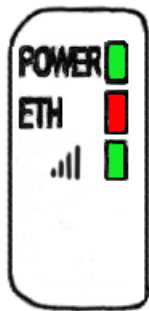
Port name	Connector	Interface	Description
Ethernet	RJ45	PoE input	10/100BASE-T, Compatible with Cambium PoE pinouts (V+ = 7 & 8, Return = 4 & 5) and Standard PoE pinouts (V+ = 4 & 5, Return = 7 & 8)
		10/100/BASE-TX Ethernet	Management and data
Reset Button	Physical button	N/A	For resetting the radio and for setting the radio back to its factory default configuration. See Using the device external reset button .


Force 200L LEDs







LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH	Ethernet port indicator Once lit, blinking indicates Ethernet activity. Green: 10 Mbps port speed Orange: 100 Mbps port speed
 RF SIGNAL	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning. Radio registered: LEDs light to indicate the RSSI level at the device.

 RSSI > -60 dBm	 -70 dBm $< \text{RSSI} \leq -60$ dBm	 -80 dBm $< \text{RSSI} \leq -70$ dBm	 RSSI ≤ -80 dBm
--	--	--	---



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH	Ethernet port indicator Once lit, blinking indicates Ethernet activity. Green: 10 Mbps port speed Orange: 100 Mbps port speed
 RF SIGNAL	Radio scanning: LEDs light in an ascending sequence to indicate that the radio is scanning. Radio registered: LEDs light to indicate the RSSI level at the device.

 RSSI	 -70 dBm	 -80 dBm	 RSSI ≤ -80 dBm
---	--	--	---

> -60 dBm	< RSSI ≤ -60 dBm	< RSSI ≤ -70 dBm	
-----------	---------------------	---------------------	--

Force 200L specifications

The Force 200L module conforms to the specifications listed in [Table 66](#) and [Table 67](#).

The device meets the low-level static discharge specifications identified in [Electromagnetic compatibility \(EMC\) compliance](#) and provides internal surge suppression but does not provide lightning suppression.

Visit the [Cambium Networks website](#) to view and download the Force 200L datasheet.

Table 66: Force 200L physical specifications

Category	Specification
Dimensions (Dia x Depth)	TBD
Weight	1.6 kg (3.5 lbs)

Table 67: Force 200L environmental specifications

Category	Specification
Temperature	-30°C to 55°C (-22°F to 122°F)
Wind loading	200 km/h (124 mph). See Force 200L Heater for a full description.
Environmental	IP55

Force 200L Heater

At startup, if the Force 200L module temperature is at or below 32°F (0°C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32°F (0°C), the heater is deactivated, and the unit continues its startup sequence.

Table 68: Force 200L startup times based on ambient temperature

Initial Temperature	Startup time (from power on to operational)
-22° F (-30° C)	20 minutes
-4° F (-20° C)	6 minutes
14° F (-10° C)	2 minute, 30 seconds

Force 200L wind loading

Ensure that the Force 200L and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed ePMP site. Wind speed statistics must be available from national meteorological offices.

The Force 200L and its mounting bracket are capable of withstanding wind speeds of up to 200 Kph (124 mph).

Wind blowing on the Force 200L will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and the surface area of the integrated module. Wind loading is estimated using the following formulae:

$$\text{Force (in kilograms)} = 0.1045aV^2$$

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

$$\text{Force (in pounds)} = 0.0042Av^2$$

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

Applying these formulae to the ePMP Force 200L at different wind speeds, the resulting wind loadings are shown in [Table 69](#) and [Table 70](#).

Table 69: Force 200L wind loading (Kg)

Type of ePMP module	Largest surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Force 200L	0.13	12.3 Kg	22 Kg	34.4 Kg	49.5 Kg	67.4 Kg

Table 70: Force 200L wind loading (lb)

Type of ePMP module	Largest surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Force 200L	1.44	38.7 lb	60.4 lb	87 lb	118 lb	136 lb

Force 200L software packages

Force 200 radios may be upgraded by downloading new software packages from the Cambium Networks website or by using the Cambium Network Services Server. The software packages applicable to ePMP Force 200 are named:

- ePMP-NonGPS_Synced-[Version].tar.gz

Chapter 3: Power Supply

This chapter describes ePMP 2000 series and ePMP 1000 series power supply.

ePMP 2000 Series Power Supply

For details of the ePMP power supply units, see:

- [Power supply description](#)
- [Power supply part numbers](#)
- [Power supply interfaces](#)
- [Power supply specifications](#)
- [Power supply location](#)

Power supply description

The power supply is an indoor unit that is connected to the ePMP module and network terminating equipment using Cat5e cable with RJ45 connectors. It is also plugged into an AC or DC power supply so that it can inject Power over Ethernet (PoE) into the module.

Power supply part numbers

Each module requires one power supply and one power supply line cord (line cord included with radio device, see [Table 2](#)). The power supplies listed in [Table 71](#) may be used for all ePMP 2000 modules.

Table 71: Power supply part numbers

Cambium description	Cambium part number
Power Supply, 30W, 56V – Gbps support	N000000L034

Power supply interfaces

The power supply interfaces are illustrated in [Figure 38](#) and described in [Table 72](#) and [Table 73](#).

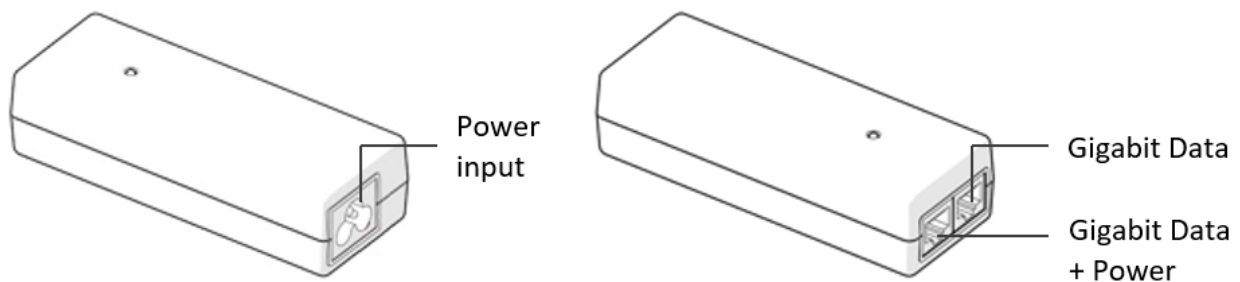


Figure 38: Power supply interfaces

Table 72: Power supply interface functions - N000000L034

Interface	Function
Power input	Mains power input.
Gigabit Data + Power	RJ45 socket for connecting Cat5e cable to the radio
Gigabit Data	RJ45 socket for connecting Cat5e cable to the network.

Table 73: Power Supply LED functions

LED	Function
Power (green)	Power supply detection

Power supply specifications

The ePMP power supply conforms to the specifications listed in [Table 74](#), [Table 75](#), and [Table 76](#). These specifications apply to ePMP 2000 product variants.

Table 74: Power supply physical specifications

Category	Specification
Dimensions (H x W x D)	14 x 6.5 x 3.6 cm (5.5 x 2.55 x 1.42 in)
Weight	0.26 lbs

Table 75: Power supply environmental specifications

Category	Specification
Ambient Operating Temperature	0° C to +40° C
Humidity	20% - 90%

Table 76: Power supply electrical specifications

Category	Specification
AC Input	100 to 240 VAC
Efficiency	Meets Energy Level 6
Over Current Protection	Short circuit, with auto-recovery
Hold up time	10 ms minimum at maximum load, 120 VAC

Power supply location

Find a location for the power supply that meets the following requirements:

- The power supply can be mounted on a wall or other flat surfaces.
- The power supply is kept dry, with no possibility of condensation, flooding, or rising dampness.

- The power supply can be accessed to view status indicators.
- The power supply can be connected to the ePMP module drop cable and network terminating equipment.
- The power supply can be connected to a mains or DC power supply that meets the requirements defined in [Table 83](#).

ePMP 1000 Series Power Supply (includes Force 180, Force 190, and Force 200)

For details of the ePMP power supply units, see:

- [ePMP 1000 Series Power Supply \(includes Force 180, Force 190, and Force 200\)](#)
- [Power supply description](#)
- [Power supply interfaces](#)
- [Power supply specifications](#)
- [Power supply location](#)

Power supply description

The power supply is an indoor unit that is connected to the ePMP module and network terminating equipment using Cat5e cable with RJ45 connectors. It is also plugged into an AC or DC power supply so that it can inject Power over Ethernet (PoE) into the module.

Power supply part numbers

Each module requires one power supply and one power supply line cord (line cord included with radio device, see [Table 11](#), [Table 28](#), [Table 56](#)). The power supplies listed in [Table 77](#) may be used for all ePMP 1000 modules, however, only N000900L001B provides a Gigabit Ethernet interface.

Table 77: Power supply part numbers

Cambium description	Cambium part number
ePMP Pwr Supply for GPS Radio - no cord (spare)	N000900L001B
ePMP Pwr Supply for non-GPS Radio - no cord (spare)	N000900L002A
ePMP Pwr Supply for Force 190 - no cord (spare)	N000900L003A

Power supply interfaces

The power supply interfaces are illustrated in [Figure 39](#) and described in [Table 78](#) and [Table 80](#).

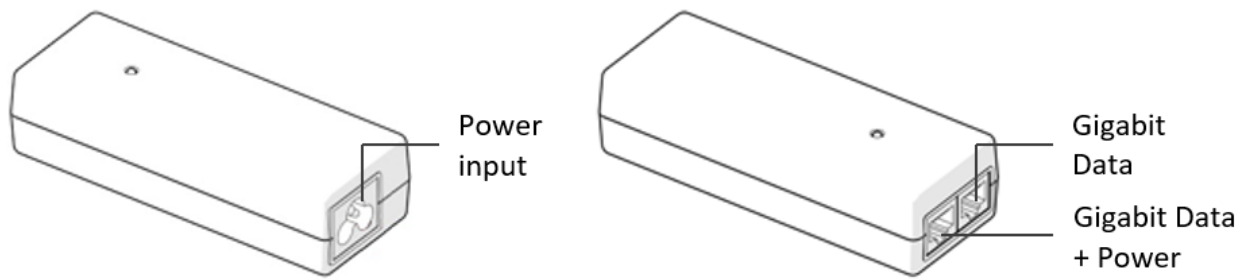


Figure 39: Power supply interfaces

Table 78: Power supply interface functions - N000900L001B


Interface	Function
Power input	Mains power input.
Gigabit Data + Power	RJ45 socket for connecting Cat5e cable to the radio  <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>This port provides a Gigabit Ethernet interface to ePMP GPS Synced connectorized radios. To ePMP integrated radios, this port provides a 10/100 Mbit/sec Ethernet interface.</p> </div>
Gigabit Data	RJ45 socket for connecting Cat5e cable to the network.

Table 79: Power supply interface functions - N000900L002A, N000900L003A

Interface	Function
Power input	Mains power input.
10/100 Mbit/sec Data + Power	RJ45 socket for connecting Cat5e cable to the radio
10/100 Mbit/sec Data	RJ45 socket for connecting Cat5e cable to the network.

Table 80: Power Supply LED functions

LED	Function
Power (green)	Power supply detection

Power supply specifications

The ePMP power supply conforms to the specifications listed in [Table 81](#), [Table 82](#), and [Table 83](#). These specifications apply to all ePMP product variants.

Table 81: Power supply physical specifications

Category	Specification
Dimensions (H x W x D)	11.8 x 4.4 x 3.2 cm (4.66 x 1.75 x 1.25 in)
Weight	0.26 lbs

Table 82: Power supply environmental specifications

Category	Specification
Ambient Operating Temperature	0° C to +40° C
Humidity	20% - 90%

Table 83: Power supply electrical specifications

Category	Specification
AC Input	100 to 240 VAC
Efficiency	Meets efficiency level 'V'
Over Current Protection	Zener clamping (38V to 45V)
Hold up time	10 ms minimum at maximum load, 120 VAC

Power supply location

Find a location for the power supply that meets the following requirements:

- The power supply can be mounted on a wall or other flat surfaces.
- The power supply is kept dry, with no possibility of condensation, flooding, or rising dampness.
- The power supply can be accessed to view status indicators.
- The power supply can be connected to the ePMP module drop cable and network terminating equipment.
- The power supply can be connected to a mains or dc power supply that meets the requirements defined in [Table 83](#).

Chapter 4: Ethernet Cabling

For details of the Ethernet cabling components of an ePMP installation, see:

- [Ethernet standards and cable lengths](#)
- [Outdoor Cat5e cable](#)

Ethernet standards and cable lengths

All configurations require a copper Ethernet connection from the power supply port to the power supply and network terminating equipment.

For each power supply, the maximum permitted drop cable length is specified in [Table 84](#).

Table 84: Power supply drop cable length restrictions

Part number	Description	Maximum cable length (*1)
N000000L034	Power supply, 30W, 56V – Gbps support	330 feet (100m)
N000900L001B	Power supply for Radio with Gigabit Ethernet (no cord)	330 feet (100m)
N000900L002A	Power supply for Radio with 100Mbit Ethernet (no cord)	330 feet (100m)

(*1) The maximum length of Ethernet cable from AP/SM to network device needs to follow 802.3 standards. If the power supply is not the network device the cable from the power supply to the network device must be included in the total maximum cable length.

Outdoor Cat5e cable

Cambium Industrial Cable

Cambium Industrial Cable uses 24 gauge solid bare copper conductors, covered by bonded-pair polymer insulation. The conductors are protected by double-layer shielding consisting of a solid foil layer under the braided tinned copper mesh, providing excellent shielding while maximizing flexibility. And, the cable is jacketed by industrial-grade UV-resistant, abrasion-resistant, and oil-resistant PVC.

Cambium's Industrial RJ45 connectors are specifically designed to work optimally with Cambium Industrial Cable.

The connectors are fully shielded with integrated strain relief for greater pull strength, utilize a staggered contact design that minimizes crosstalk and maximizes electrical performance, and the contacts are plated with a 50 micro-inch thick 24-carat gold, exceeding TIA-1096 specifications and ensuring the best possible connection and oxidation resistance.

Cambium Networks' industrial-grade cable is well suited for high-quality durable installations of subscriber modules, access points, and enterprise Point-to-Point (PTP) links as well as in tactical non-permanent deployments of infrastructure.

Table 85: Cambium Industrial Cable part numbers

Cambium description	Cambium part number
Industrial Grade CAT 5 Cable 50 meter unterminated	N000000L106A
Industrial Grade CAT 5 Cable 100 meter unterminated	N000000L106A
Industrial Grade CAT 5 Cable 300 meter unterminated	N000000L108A
Industrial Grade RJ45 Connector 100 Pack	C000000L109A
Termination Tool for C000000L109A RJ45 connectors	C000000L110A

Surge suppression unit



Note

Lightning-prone installations can be improved by:

1. Installing a 600SS Surge Suppressor near the device (transient surge suppression)
2. Grounding the device to the pole (ground bonding)
3. Lowering the device/dish such that it is not the highest metallic object on the pole

Structures, equipment, and people must be protected against power surges (typically caused by lightning) by conducting the surge current to the ground via a separate preferential solid path.

The actual degree of protection required depends on local conditions and applicable local regulations. To adequately protect an ePMP installation, both ground bonding and transient voltage surge suppression are required.

Network operators should always follow best-practices for grounding and lightning protection. Doing so will minimize network outages and reduce the associated costs of tower climbs and equipment repair/replacement.

Gigabit Ethernet Surge Suppressor

The Gigabit Ethernet Surge Suppressor is critical for lightning protection to minimize the potential for damage.

An overview of Gigabit Ethernet Surge Suppressor is shown in [Figure 40](#).



Figure 40: Gigabit Ethernet Surge Suppressor

Table 86: Surge suppressor part numbers

Cambium description	Cambium part number
Gigabit Surge Suppressor (30V)	C000000L065A
Gigabit Surge Suppressor (56V)	C000000L033A



Note

Choose the 30V or 56V Surge Suppressor option based on your installed device power rating. Installing a 30V surge suppressor for a 56V device or a 56V surge suppressor for a 30V device may result in inadequate surge protection.

30V ePMP installations with Ethernet connections that require only a 100 Mbit/sec connection may also be protected with the Cambium Networks 600SSH surge suppressor.

Chapter 5: System Planning

This chapter provides information to help the user to plan an ePMP link.

The following topics are described in this chapter:

- How to plan ePMP links to conform to the regulatory restrictions that apply in the country of operation is explained under [Radio spectrum planning](#).
- Factors to be considered when planning links such as range, path loss, and throughput are described under [Link planning](#).
- Factors to be considered when planning to use connectorized APs with external antennas in ePMP links are described under [Planning for connectorized units](#).
- The grounding and lightning protection requirements of an ePMP installation are described under [Grounding and lightning protection](#).
- Factors to be considered when planning ePMP data networks are described under [Data network planning](#).

Radio spectrum planning

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



Caution

The user must ensure the ePMP product operates in accordance with local regulatory limits.



Note

Contact the applicable radio regulator to check if the registration of the ePMP link is required.

General wireless specifications

The wireless specifications that apply to all ePMP variants are listed under [Table 87](#). The wireless specifications that are specific to each frequency variant are listed in [Table 88](#) and [Table 89](#).

Table 87: ePMP wireless specifications (all variants)

Item	Specification
Channel selection	Automatic and Manual selection (fixed frequency).
Manual power control	To avoid interference to other users of the band, maximum power can be set lower than the default power limit.

Item	Specification
Integrated device antenna type	Patch antenna
Duplex scheme	Adaptive TDD (with optional Standard 802.11n Wi-Fi on SM)
Range	21 mi (5 MHz channel bandwidth) 17 mi (10 MHz channel bandwidth) 13 mi (20 MHz channel bandwidth) 9 mi (40 MHz channel bandwidth)
Over-the-air encryption	AES
Error Correction	FEC

Table 88: ePMP 2000 wireless specifications (per frequency band)

Item	5 GHz
RF band (GHz)	5150 - 5970 MHz
Channel bandwidth	5 MHz, 10 MHz, 20 MHz, or 40 MHz
Typical antenna gain	Connectorized antenna - 18 dBi

Table 89: ePMP 1000 wireless specifications (per frequency band)

Item	2.4 GHz	2.5 GHz	5 GHz
RF band (GHz)	2407 - 2472 MHz	2570 - 2620 MHz	4900 - 5980 MHz
Channel bandwidth	5 MHz, 10 MHz, 20 MHz, or 40 MHz	5 MHz, 10 MHz, 20 MHz, or 40 MHz	5 MHz, 10 MHz, 20 MHz, or 40 MHz
Typical antenna gain	Connectorized antenna - 15 dBi Integrated patch antenna - 11 dBi Reflector dish antenna - 8 dBi	Connectorized antenna - 15 dBi Reflector dish antenna - 8 dBi	Connectorized antenna - 15 dBi Integrated patch antenna - 13 dBi Reflector dish antenna - 6 dBi
Antenna beamwidth (Integrated)	24° azimuth, 12° elevation	24° azimuth, 12° elevation	24° azimuth, 12° elevation
Antenna beamwidth (Reflector dish)	10° azimuth, 28° elevation	10° azimuth, 28° elevation	10° azimuth, 25° elevation

Regulatory limits

The local regulator may restrict frequency usage and channel width and may limit the amount of conducted or radiated transmitter power. For details of these restrictions, see [Examples of regulatory limits](#).

Many countries impose EIRP limits (Allowed EIRP) on products operating in the bands used by the ePMP Series. For example, in the 5 GHz and 2.4 GHz bands, these limits are calculated as follows:

- In the 5.2 GHz (5250 MHz to 5350 MHz) and 5.4 GHz (5470 MHz to 5725 MHz) band, the EIRP must not exceed the lesser of 30 dBm or $(17 + 10 \times \text{Log Channel width in MHz})$ dBm.
- In the 5.8 GHz band (5725 MHz to 5875 MHz), the EIRP must not exceed the lesser of 36 dBm or $(23 + 10 \times \text{Log Channel width in MHz})$ dBm.
- In the 2.4 GHz band (2400 MHz to 2500 MHz), the EIRP must not exceed the lesser of 36 dBm or $(23 + 10 \times \text{Log Channel width in MHz})$ dBm.

Some countries (for example the USA) impose conducted power limits on products operating in the 5 GHz and 2.4 GHz band.

Conforming to the limits

Ensure the link is configured to conform to local regulatory requirements by configuring the correct country code (located in the web management interface, under **Configure > Radio**). In the following situations, the country code does not automatically prevent operation outside the regulations:

- 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, see [Calculating maximum power level for connectorized units](#). When operating in ETSI regions, it is required to enter a license key in the ePMP web management interface to unlock valid country-specific frequencies. This key may be obtained from <https://support.cambiumnetworks.com/licensekeys/epmp>.
- When installing 5.4 GHz links in the USA, it may be necessary to avoid frequencies used by Terminal Doppler Weather Radar (TDWR) systems. For more information, see [Avoidance of weather radars](#).

Available spectrum

The available spectrum for the operation depends on the region. When configured with the appropriate country code, the unit will only allow operation on those channels which are permitted by the regulations.



Note

In Italy, there is a regulation that requires a general authorization of any 5.4 GHz radio link which is used outside the operator's premises. It is the responsibility of the installer or operator to have the link authorized. For details, see:

www.sviluppoeconomico.gov.it

For the form that must be used for general authorization, see:

http://www.sviluppoeconomico.gov.it/images/stories/mise_extra/Allegato%20n19.doc

Certain regulations have allocated certain channels as unavailable for use:

- ETSI has allocated part of the 5.4 GHz band to weather radar.
- Some European countries have allocated part of the 5.8 GHz band to Road Transport and Traffic Telematics (RTTT) systems.

For details of these restrictions, see [Examples of regulatory limits..](#)

Where regulatory restrictions apply to certain channels, these channels are barred automatically by the use of the correct country code. For example, in some European countries the RTTT band 5795 MHz to 5815 MHz is barred. With the appropriate country code configured for this region, the ePMP will not operate on channels within this band.

The number and identity of channels barred by the license key and country code are dependent on the channel bandwidth.

For more information about configuring the **Country Code** parameter, see the [AP Radio page](#) and the [SM Radio page](#).

Channel bandwidth

Select the required channel bandwidth for the link. The selection depends upon the ePMP frequency variant and country code.

The wider a channel bandwidth the greater is its capacity. As narrower channel bandwidths take up less spectrum, selecting a narrow channel bandwidth may be a better choice when operating in locations where the spectrum is very busy.

Both ends of the link must be configured to operate on the same channel bandwidth.

Avoidance of weather radars

To comply with FCC rules (KDB 443999: Interim Plans to Approve UNII Devices Operating in the 5470 - 5725 MHz Band with Radar Detection and DFS Capabilities), units which are installed within 35 km (22 miles) of a Terminal Doppler Weather Radar (TDWR) system (or have a line of sight propagation path to such a system) must be configured to avoid any frequency within +30 MHz or -30 MHz of the frequency of the TDWR device. This requirement applies even if the master is outside the 35 km (22 miles) radius but communicates with outdoor clients which may be within the 35 km (22 miles) radius of the TDWRs.

The requirement for ensuring 30 MHz frequency separation is based on the best information available to date. If interference is not eliminated, a distance limitation based on line-of-sight from TDWR will need to be used. Also, devices with bandwidths greater than 20 MHz may require greater frequency separation.

When planning a link in the USA, visit <http://spectrumbridge.com/udia/home.aspx>, enter the location of the planned link and search for TDWR radars. If a TDWR system is located within 35 km (22 miles) or has a line of sight propagation to the PMP device, perform the following tasks:

- Register the installation on <http://spectrumbridge.com/udia/home.aspx>.
- Make a list of channel center frequencies that must be barred, that is, those falling within +30 MHz or -30 MHz of the frequency of the TDWR radars.

In ETSI regions, the band 5600 MHz to 5650 MHz is reserved for the use of weather radars.

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 to achieve an accurate link feasibility assessment.

Path loss

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

Free space path loss is a major determinant in received (Rx) 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, the fade margin is the difference between the strength of the received signal and the strength that the receiver requires for maintaining a reliable link.

Adaptive modulation

Adaptive modulation ensures that the highest throughput that can be achieved instantaneously will be obtained, taking account of propagation and interference. When the link has been installed, web pages provide information about the link loss currently measured by the equipment, both instantaneously and averaged.

Planning for connectorized units

This section describes factors to be taken into account when planning to use connectorized APs with external antennas in ePMP networks.

Calculating maximum power level for connectorized units

If a connectorized ePMP link is to be installed in a country that imposes an EIRP limit in the selected band, choose an external antenna and RF cable that will not cause the ePMP to exceed the EIRP limit. To calculate the highest setting of Maximum Power Level that will be permitted, use this formula:

$$\text{Maximum Power Level (dBm)} = \text{Allowed EIRP (dBm)} - \text{Antenna Gain (dBi)} + \text{Cable Loss (dB)}$$

Where:	Is:
Maximum Power Level (dBm)	the highest permissible setting of the Maximum Power Level attribute in Step 2: Wireless Configuration page,
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.

As the 2.4 GHz, 2.5 GHz, 5.4 GHz, and 5.8 GHz have an operating bandwidth of 5 MHz, 10 MHz, 20 MHz, or 40 MHz then the maximum allowed EIRP depends on the operating bandwidth of the radio as shown in [Table 90](#).

Table 90: Normal EIRP limits with operating channel bandwidth

Operating bandwidth (MHz)	Allowed EIRP (dBm) at 2.4 GHz	Allowed EIRP (dBm) at 2.5 GHz	Allowed EIRP (dBm) at 5.2 GHz	Allowed EIRP (dBm) at 5.4 GHz	Allowed EIRP (dBm) at 5.8 GHz
5, 10, 20, 40	36	N/A	24 - 30	24 - 30	36

The settings to be used for regions with the EIRP limits in [Table 90](#) are shown in [Table 91](#).

Table 91: Setting maximum transmit power to meet general EIRP limits

Antenna	Maximum available antenna gain (dBi)	Operating bandwidth (MHz)	Transmitter Output Power parameter setting (dBm)				
			2.4 GHz	2.5 GHz	5.2 GHz	5.4 GHz	5.8 GHz
ePMP 2000 Conn. module Sector antenna	18	5, 10, 20, 40	N/A	N/A	12	12	18
ePMP 1000 Conn. module Sector antenna	15	5, 10, 20, 40	21	27	15	15	21

**Note**

Calculations under [Table 91](#) are based on 0.5 dB cable loss and the highest gain antennas per size of which Cambium Networks are aware. At these operating frequencies, antenna cable losses even with short cables are unlikely to ever be below 0.5 dB for practical installations and cable diameters.

Data network planning

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

Ethernet interfaces

The ePMP Ethernet ports conform to the specifications listed in [Table 92](#) and [Table 93](#).

Table 92: ePMP 2000 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	10BASE-Te/100BASE-Tx/1000BASE-T IEEE 802.3 IEEE 802.3at (PoE) IEEE802.3u compliant Auto-negotiation
QoS	Proprietary QoS
Interface	10/100/1000BASE-T (RJ-45)
Data Rates	See Data throughput tables
Maximum Ethernet Frame Size	1700 bytes
Service classes for bridged traffic	3 classes

Table 93: ePMP 1000 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	10BASE-Te/100BASE-Tx/1000BASE-T IEEE 802.3 IEEE 802.3af (PoE) IEEE802.3u compliant Auto-negotiation
QoS	Proprietary QoS
Interface	10/100/1000BASE-T (RJ-45)
Data Rates	See Data throughput tables
Maximum Ethernet Frame Size	1700 bytes
Service classes for bridged traffic	3 classes

**Note**

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

Over the air, throughput will be capped to the rate of the Ethernet interface at the receiving end of the link.

Management VLAN

Decide if the IP interface of the AP/SM management agent will be connected in a VLAN. If so, decide if this is a standard (IEEE 802.1Q) VLAN or provider bridged (IEEE 802.1ad) VLAN, and select the VLAN ID for this VLAN.

The use of a separate management VLAN is strongly recommended. The use of the management VLAN helps to ensure that the AP/SM management agent cannot be accessed by customers.

Quality of service for bridged Ethernet traffic

Decide how the quality of service will be configured in ePMP to minimize frame loss and latency for high-priority traffic. Wireless links often have lower data capacity than wired links or network equipment like switches and routers, and quality of service configuration is most critical at network bottlenecks.

ePMP provides three priority types for traffic waiting for transmission over the wireless link - Voice, High and Low. Low is the lowest priority and Voice is the highest priority. Traffic is scheduled using strict priority; in other words, traffic in a given priority is transmitted when all higher-priority transmissions are complete.

Chapter 6: Configuration

This chapter describes all configuration and alignment tasks that are performed when an ePMP system is deployed.

Configure the units by performing the following tasks:

- [Preparing for configuration](#)
- [Using the web interface](#)
- [Configuring connectorized radios using the Quick Start menu](#)
- [Configuring SM units using the Quick Start menu](#)
- [Using the AP menu options](#)
- [Using the SM menu options](#)

Preparing for configuration

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

Safety precautions

All national and local safety standards must be followed while configuring the units.



Warning

Ensure that personnel is not exposed to unsafe levels of RF energy. The units start to radiate as soon as they are powered up. Respect the safety standards defined in [Compliance with safety standards](#), in particular the minimum separation distances.

Observe the following guidelines:

- Never work in front of the antenna when the AP is powered.
- Always power down the power supply before connecting or disconnecting the Ethernet cable from the module.

Regulatory compliance

All applicable radio regulations must be followed while configuring the units and aligning the antennas. For more information, [Compliance with safety standards](#).

Connecting to the unit

To connect the unit to a management PC, use the following procedures:

- [Connecting to the unit](#)
- [Connecting to the PC and powering up](#)

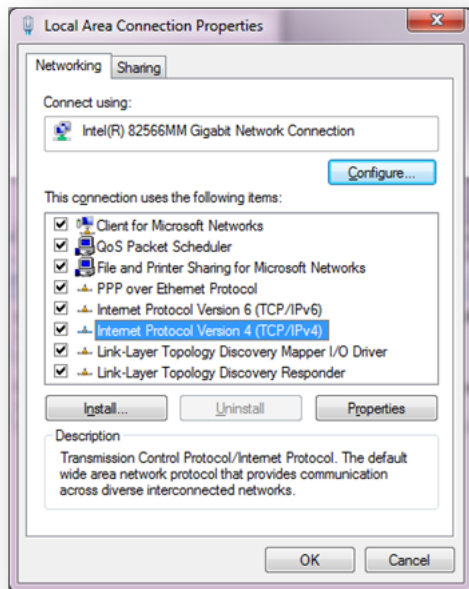
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the ePMP module.

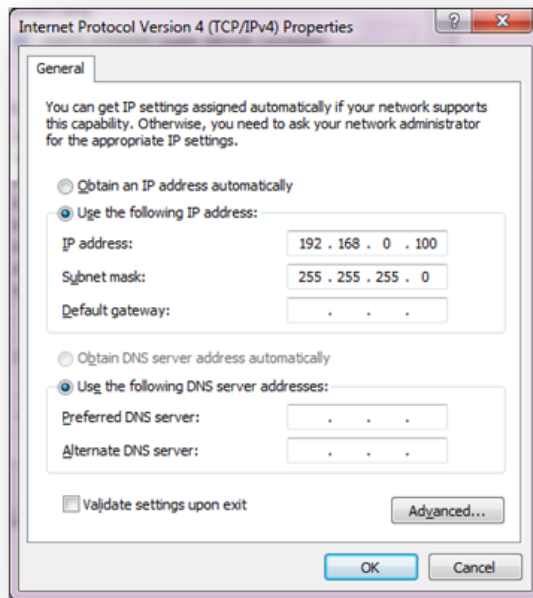
Procedure:

1. Select **Properties** for the Ethernet port.

In Windows 7 this is found in **Control Panel > Network and Internet > Network Connections > Local Area Connection**.



2. Select the Internet Protocol (TCP/IP) item.
3. Click **Properties**.
4. Enter an IP address that is valid for the 192.168.0.X network, avoiding:
192.168.0.1, 192.168.0.2 and 192.168.0.3
A good example is 192.168.0.100:



5. Enter a subnet mask of 255.255.255.0.
Leave the default gateway blank.
6. Click **OK**, and then click **Close**.

Connecting to the PC and powering up

Use this procedure to connect a management PC directly to the ePMP for configuration and alignment purposes and to power up the ePMP device.

Procedure:

1. Check that the device and power supply are correctly connected (the device Ethernet port is connected to the power supply Ethernet power port).
2. Connect the PC Ethernet port to the LAN (AP: “Gigabit Data”, SM: “10/100Mbit Data”) port of the power supply using a standard (not crossed) Ethernet cable.
3. Apply mains or battery power to the power supply. The green Power LED must illuminate continuously.



Note

If the Power and Ethernet LEDs do not illuminate correctly, see [Testing hardware](#).

Using the web interface

To understand how to use the ePMP web interface, see:

- [Logging into the web interface](#)
- [Layout of the web interface](#)
- [Configuring connectorized radios using the Quick Start menu](#)
- [Configuring SM units using the Quick Start menu](#)
- [Using the AP menu options](#)

Logging into the web interface

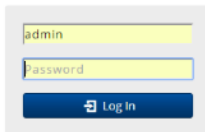
Use this procedure to log into the web interface as a system administrator.

Equipment and tools:

- Connectorized or integrated device connected to the power supply by Ethernet cable.
- PC connected to the power supply by Ethernet cable.
- Power Supply powered up.
- Minimum supported browser version – Chrome v29, Firefox v24, Internet Explorer 10, Safari v5.

Procedure:

1. Start the web browser from the management PC.



2. Type the IP address of the unit into the address bar. The factory default IP address is either 192.168.0.1 (AP mode) or 192.168.0.2 (SM mode). Press **Enter**. The web interface dashboard and login input are displayed.



Note

If **Device IP address Mode** is set to **DHCP** and the device is unable to retrieve IP address information via DHCP, the device management IP is set to fallback IP 192.168.0.1 (AP mode), 192.168.0.2 (SM mode), 192.168.0.3 (Spectrum Analyzer mode), or the previously-configured static Device IP Address. Units may always be accessed via the Ethernet port. With Release 2.1, the fallback IP address has changed from 10.1.1.254 to 169.254.1.1.

3. Enter **Username** (default: admin) and **Password** (default: admin).
4. Click **Login**.



Note

New ePMP devices all contain default username and password configurations. It is recommended to change these password configurations immediately. These passwords may be configured in the management GUI in section **Configuration > System > Account Management**.

Layout of the web interface

After logging in, the web interface first displays a dashboard view of vital system status and statistics. Also, the first level of navigation is displayed across the top (**Configure, Monitor, Tools, and Quick Start**).

© 2016 Cambium Networks. All Rights Reserved | Version 3.1 | Support | Community Forum


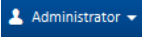






Figure 41: ePMP 2000 GUI dashboard (includes additional fields not resident in ePMP 1000)



© 2017 Cambium Networks. All Rights Reserved | Version 3.5-RC13 | Support | Community Forum

Figure 42: ePMP 1000 GUI dashboard

The top of the interface contains the following attributes:

Table 94: GUI status bar attributes

Icon	Attribute	Meaning
	Cambium Networks logo	Hyperlink to the Cambium Networks website.
	Login Level indicator	Displays the current user login level.
	Internet Connectivity Indicator	<p>Green indicates that the AP has IP connectivity to the configured DNS server.</p> <p>Grey indicates that the AP has no IP connectivity to the configured DNS server.</p> <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px; margin-top: 10px;"> <p>Note The Internet Connectivity Indicator state is determined by receipt of ping responses from the configured DNS server.</p> </div>
	GPS Synchronization Receive Indicator	<p>Green indicates that the AP is receiving a valid GPS synchronization timing pulse via a connected GPS antenna or a CMM.</p> <p>Red indicates that the AP is not receiving GPS synchronization due to a lack of satellite fix.</p> <p>Grey indicates that the AP is not receiving GPS synchronization due to the configuration of Synchronization Source to Internal.</p>
	Notifications Button	<p>The Notifications button may be clicked to display system messaging. When a new notification is available, the icon is highlighted and displays the number of notifications available. The outer icon highlighting indicates the type of notification pending:</p> <p>Green: Successful operation has completed (i.e. Changes successfully saved)</p> <p>Grey: Informational message (i.e. tips regarding GUI operation)</p> <p>Blue: Operations information message (i.e. Initializing upgrade...)</p> <p>Orange: Warning message (i.e. Login session has expired)</p> <p>Red: Error message (i.e. Software update file download failed)</p>
	Active Users Indicator	When the mouse pointer hovers over this indicator, it displays the number of active Read-Only and Read-Write users currently logged into the radio.
	Undo Button	The Undo button may be used to undo changes before a Save operation. All changes made on any section of the GUI are undone.
	Save Button	The Save button is used to commit configuration changes to the device. When configuration changes are made, the outer area of the icon is highlighted blue to indicate that a save operation is required.

Icon	Attribute	Meaning
	Reset Button	The Reset button is used to reset the device. When a configuration change requires a radio reset, the outer area of this icon is highlighted orange to indicate that a reset is necessary to complete the change.
	Logout Button	The Logout button is used to logout from the current session and return to the initial GUI landing page (login screen).

The bottom of the interface contains the following attributes:

Table 95: GUI footer attributes

Attribute	Meaning
Copyright	Copyright information.
Version	The current software version is reported in the footer bar and can be clicked to navigate to the Cambium Networks software support website.
Support	Hyperlink to the Cambium Networks support website.
Community Forum	Hyperlink to the Cambium Community Forum website.

The AP dashboard contains the following attributes:

Table 96: AP dashboard attributes

Attribute	Meaning
Device Name	The configured device name of the AP, used for identifying the device in an NMS such as the Cambium Network Services Server (CNSS).
SSID	The current configured name/SSID of the AP.
Operating Frequency	The current frequency carrier used for radio transmission, based on the configuration of the Frequency Carrier parameter (in DFS regions, if radar has been detected, this field may display either DFS Alternate Frequency Carrier 1 or DFS Alternate Frequency Carrier 2).
Operating Channel Bandwidth	The current channel bandwidth used for radio transmission, based on the configuration of the Channel Bandwidth parameter.
Transmitter Output Power	The current operating transmit power of the AP.
Antenna Gain	The configured gain of the external antenna.
Country	The current configured country code, which has an effect on DFS operation and transmit power restrictions. Registered Subscriber Modules will inherit this country code when registration is complete (unless SM is locked to the US region).

Attribute	Meaning
Access Point Mode	<p>TDD: The Access Point is operating in point-to-multipoint (PMP) mode using TDD scheduling. The AP can GPS synchronize in this mode (except when in Flexible mode).</p> <p>ePTP Master: The Access Point is operating as a Master in point-to-point mode. The AP does not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode.</p> <p>PTP: The Access Point is operating in point-to-point (PTP) mode using TDD scheduling. The AP can GPS synchronize in this mode (except when in Flexible mode).</p>
Downlink/Uplink Frame Ratio	The current configured schedule of downlink traffic to uplink traffic on the radio link. In other words, this ratio represents the amount of the total radio link's aggregate throughput that will be used for downlink resources and the amount of the total radio link's aggregate throughput that will be used for uplink resources.
Wireless Security	The currently configured authentication type is used for radio link encryption as well as SM authentication.
cnMaestro Remote Management	Indicates whether the device is currently configured to be managed by the Cambium cloud management system - cnMaestro™.
cnMaestro Connection Status	The current management status of the device concerning the Cambium Cloud Server. When Enabled under Configuration->System, the device will be managed by the Cambium Remote Management System, which allows all Cambium devices to be managed from the Cambium Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Cloud Server.
Wireless MAC Address	The MAC address of the device wireless interface.
Ethernet MAC Address	The MAC address of the device Ethernet (LAN) interface.
IP Address	The currently configured device IP address (LAN) is used for management access.
IPv6 Link Local Address	A link-local address is required for the IPv6-enabled interface (applications may rely on the link-local address even when there is no IPv6 routing). The IPv6 link-local address is comparable to the auto-configured IPv4 address 169.254.0.0/16.
IPv6 Address	The IPv6 address for device management.
Date and Time	The current date and time on the device, subject to the configuration of the parameter Time Zone .
System Uptime	The total uptime of the radio since the last reset.
System Description	The current configured system description.

Attribute	Meaning
Sync Source Status	Displays the current source (GPS, CMM, or Internal) of sync timing for the AP.
Device Coordinates	The current configured Latitude and Longitude coordinates in decimal format.
DFS Status	Current DFS operational status.
Ethernet Status	<p>Up: The Ethernet (LAN) interface is functioning properly. This also displays the current port speed and duplex mode to which the Ethernet port has auto-negotiated to or configured for.</p> <p>Down: The Ethernet (LAN) interface is either disconnected or has encountered an error and is not servicing traffic.</p>
Wireless Status	<p>Up: The radio (WAN) interface is functioning properly</p> <p>Down: The radio (WAN) interface has encountered an error and is not servicing traffic.</p>
Registered Subscriber Modules	The total number of SMs currently registered to the AP.
Smart Antenna (ePMP 2000 only)	<p>Beginning with Software Release 3.4, the ePMP 2000 unit automatically detects when the Smart Antenna is connected or disconnected (without requiring a reboot).</p> <p>Smart Antenna is Connected, Power On: ePMP 2000 is communicating with the Smart Antenna, and a proper power supply is in use</p> <p>Smart Antenna is Connected, Power Off: ePMP 2000 established communication with the Smart Antenna, but subsequent communication errors occurred or an improper power supply was detected</p> <p>Smart Antenna is Disconnected: Communication between ePMP 2000 and Smart Antenna is down</p>
Power Supply	<p>This field indicates the type of power supply being used to power ePMP 2000. Values are 802.3at and Generic Power Supply.</p> <p>The Cambium Power Supply provided with ePMP 2000 will be displayed as "Generic Power Supply". If a different power supply is used and "Generic Power Supply" is indicated, please make sure that the power supply wattage is a minimum of 20 watts.</p>

The SM dashboard is as shown in [Figure 43](#) and the attributes are explained in [Table 97](#).

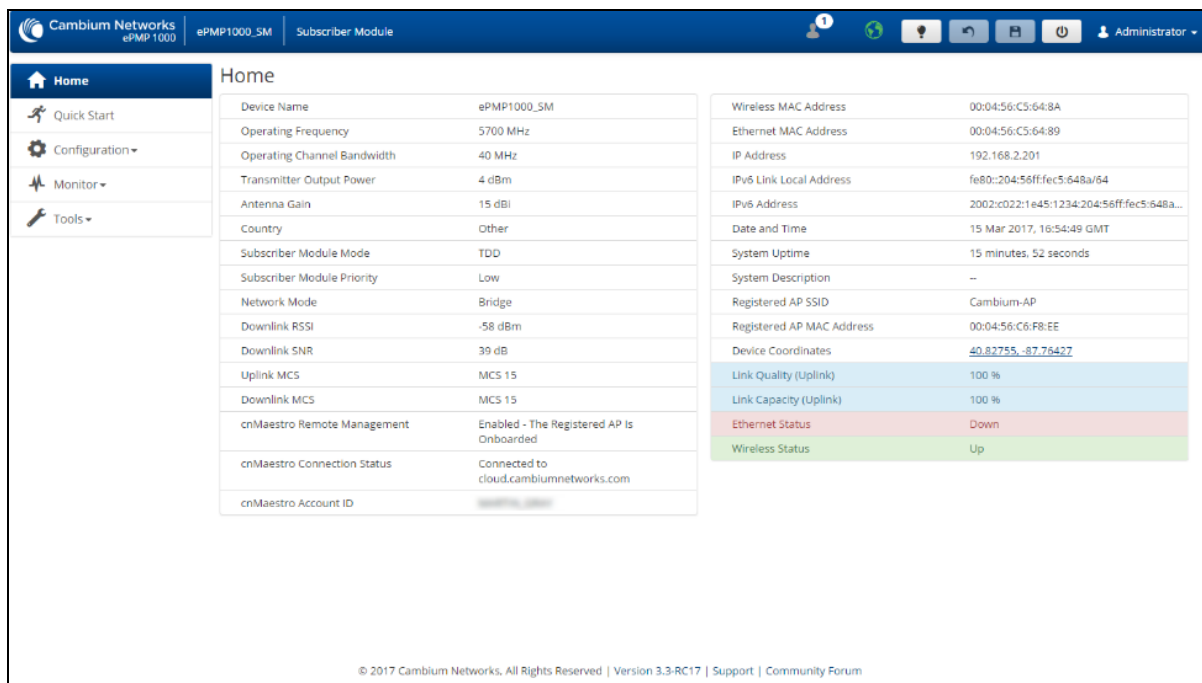


Figure 43: SM Dashboard

Table 97: SM Dashboard Attributes

Attribute	Meaning
Device Name	The configured device name of the SM, used for identifying the device in an NMS such as the Cambium Network Services Server (CNSS).
Operating Frequency	The current operating frequency.
Operating Channel Bandwidth	The current operating width of the channel used for the radio link.
Transmitter Output Power	The current power level at which the SM is transmitting (which is adjusted dynamically by the AP based on radio conditions).
Antenna Gain	The configured gain of the external antenna.
Country	The current configured country code, which has an effect on DFS operation and transmit power restrictions. Registered Subscriber Modules will inherit this country code when registration is complete (unless SM is locked to the US region).
Subscriber Module Mode	<p>TDD: The SM is operating in the proprietary TDD mode and will only connect to another ePMP Access Point.</p> <p>Standard WiFi: The SM is operating in the Standard 802.11n WiFi mode and will be able to connect to any Access Point operating in standard WiFi mode.</p>

Attribute	Meaning
	ePTP Slave: The SM is operating as a Slave in point-to-point mode. The AP and the system do not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode.
Subscriber Module Priority	The configured priority of the SM in the sector.
Network Mode	<p>Bridge: The SM acts as a switch, and packets are forwarded or filtered based on their MAC destination address.</p> <p>NAT: The SM acts as a router, and packets are forwarded or filtered based on their IP header (source or destination) which can be grouped into subnets for finer granularity.</p> <p>Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.</p>
Downlink RSSI	The Received Signal Strength Indicator, which is a measurement of the power level being received by the SM's antenna.
Downlink SNR	The Signal to Noise Ratio, which is an expression of the carrier signal quality concerning signal noise and co-channel interference (or both).
Uplink MCS	Modulation and Coding Scheme - indicates the modulation mode used for the radio uplink, based on radio conditions (MCS 1-7, 9-15).
Downlink MCS	Modulation and Coding Scheme - indicates the modulation mode used for the radio downlink, based on radio conditions (MCS 1-7, 9-15).
cnMaestro Remote Management	Indicates whether the device is currently configured to be managed by the Cambium cloud management system - cnMaestro™.
cnMaestro Connection Status	The current management status of the device concerning the Cambium Cloud Server. When Enabled under Configuration > System , the device will be managed by the Cambium Remote Management System, which allows all Cambium devices to be managed from the Cambium Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Cloud Server.
Wireless MAC Address	The MAC address of the device Wireless interface.
Ethernet MAC Address	The MAC address of the device LAN (Ethernet) interface.
IP Address	The currently configured device IP address (LAN, Ethernet interface) is used for management access.
IPv6 Link Local Address	A link-local address is required for the IPv6-enabled interface (applications may rely on the link-local address even when there is no IPv6 routing). The IPv6 link-local address is comparable to the auto-configured IPv4 address 169.254.0.0/16.

Attribute	Meaning
IPv6 Address	The IPv6 address for the device when the device is used in Bridge mode. This is the IPv6 address for the subnet associated with the Ethernet interface when the device is used in NAT and Router modes.
Wireless IP Address	The currently configured device IP address (Wireless interface), when the SM is in Router (NAT) mode.
Separate Wireless Management IP Address	The currently configured device IP address (Separate Wireless Management interface) is used for management access when the SM is in Router (NAT) mode.
Date and Time	The current date and time on the device, subject to the configuration of the parameter Time Zone . If an NTP server is not specified, the date and time will begin from factory default upon radio startup.
System Uptime	The total uptime of the radio since the last reset.
System Description	The current configured system description.
Registered AP SSID	The AP SSID of the AP to which the SM is registered.
Registered AP MAC Address	The Wireless MAC Address of the AP to which the SM is registered.
Device Coordinates	The current configured Latitude and Longitude coordinates in decimal format.
DFS Status	Current DFS operational status.
Link Quality (Uplink)	The Uplink quality is based on the current MCS and Packet Error Rate (PER).
Link Capacity (Uplink)	The uplink capacity is based on the current MCS concerning the highest supported MCS (MCS15).
Ethernet Status	<p>Up: The Ethernet (LAN) interface is functioning properly. This also displays the current port speed and duplex mode to which the Ethernet port has auto-negotiated to or configured for.</p> <p>Down: The Ethernet (LAN) interface is either disconnected or has encountered an error and is not servicing traffic.</p>
Wireless Status	<p>Up: The radio (WAN) interface is functioning properly.</p> <p>Down: The radio (WAN) interface has encountered an error and is not servicing traffic.</p>

ePMP Device Configuration Parameters - Default Values

The following tables may be referenced for listings of default configuration values for ePMP device parameters.

Each factory default procedure will return the device to the values listed in the tables below.

Table 98: AP Ethernet Interface, Configuration Defaults

Attribute	Default Value
IP Assignment	DHCP
IP Address	192.168.0.1 (Default IP Address)
Subnet Mask	255.255.255.0
Management Access	Ethernet
Ethernet MTU	1500 bytes
Port Setting	Auto-Negotiate
VLANs	Disabled
Spanning Tree Protocol	Disabled
SM Traffic Isolation	Disabled
DHCP Option 82	Disabled
LLDP	Enabled(Receive and Transmit)

Table 99: AP Wireless Interface, Configuration Defaults

Attribute	Default Value
Driver Mode	TDD
Country Code	None / United States / Generic ETSI (ROW / FCC / ETSI device type, respectively) ROW devices do not transmit with Country Code set to None
Default SSID	Cambium-AP
ACS	Enabled
Channel Bandwidth	20 MHz
Downlink/Uplink Ratio	Flexible
Frame Size	5 ms
Max Range	3 Miles
Max Registrations Allowed	10/120 (Lite Devices / Full Capacity Devices, respectively)
Subscriber Module Receive Level	-60/-55 (ePMP 1000 / ePMP 2000, respectively)
Downlink Max Rage	MCS15

Attribute	Default Value
Management Traffic Rate	MCS1
Colocation Mode	Disabled
Synchronization Mode	Disabled
Uplink Antenna Selection	Auto (ePMP 2000 with Smart Antenna only)

Table 100: AP Security Parameters, Configuration Defaults

Attribute	Default Value
WPA2 Security	Enabled (default value Cam39-Tai!wdmv)
L2/L3 Firewall	Disabled
Wireless MAC Address Filtering	Disabled
SNMPv2	Enabled (with default Community Strings) Read-Only Community String - public Read-Write Community String - private Trap Community String - cambiumtrap

Table 101: SM Ethernet Interface, Configuration Defaults

Attribute	Default Value
Network Mode	Bridge
IP Assignment	DHCP
IP Address	192.168.0.2 (Default IP Address)
Subnet Mask	255.255.255.0
Ethernet MTU	1500 bytes
Port Setting	Auto-negotiate
Management VLAN	Disabled
Data VLAN	Disabled
Membership VLANs	Disabled
IPv6	Disabled
ARP-NAT	Disabled
Spanning Tree Protocol	Disabled

Attribute	Default Value
DHCP Server Below SM	Disabled
LLDP	Enabled (Receive and Transmit)
Ethernet Port Security	Disabled

Table 102: SM Wireless Interface, Configuration Defaults

Attribute	Default Value
Driver Mode	TDD
Country Code	Follow AP / United States (ROW, ETSI devices / FCC devices, respectively)
Scanning List	All available frequencies selected for 20 MHz and 40 MHz channel bandwidths
Network Entry RSSI Threshold	-90 dBm
Network Entry SNR Threshold	0 dB
Uplink Max Rate	MCS15
Uplink Antenna Selection	Auto (5 GHz SMs only)
Max Tx Power	Auto (Automatic Transmit Power Control and Regulatory-controlled)

Table 103: SM Security, Configuration Defaults

Attribute	Default Value
RADIUS	Enabled (default EAP-TTLS credentials username: subscriber1, password: cambium)
WPA2	Enabled (default value Cam39-Tailwdmv)
L2/L3 Firewall	Disabled
SNMPv2	Enabled (with default Community Strings) Read-Only Community String - public Read-Write Community String - private Trap Community String - cambiumtrap

Configuring connectorized radios using the Quick Start menu

The **Quick Start** tab contains a listing of parameters required to configure a simple radio link and to configure requisite networking parameters. After configuring an AP, SM and resetting both devices, the SM is ready to associate (register) to the AP.

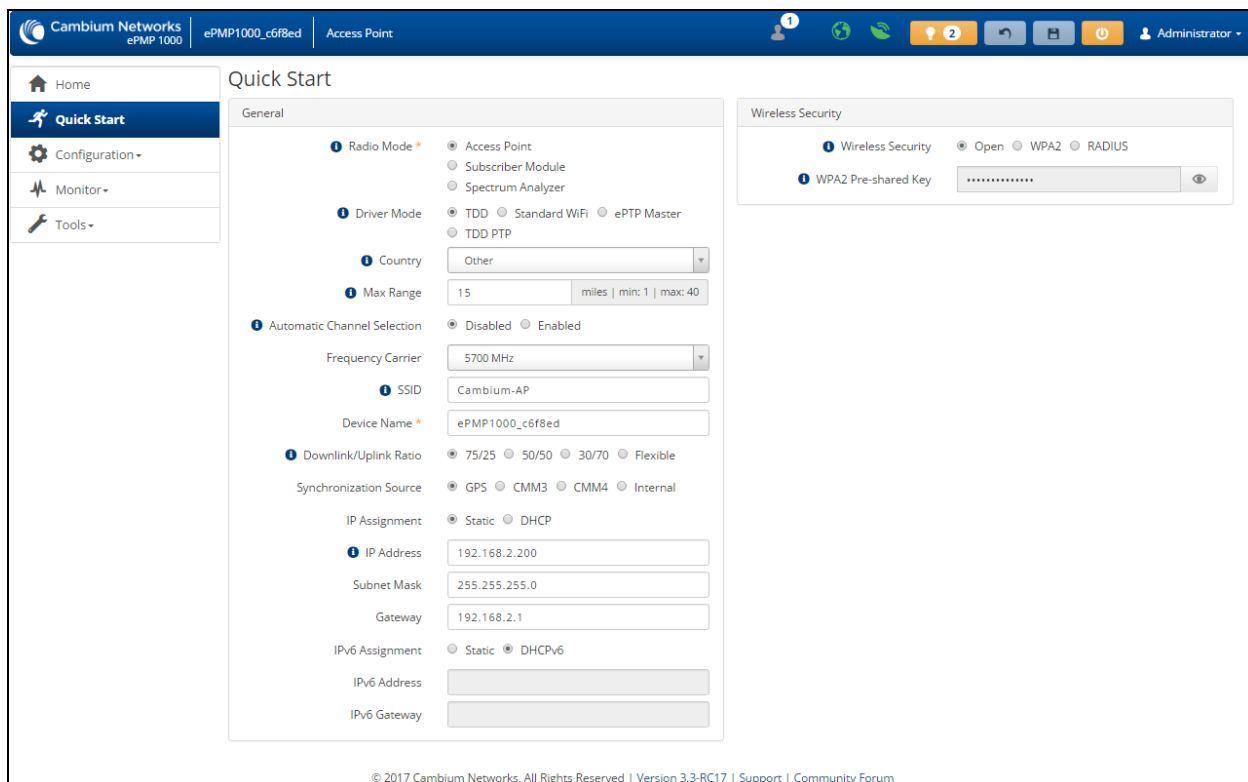


Figure 44: AP Quick Start menu

To configure an AP via the Quick Start menu, follow this procedure:

Procedure:

1. Start the web browser from the management PC.
2. Navigate to the **Quick Start** menu.
3. Configure the parameter **Radio Mode**:
 This parameter controls the function of the device – All ePMP devices may be configured to operate as an Access Point (AP), Subscriber Module (SM), or as a Spectrum Analyzer. For initial link bring-up, choose **Access Point**.
4. Configure the parameter **Access Point Mode**:
 This parameter controls the mode of operation of the Access Point – An AP may be configured to operate in TDD mode for multipoint access, PTP mode for point-to-point access using TDD, Standard WiFi, or as an ePTP Master. For initial link bring-up, choose **TDD**. When the AP is an **ePTP Master**, the system does not support GPS Synchronization but can provide **significantly lower latency** than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode. Configuring the AP in **Standard WiFi** mode allows any 802.11 clients to register to the AP.
5. Configure the parameter **Country**:
Country 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 country code, if applicable
- Frequency selection limiting (based on valid frequencies for the configured **Country**)

Select the country in which your network will be operating.

6. Configure the parameter **Automatic Channel Selection (ACS)**:

When ACS is enabled, the AP will automatically scan the available spectrum and choose a channel with the lowest occupancy. For more information on this parameter please see [AP Automatic Channel Selection page](#).

7. Configure the parameter **Frequency Carrier**:

Configure the frequency carrier for RF transmission. This list is dynamically adjusted to the regional restrictions based on the setting of the **Country Code** parameter. Ensure that a thorough spectrum analysis has been completed before configuring this parameter.

8. Configure parameter **AP SSID (Name)**:

The **AP SSID (Name)** is used to identify the AP and is used to configure the SM with the appropriate AP with which to register. Ensure that this parameter is configured uniquely for each AP in the network.

9. Configure the parameter **Downlink/Uplink Ratio**:

Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the SM). For example, if the aggregate (uplink and downlink total) throughput on the AP is 90 Mbps, then 75/25 specified for this parameter allocates 67.5 Mbps for the downlink and 22.5 Mbps for the uplink. The default for this parameter is 75/25.



Caution
You must set this parameter the same for all APs in a cluster.

10. Configure the parameter **Synchronization Source**:

This parameter defines the timing source for the device which can be GPS-based or internally generated. Select **GPS** if the AP will receive synchronization pulses from a connected GPS antenna. Select **CMM3 or CMM4** if the device will receive GPS synchronization pulses from a co-located Cambium Cluster Management Module (see PMP Synchronization Solutions User Guide). Select **Internal** if no GPS synchronization source is available (in this mode, transmission between co-located devices will create radio interference). If **Flexible** is chosen as the **DL/UL Ratio** or if the **Access Point Mode** is chosen as **ePTP Master**, then this parameter will be greyed out.

11. Configure the parameter **IP Assignment**:

If **DHCP** is selected, the DHCP server automatically assigns the IP configuration (Ethernet (LAN) IP Address, Ethernet (LAN) IP Subnet Mask, Gateway IP Address (LAN)) and the values of those individual parameters (below) are not used. To configure a simple test network, select mode **Static**.

12. Configure the parameter **IP address**:

Internet Protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. To configure a simple test network, this field may be left at default (192.168.0.1).

13. Configure the parameter **Subnet Mask**:

The Subnet Mask defines the address range of the connected IP network. To configure a simple test network, this field may be left at default (255.255.255.0).

14. Configure the parameter **Gateway**:

The IP address of the device on the current network acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks. To configure a simple test network, this parameter may be left at default (blank).

15. Configure the parameter **IPv6 Assignment**

IPv6 Assignment specifies how the IPv6 address is obtained.

Static: Device management IP addressing is configured manually in fields IPv6 Address and IPv6 Gateway.

DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters **IPv6 Address** and **IPv6 Gateway** are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.

16. Configure the parameter **IPv6 Address**


Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.

17. Configure the parameter **IPv6 Gateway**

Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.

18. Configure the parameter **WPA2 Pre-shared Key**

Configure this key on the AP and then configure each of the network SMs with this key to complete the authentication configuration. This key must be between 8 to 128 symbols. Click the

visibility icon  to toggle the display of the key's contents.

19. Click the **Save** icon, then click the **Reset** icon

Configuring SM units using the Quick Start menu

The **Quick Start** tab contains a simple listing of parameters required to configure a simple radio link and to configure requisite networking parameters.

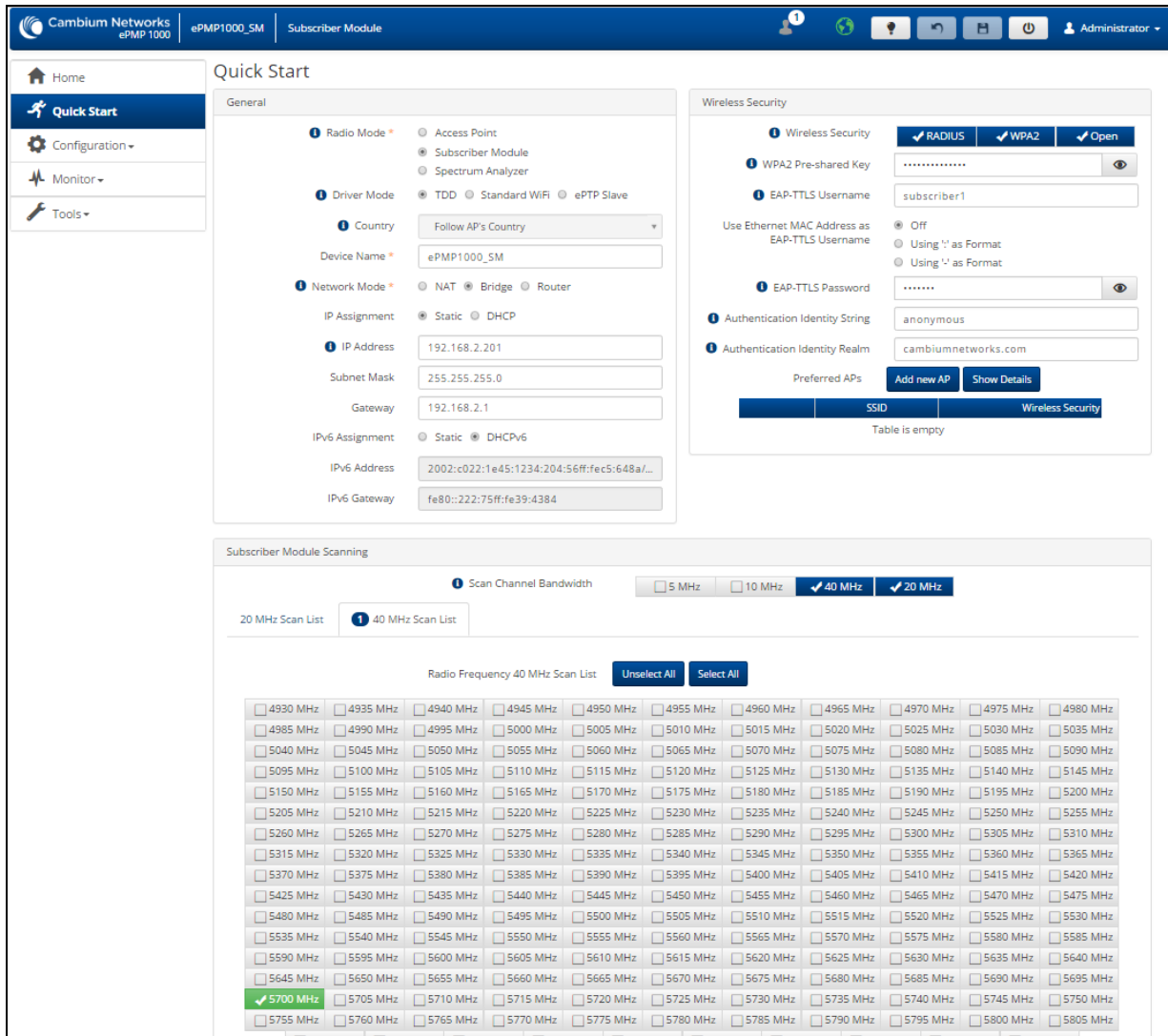


Figure 45: SM Quick Start menu

To configure an SM via the **Quick Start** menu, follow this procedure:

Procedure:

1. Start the web browser from the management PC.
2. Navigate to **Quick Start** menu.
3. Configure the parameter **Radio Mode**:

This parameter controls the function of the device – all ePMP devices may be configured to operate as an Access Point (AP), Subscriber Module (SM), or as a Spectrum Analyzer. For initial link bring-up, choose **Subscriber Module**.

4. Configure the parameter Subscriber Module Mode:

This parameter controls the mode of operation of the Subscriber Module – An SM may be configured to operate in **TDD** mode for point-to-point and point-to-multipoint access, **Standard WiFi** mode providing the capability to connect to any AP operating in standard WiFi mode or as an **ePTP Slave**. For initial link bring-up, choose **TDD**. When the SM is an **ePTP Slave**, the system does not support GPS Synchronization but can provide **significantly lower latency** than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode.

5. The **Country** is automatically retrieved from the AP and requires no configuration.

Country 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 country code, if applicable
- The frequency range of operation depending on local limitations

6. Configure the parameter **Device Name**:

The SM Device Name is used to identify the device on the network. This parameter may be modified or left at the default value of **Cambium-SM**.

7. Configure the parameter **Network Mode**:

Bridge: The SM acts as a switch, and packets are forwarded or filtered based on their MAC destination address.

NAT: The SM acts as a router, and packets are forwarded or filtered based on their IP header (source or destination) which can be grouped into subnets for finer granularity.

Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.

8. Configure the parameter **Wireless IP Assignment**:

If **DHCP** is selected, the DHCP server automatically assigns the IP configuration (Ethernet (LAN) IP Address, Ethernet (LAN) IP Subnet Mask, Gateway IP Address (LAN)) and the values of those individual parameters (below) are not used. To configure a simple test network, this parameter must be configured to **Static**.

9. Configure the parameter **Wireless IP Address**:

Internet Protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. To configure a simple test network, this field must be configured to 192.168.0.2.

10. Configure the parameter **Wireless Subnet Mask**:

The Subnet Mask defines the address range of the connected IP network. To configure a simple test network, this field may be left at default (255.255.255.0).

11. Configure the parameter **Wireless Gateway**:

The IP address of the device on the current network acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks. To configure a simple test network, this parameter may be left at default (blank).

12. Configure the parameter **IPv6 Assignment**

IPv6 Assignment specifies how the IPv6 address is obtained.

Static: Device management IP addressing is configured manually in fields IPv6 Address and IPv6 Gateway.

DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters **IPv6 Address** and **IPv6 Gateway** are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.

13. Configure the parameter IPv6 Address


Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.

14. Configure the parameter IPv6 Gateway

Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.

15. Configure the parameter **WPA2 Pre-shared Key:**


Configure each of the network SMs with this key (matching the AP's configured key) to complete the authentication configuration. This key must be between 8 to 128 symbols. Click the visibility

icon  to toggle the display of the key's contents.

16. Configure the parameter **EAP-TTLS Username:**

Configure each of the network SMs with this EAP-TTLS Username (matching the credentials on the RADIUS server being used for the network). Optionally, the device MAC Address can be used as the EAP-TTLS Username in either “.” or “-” delimited format.

17. Configure the parameter **EAP-TTLS Password:**

Configure each of the network SMs with this EAP-TTLS Password (matching the credentials on the RADIUS server being used for the network). Click the visibility icon  to toggle the display of the password's contents.

18. Configure the parameter Authentication Identity String:

Configure each of the network SMs with this Identity string (matching the credentials on the RADIUS server being used for the network). The default value for this parameter is “anonymous”.

19. Configure the parameter Authentication Identity Realm:

Configure each of the network SMs with this Identity realm (matching the credentials on the RADIUS server being used for the network). The default value for this parameter is “cambiumnetworks.com”.

20. Configure the **Preferred AP's**

The **Preferred AP's** is comprised of a list of up to 16 APs to which the SM sequentially attempts registration. For each AP configured, if authentication is required, enter a **Pre-shared Key** associated with the configured **AP SSID**. If this list is empty or if none of the configured APs are found, the SM scans and registers to the best AP signal found (with matching radio and/or authentication settings).

21. Configure the parameter Subscriber Module Scanning:

The Radio Scan List determines the frequencies for which the SM scans for AP signaling. For a simple radio network setup, click **Select All** to scan all frequencies.

22. Click the **Save** icon, then click the **Reset** icon

Using the AP menu options

Use the menu navigation bar in the top and left panels to navigate to each web page. The functional areas that may be accessed from each menu option are listed in [Table 104](#). Some of the parameters are only displayed for specific system configurations.

Table 104: Functional areas accessed from each AP menu option

Menu option	Menu Details
Quick Start	Configuring connectorized radios using the Quick Start menu
Configuration	AP Configure menu
Radio	AP Radio page
Quality of Service	AP Quality of Service page
System	AP System page
Network	AP Network page
Security	AP Security page
Monitor	AP Monitor menu
Performance	AP Performance page
System	AP System page
Wireless	AP Wireless page
Throughput Chart	AP Throughput Chart page
GPS	AP GPS page
Network	AP Network page
System Log	AP System Log page
Tools	AP Tools menu
Software Upgrade	AP Software Upgrade page
Backup / Restore	AP Backup/Restore page

Menu option	Menu Details
License Management	AP Backup/Restore page
eDetect	AP eDetect page
Spectrum Analyzer	AP Spectrum Analyzer page
Automatic Channel Selection	AP Automatic Channel Selection page
eAlign	AP eAlign page
Wireless Link Test	AP Wireless Link Test page
Ping	AP Ping page
Traceroute	AP Traceroute page

AP Configure menu

Use the Configure menu to access all applicable device configuration parameters. The configuration menu contains the following pages:

- [AP Radio page](#)
- [AP Quality of Service page](#)
- [AP System page](#)
- [AP Network page](#)
- [AP Security page](#)

AP Radio page

Use the Radio page to configure the device radio interface parameters.



Caution

Plan Configuration modifications since modifying radio parameters may result in a wireless outage.

Cambium Networks ePMP 2000 Zurich ePMP2000_d1f2... Access Point Administrator

Configuration > Radio

General

- Radio Mode: Access Point, Subscriber Module, Spectrum Analyzer
- Driver Mode: TDD, Standard WiFi, ePTP Master, TDD PTP
- Country:
- Range Unit: Miles, Kilometers

Access Point Configuration

- SSID:
- Max Registrations Allowed: subscribers | min: 1 | max: 120
- Max Range: miles | min: 1 | max: 40
- Automatic Channel Selection: Disabled, Enabled
 - Channel Bandwidth: 5 MHz, 10 MHz, 20 MHz, 40 MHz
 - Frequency Carrier:
- Frequency Reuse: Off, Front Sector, Back Sector
 - Alternate Frequency Carrier 1 Channel Bandwidth: 5 MHz, 10 MHz, 20 MHz, 40 MHz
 - Alternate Frequency Carrier 1:
 - Alternate Frequency Carrier 2 Channel Bandwidth: 5 MHz, 10 MHz, 20 MHz, 40 MHz
 - Alternate Frequency Carrier 2:

Power Control

- Transmitter Output Power: dBm | min: 0 | max: 30
- Antenna Gain: dBi | min: 0 | max: 40
- Subscriber Module Target Receive Level: dBm | min: -80 | max: -40
- Uplink Antenna Selection: Auto, Forced Sector Antenna, Forced Smart Antenna

Scheduler

- Downlink/Uplink Ratio: 75/25, 50/50, 30/70, Flexible
- Frame Size: 2.5 ms, 5 ms
- Downlink Max Rate:
- Management Traffic Rate: MCS0, MCS1

Synchronization

- Co-location Mode: Disabled, Enabled
- Synchronization Source: GPS, CMM3, CMM4, Internal
- Synchronization Holdoff Time: sec | min: 20 | max: 86400


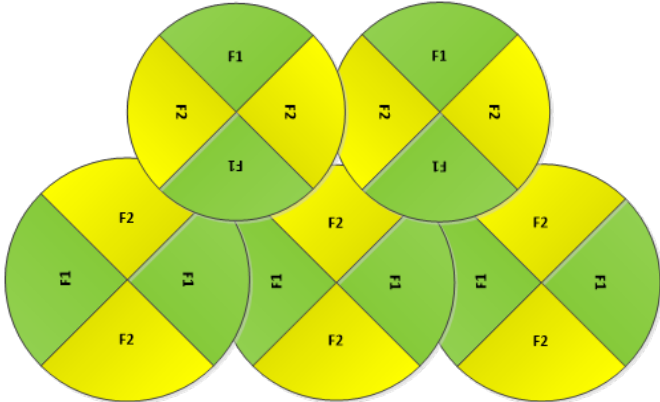
© 2017 Cambium Networks, All Rights Reserved | Version 3.3-RC14 | Support | Community Forum

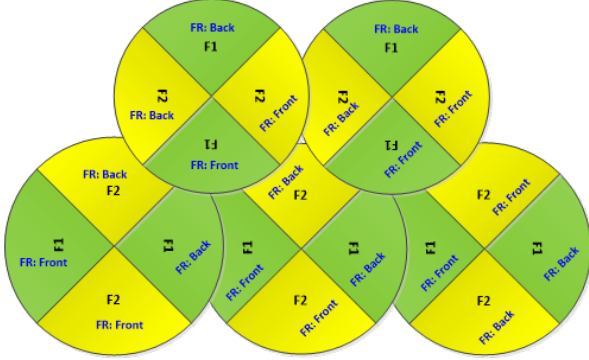
Figure 46: Figure 40 AP Radio page

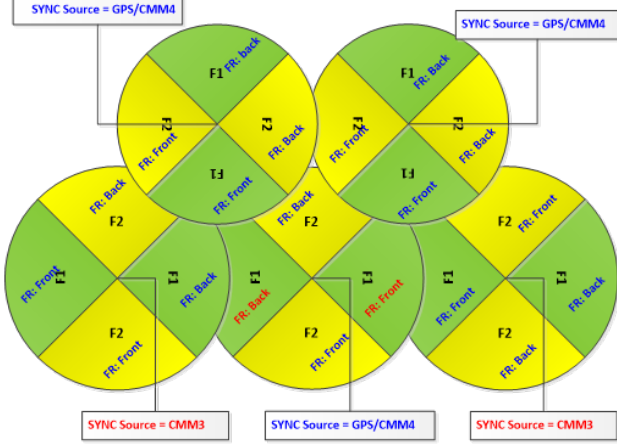
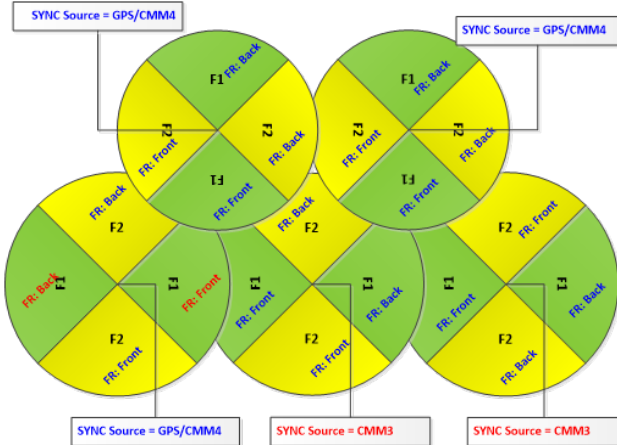
Table 105: AP Radio Configuration attributes

Attribute	Meaning
General	
Radio Mode	This parameter controls the function of the device - All ePMP devices may be configured to operate as an Access Point (AP), Subscriber Module (SM), or Spectrum Analyzer. For initial link bring-up, choose AP .
Driver Mode	<p>TDD: The Access Point is operating in point-to-multipoint (PMP) mode using TDD scheduling. The AP can GPS synchronize in this mode (except when in Flexible mode).</p> <p>Standard WiFi: The Access Point is operating as a Standard 802.11n Access Point and will allow any 802.11 clients to connect to it. QoS capability and Link Quality/Capacity indicators are not available in this mode.</p> <p>ePTP Master: The Access Point is operating as a Master in point-to-point mode. The AP does not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode.</p> <p>TDD PTP: The Access Point is operating in point-to-point (PTP) mode using TDD scheduling. The AP can GPS synchronize in this mode (except when in Flexible mode).</p>
Point-to-Point Access	<p>First Subscriber Module: The system is configured to accept only the 1st registered SM. Network entry is denied for all subsequent SM network entry requests.</p> <p>MAC Filtering: The system is configured to accept only one SM registration, and this registration is limited by SM MAC Address (the SM Wireless MAC Address).</p>
Subscriber Module Wireless MAC	Configure the Wireless MAC Address of the sole SM which is granted registration to the AP. All other network entry attempts are rejected by the AP. The SM's Preferred AP List may be configured with the destination point-to-point AP to ensure that the SM connects with the intended AP.
Country	<p>From the drop-down list, select the country in which the radio is operating.</p> <p>Country Code settings affect the radios in the following ways:</p> <ul style="list-style-type: none"> • Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain) • DFS operation is enabled based on the configured country code, if applicable • Frequency selection limiting, based on regional limitations
Range Unit	<p>Miles: The Max Range setting and resulting frame calculations are configured in units of miles.</p> <p>Kilometers: The Kilometers setting and resulting frame calculations are configured in units of kilometers.</p>
Access Point Configuration	


Attribute	Meaning
SSID	The AP SSID is used to identify the AP and is used to configure the SM with the appropriate AP with which to register. Ensure that this parameter is configured uniquely for each AP in the network.
Max Registrations Allowed	<p>Based on sector/network planning and SM service level implementations, this parameter allows the user to set the maximum number of SMs that are allowed to register/network entry. The maximum number of SMs allowed for each channel bandwidth is as follows:</p> <p>20/40 MHz: 120 subscribers</p> <p>10 MHz: 60 subscribers</p> <p>5 MHz: 30 subscribers</p> <p>The default value is 60.</p> <p>For DFS regions, the max number of SMs will be limited based on the channel bandwidth of the current operating channel, i.e. Frequency Carrier, Alternate Frequency Carrier 1, or Alternate Frequency Carrier 2.</p>
Max Range	<p>Enter the number of miles or kilometers for the furthest distance from which an SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance:</p> <ul style="list-style-type: none"> • does not increase the power of transmission from the AP. • can reduce aggregate throughput. <p>Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. The AP will reject any SM network entry attempts from outside the configured maximum range. The default value is 3 miles.</p>
WLAN	<p>When the Access Point Mode is set to Standard WiFi, configure this parameter:</p> <p>Enabled: The ePMP AP operates as WLAN device and allows any 802.11 clients to connect to it within a 100-meter radius.</p> <p>Disabled: The ePMP AP operates in Standard WiFi mode to allow outdoor 802.11n clients to connect to it at longer distances and is typically used to migrate non-Cambium SMs to ePMP SMs.</p>
Automatic Channel Selection	<p>Enabled – This enables the Automatic Channel Selection (ACS) feature. ACS allows the radio to scan the entire band (governed by the Country setting) and chooses a channel with the lowest channel occupancy i.e. lowest interference level. To run the ACS feature (once enabled), the radio will have to be rebooted or manually triggered using Tools->Automatic Channel Selection. When ACS is running, the radio measures the occupancy level of the channel (measured in terms of an internal interference metric) and uses an algorithm to decide to choose the best channel within the band. The channel chosen is not based just on the occupancy level channel but also on the occupancy level of adjacent channels.</p> <p>Disabled – ACS is disabled and the operator should configure a Frequency Carrier manually.</p>


Attribute	Meaning
	<div style="display: flex; align-items: center;">  <div style="border: 1px solid black; padding: 5px; background-color: #e6f2ff;"> <p>Note</p> <p>The channel bandwidth configured before enabling and running ACS will be used to automatically select a channel. For example: If the operator manually configured a channel bandwidth of 20MHz, ACS will scan and choose a channel of 20MHz wide channel. To switch ACS to 40MHz or other channel bandwidth, the operator should disable ACS, manually configure 40MHz or desired channel bandwidth on the radio, then enable and run ACS.</p> </div> </div>
Channel Bandwidth	Configure the channel size used by the radio for RF transmission. This value must match between the AP and SMs.
Frequency Carrier	Configure the frequency carrier for RF transmission. This list is dynamically adjusted to the regional restrictions based on the setting of the Country Code parameter.
Frequency Reuse	<p>The Frequency Reuse Mode parameter allows operators to define which APs are co-located (or within radio range) with other APs. This definition results in an automatic radio network modification such that self-interference is reduced amongst the co-located sectors.</p> <p>A network in which two frequencies “F1” and “F2” are reused throughout the installation is shown in AP Radio page. Frequency reuse installation</p>  <p>The set of APs to configure the Frequency Reuse Mode option is dependent on the GPS synchronization sources in the whole network, CMM3, CMM4, or “onboard GPS” (GUI options are: GPS or CMM).</p> <p><i>The GPS sync source is the same on all APs or is a combination of “onboard GPS” and CMM4</i></p> <p>In this configuration the GPS synchronization source in the whole network is one of the following:</p> <ol style="list-style-type: none"> 1. “onboard GPS” or 2. CMM4 or 3. CMM3 or


Attribute	Meaning
	<p data-bbox="505 258 1170 285">4. A mix of “onboard GPS” and CMM4 (but NOT CMM3)</p> <p data-bbox="467 310 1354 369">For instructions on how to configure Frequency Reuse Mode to ensure that interference is reduced throughout the installation, see Figure 47.</p> <p data-bbox="485 392 1084 420"><i>Figure 47: Frequency reuse configuration example</i></p>  <p data-bbox="467 850 1336 909">The rules in selecting the APs to enable the Frequency Reuse Mode in this installation are:</p> <ol data-bbox="509 934 1422 1045" style="list-style-type: none"> 1. Only ONE of the APs on the same tower configured with the same frequency must be configured with the Frequency Reuse Mode parameter set to Frequency-Reuse-Back; the other AP must be configured with Frequency Reuse Mode set to Frequency-Reuse-Front. <p data-bbox="467 1071 1406 1129">Also, APs on different towers facing each other with overlapped coverage must be configured with Frequency Reuse Mode set to Frequency-Reuse-Back.</p> <p data-bbox="467 1152 1390 1180"><i>The GPS sync source is a mixture of all types (CMM3, CMM4 & “onboard GPS”)</i></p> <p data-bbox="467 1203 1354 1262">In this configuration the GPS sync source in the whole network is one of the following:</p> <ol data-bbox="509 1287 1008 1430" style="list-style-type: none"> 1. (CMM3 and “onboard GPS”) or 2. (CMM3 and CMM4) or 3. (CMM3 and CMM4 and “onboard GPS”) <p data-bbox="467 1455 1422 1514">For more examples of which APs to enable the Frequency Reuse Mode feature in this mixture of sync sources, see Figure 48 and Figure 49.</p>

Attribute	Meaning
	 <p data-bbox="483 730 1404 793">Figure 48: Figure 43 Example 1 - Frequency reuse configuration, a mixture of GPS synchronization sources</p>  <p data-bbox="483 1312 1404 1375">Figure 49: Figure 44 Example 2 - Frequency Reuse Configuration with Mixture of GPS sources</p> <p data-bbox="467 1417 1412 1501">The rules in selecting the APs to configure Frequency Reuse Mode to Frequency Reuse Mode to Frequency-Reuse-Front or Frequency-Reuse-Back in a mixture of sync sources installations are:</p> <ol data-bbox="511 1522 1380 1743" style="list-style-type: none"> 1. Only ONE of the APs on the same tower configured with the same frequency must have Frequency Reuse Mode set to Frequency-Reuse-Back if the sync source of both APs is the same or the sync is a combination of “onboard GPS” and CMM4; the other AP will have the Frequency-Reuse-Front ON. 2. For the APs on different towers facing each other with overlapped coverage:

Attribute	Meaning
	<ul style="list-style-type: none"> a. If both APs have the same sync source then only ONE of them must have the Frequency-Reuse-Back ON; the other AP shall have the Frequency-Reuse-Front ON. b. If one AP has “onboard GPS” as sync source and the other one has CMM4 then only ONE of them must have Frequency-Reuse - Back ON; the other AP shall have Frequency-Reuse-Front ON. c. If one AP has “onboard GPS” or CMM4 as sync source and the other one has CMM3 then: <ul style="list-style-type: none"> 1. If the AP with CMM3 sync source has Frequency-Reuse-Back ON, then the other AP (with “onboard GPS” or CMM4 sync source) must have the Frequency-Reuse-Back ON. 2. If the AP with CMM3 sync source has Frequency Reuse Mode set to Off, then the other AP (with “onboard GPS” or CMM4 sync source) must have Frequency Reuse Mode set to Off.
Alternate Frequency Carrier 1 Channel Bandwidth	Configure the first channel bandwidth configuration that will be used for RF transmission if DFS detection causes the radio to switch from using the channel bandwidth configured in Channel Bandwidth .
Alternate Frequency Carrier 1	Configure the first frequency that will be used for RF transmission if DFS detection causes the radio to switch from using the frequency configured in Frequency Carrier . It is important to set this frequency also in the SMScan List .
Alternate Frequency Carrier 2 Channel Bandwidth	Configure the second channel bandwidth configuration that will be used for RF transmission if DFS detection causes the radio to switch from using the channel bandwidth configured in Channel Bandwidth .
Alternate Frequency Carrier 2	Configure the second frequency that is used for RF transmission if DFS detection causes the radio to switch from using the frequencies configured in Frequency Carrier and DFS Alternate Frequency Carrier 1 . It is important to set this frequency also in the SMScan List .
Power Control	
Transmitter Output Power	<p>This value represents the combined power of the AP’s two transmitters. This value may be automatically adjusted based on the configuration of the parameter Country.</p> <p>Nations and regions may regulate transmitter output power. For example</p> <ul style="list-style-type: none"> • 2.4 GHz and 5 GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. <p>The professional installer of the equipment has the responsibility to</p> <ul style="list-style-type: none"> • maintain awareness of applicable regulations. • calculate the permissible transmitter output power for the module. • confirm that the initial power setting is compliant with national or regional regulations

Attribute	Meaning
	<ul style="list-style-type: none"> confirm that the power setting is compliant following any reset of the module to factory defaults.
Antenna Gain	This value represents the amount of gain introduced by an external antenna (minus cable loss). This value is used in calculating the unit's Equivalent Isotropic Radiated Power (EIRP) level. For certain Country Code configurations, the unit's EIRP may be limited based on regional regulations.
Subscriber Module Target Receive Level	<p>Each SM's transmitter output power is automatically set by the AP. The AP monitors the received power from each SM and adjusts each SM's transmitter output power so that the received power at the AP from the SM is not greater than what is configured in SM Target Received Power Level. These automatic power adjustments ensure that the SM is not transmitting excessive energy (raising system noise level) and that the SM can achieve an optimal modulation state (and maximum achievable throughput). Nominally, target receive levels must be set lesser than -60 dBm to prevent interference from co-located co-channel sectors.</p>
Uplink Antenna Selection	<p>Uplink Antenna Selection specifies the antenna to be used in the uplink. This parameter is specific to ePMP 2000 APs with an optional Smart Antenna.</p> <p>Auto: The AP decides which antenna to use (sector or Smart Antenna) for uplink communications based on internal quality metrics.</p> <p>Forced Sector Antenna: The AP uses the Sector Antenna for all SM uplink communications.</p> <p>Forced Smart Antenna: The AP uses the smart antenna for all SM uplink communications.</p> <div data-bbox="479 1129 1417 1390" style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p> Note</p> <p>If the AP is configured with Uplink Antenna Selection set to Auto and an SM is set to Forced Sector Antenna or Forced Smart Antenna, the SM setting will be enforced.</p> <p>If the AP is configured with Uplink Antenna Selection set to Forced Sector Antenna or Forced Smart Antenna and an SM is set to a conflicting Forced setting, the AP's setting will be enforced.</p> </div>
Scheduler	
Downlink/Uplink Ratio	Configure the schedule of downlink traffic to uplink traffic on the radio link. The first three options, 75/25 , 50/50 , and 30/70 , allow the radio to operate in a fixed ratio on every frame. In other words, this ratio represents the amount of the total radio link's aggregate throughput that will be used for downlink resources, and the amount of the total radio link's aggregate throughput that will be used for uplink resources. The fourth option, Flexible , allows the radio to dynamically choose the amount of the total radio's aggregate throughput that is used for downlink and uplink resources, every frame.

Attribute	Meaning
	 <div style="background-color: #f4a460; padding: 5px; border: 1px solid black;"> <p>Caution</p> <p>Setting this parameter to Flexible causes the radio to operate in unsynchronized mode. For all other settings, if the AP is in a cluster or is in the range of another AP, then you must set this parameter on all other APs in the cluster and range the same. Otherwise, overlapping RF transmissions will introduce system interference.</p> </div>
Frame Size	<p>Configure the frame size for use when in TDD or TDD PTP mode. 2.5 ms frame size allows for co-location (Synchronization) with PMP 100 series of radios. It provides lower latency than a 5 ms frame with approximately 10% lower throughput. Frame size is irrelevant when the Downlink/Uplink Ratio is set to Flexible. Please refer to the ePMP and PMP 100 Co-location and Migration Recommendations Guide for guidance on synchronizing ePMP and PMP 100.</p>
Downlink Max Rate	<p>Configure the MCS (Modulation and Coding Scheme) rate beyond which the radio's scheduler should not exceed when transmitting data traffic on the downlink. This is useful in situations where there are high variance and unpredictability in the interference present in the environment causing packet loss. Reducing the max rate to a lower MCS (than the default MCS 15) may help in these situations. Reducing the Downlink Max Rate will result in reduced sector capacity. Not available when AP is an ePTP Master or Standard WiFi.</p>
Management Traffic Rate	<p>MCS0: The system is configured to use the MCS0 rate for all management messages. This allows for improved link stability and range in a high interference environment.</p> <p>MCS1: The system is configured to use the MCS1 rate for all management messages. This allows for slightly higher sector throughput. This is the default setting.</p>
Synchronization	
Co-location Mode	<p>Disabled: The ePMP device can synchronize only with other ePMP Access Points.</p> <p>Enabled: The ePMP device can be configured to synchronize with PMP 100 or PMP 450 series of radios in addition to other ePMP Access Points. Please refer to the ePMP and PMP 100 Co-location and Migration Recommendations Guide for guidance on synchronizing ePMP and PMP 100. Verify that frame size (ms) is configured equally across the co-located installations.</p>
Synchronization Source	<p>GPS: Synchronization timing is received via the AP's connected GPS antenna. Co-located or in-range APs receiving synchronization via GPS or CMM transmits and receives at the same time, thereby reducing self-interference.</p> <p>CMM3 and CMM4: Synchronization timing is received via the AP's Ethernet port via a connected Cambium Cluster Management Module (CMM). Co-located or in-range APs receiving synchronization via GPS or CMM will transmit and receive at the same time, thereby reducing self-interference. For more information on CMM configuration, refer to the PMP Synchronization Solutions User Guide.</p> <p>Internal: Synchronization timing is generated by the AP and the timing is not based on GPS pulses.</p>

Attribute	Meaning
	 <p data-bbox="618 260 711 285">Caution</p> <p data-bbox="618 310 1393 401">If a CMM is being used, verify that the cables from the CMM to the network switch are at most 30 ft (shielded) or 10 Ft (unshielded) and that the network switch is not PoE (802.3af).</p> <p data-bbox="618 426 1398 516">APs using Synchronization Source of Internal will not transmit and receive in sync with other co-located or in-range APs, which introduces self-interference into the system.</p>
Synchronization Source of Co-located System	<p data-bbox="467 552 1398 577">Configure the Synchronization source of the co-located PMP 100 Access Point.</p> <p data-bbox="467 602 1414 722">GPS: The co-located PMP 100 AP receives synchronization timing via the Cambium UGPS (Universal Global Positioning System) module. Co-located or in-range ePMP APs receiving synchronization via GPS or CMM transmits and receives at the same time, thereby reducing self-interference.</p> <p data-bbox="467 747 1414 995">CMM3 and CMM4: The co-located PMP 100 AP receives synchronization timing its Ethernet port via a connected Cambium Cluster Management Module (CMM). Co-located or in-range ePMP APs receiving synchronization via GPS or CMM will transmit and receive at the same time, thereby reducing self-interference. For more information on CMM configuration, refer to the PMP Synchronization Solutions User Guide. Please refer to the ePMP and PMP 100 Co-location and Migration Recommendations Guide for guidance on synchronizing ePMP and PMP 100.</p>
Synchronization Holdoff Time	<p data-bbox="467 1024 1414 1304">The Synchronization Holdoff Time is designed to gracefully handle fluctuations/losses in the GPS synchronization signaling. After the AP has received a reliable synchronization pulse for at least 60 seconds, if there is a loss of synchronization signal, the Synchronization Holdoff timer is started. During the holdoff interval, all SM registrations are maintained. If a valid GPS synchronization pulse is regained during the holdoff interval, then the AP continues to operate normally. If a valid synchronization pulse is not regained from the GPS source during the holdoff interval, then the AP ceases radio transmission. Default is 30 seconds.</p>
Advanced	<p data-bbox="467 1329 1414 1541">RTS/CTS (Request to Send / Clear to Send) is the optional mechanism used by the 802.11 (Standard WiFi) wireless networking protocol to reduce frame collisions introduced by the problem known as the hidden node problem. Under this mechanism, specific RTS, CTS, and ACK (Acknowledgement) frames are exchanged between the AP and SM to schedule transmission of packets over the wireless link. The ability to use this mechanism is available when Access Point Mode is configured as Standard WiFi.</p>
Downlink CTS	<p data-bbox="467 1570 1382 1596">This parameter applies to the CTS mechanism for downlink data transmission.</p> <p data-bbox="467 1621 1365 1680">Disabled: The AP does not wait for a CTS frame from the SM/Client before it sends downlink data.</p> <p data-bbox="467 1705 1292 1764">Enabled: The AP simulates a CTS frame sent to itself notifying the SMs connected to it that it is going to transmit data on the downlink.</p>
Uplink CTS/RTS	<p data-bbox="467 1791 1360 1816">This parameter applies to RTS/CTS mechanism for uplink data transmission.</p>

Attribute	Meaning
	When Enabled , SM/Client must send an RTS frame and, only upon receiving a CTS frame from the AP can it transmit uplink data.
RTS Threshold	Configure the RTS packet size threshold for downlink data transmission. The range is between 0–2347 octets. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold. If the packet size that the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. Otherwise, the data frame gets sent immediately.

AP Quality of Service page

The ePMP platform supports three QoS priority levels (not available in ePTP Master mode) using air fairness, priority-based starvation avoidance scheduling algorithm.

Ordering of traffic amongst the priority levels is based on a percentage of total link throughput. In other words, all priorities receive some throughput so that low priority traffic is not starved from the transmission. In effect, the greatest amount of throughput is guaranteed to the VOIP priority level, then High, then Low.

Priority Level	ePMP Traffic Priority Label
Highest Priority	VOIP (only utilized when VOIP Enable is set to Enabled)
Medium Priority	High
Lowest Priority	Low

By default, all traffic passed over the air interface is low priority. The AP's Quality of Service page may be utilized to map traffic to certain priority levels using QoS classification rules. The rules included in the table are enforced starting with the first row of the table.



Caution

Each additional traffic classification rule increases device CPU utilization. Careful network traffic planning is required to efficiently use the device processor.

The ePMP platform also supports radio data rate-limiting (Maximum Information Rate, or MIR) based on the configuration of the MIR table. Operators may add up to 16 MIR profiles on the AP, each with unique limits for uplink and downlink data rates. The SM field **MIR Profile Setting** is used to configure the appropriate MIR profile for limiting the SM's data rate.

Cambium Networks ePMP 2000 | ePMP2000_d184b5 | Access Point | Administrator

Home | Quick Start | Configuration - | Radio | **Quality of Service** | System | Network | Security | Monitor - | Tools -

Configuration > Quality of Service

Maximum Information Rate (MIR)

MIR Disabled Enabled

MIR Profiles [Add](#) [Show Details](#)

Number	Description	Downlink MIR	Uplink MIR (kbps)
0	default	100000	100000

Traffic Priority

Traffic Priority Disabled Enabled

VoIP Priority Disabled Enabled

Broadcast Priority Low High

Multicast Priority Low High

QoS Classification Rules [Add](#) [Show Details](#)

Type	Details	Priority
CoS	5	Voice
DSCP	46	Voice

© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 50: AP Quality of Service page

Table 106: AP Radio Configuration attributes

Attribute	Meaning
Maximum Information Rate (MIR)	
MIR	<p>Disabled: When disabled, RF transmission is only limited by the capacity of the link (and any active QoS classification rules).</p> <p>Enabled: When enabled, all downlink and uplink traffic is limited based on the profiles configured in the MIR table.</p>
MIR Profiles	The MIR (Maximum Information Rate) table is comprised of up to sixteen profiles which, after configured, may be set on the SM to employ a certain service level or data rate.
Number	Assign a profile number to each row in the AP MIR table. This profile number is then set on each SM to limit data transfer rates based on the operator's configuration of the MIR table and its profiles.
Description	Assign a logical description for each service level. For example, a tiered service-level provider may deploy service levels "Gold", "Silver" and "Bronze" or "20 Mbps", "10 Mbps" and "5 Mbps" to offer a clear description.
Downlink MIR (kbps)	Specify the downlink rate at which the AP is allowed to transmit for this configured profile.
Uplink MIR (kbps)	Specify the uplink rate at which the AP is allowed to transmit for this configured profile.
Traffic Priority	
Traffic Priority	<p>Disabled: No traffic prioritization is performed. All traffic is treated with equal priority (low priority).</p> <p>Enabled: Traffic prioritization is enabled and specific types of traffic can be prioritized using the fields below.</p>
VoIP Priority	<p>Enabled: When enabled, two entries are automatically added to the first and second rows of the QoS Classification Rules table, one with Rule Type CoS (5) and one with Rule Type DSCP (46). The addition of these rules ensures that VoIP traffic passed over the radio downlink is given the highest priority. The CoS and DSCP values may be modified to accommodate non-standard VoIP equipment.</p> <p>Disabled: When disabled, VoIP traffic is scheduled normally along with all other user data.</p>
Broadcast Priority	<p>Low Priority: All Broadcast traffic sent over the downlink is prioritized as low priority and is delivered to the SM after scheduled high priority and VoIP traffic.</p> <p>High Priority: All Broadcast traffic sent over the downlink is prioritized as a high priority and is scheduled for delivery to SMs before low priority traffic but after VoIP traffic.</p>
Multicast Priority	Low Priority: All Multicast traffic sent over the downlink is prioritized as a low priority, and will be delivered to the SM after scheduled high priority and VoIP traffic.

Attribute	Meaning
	High Priority: All Multicast traffic sent over the downlink is prioritized as a high priority and is scheduled for delivery to SMs before low priority traffic but after VoIP traffic.
QoS Classification Rules	The QoS Classification Rules table contains all of the rules enforced by the device when passing traffic over the radio downlink. Traffic passed through the device is matched against each rule in the table; when a match is made the traffic is sent over the radio link using the priority defined in column Traffic Priority .
Type	<p>CoS: Class of Service; traffic prioritization is based on the 3-bit header present in the 802.1Q VLAN-tagged Ethernet frame header in the packet entering the AP's Ethernet port.</p> <p>VLAN ID: traffic prioritization is based on the VLAN ID of the packet entering the AP's Ethernet port.</p> <p>EtherType: traffic prioritization is based on the two-octet Ethertype field in the Ethernet frame entering the AP's Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame.</p> <p>IP: traffic prioritization is based on the source and (or) destination IP address of the packet entering the AP's Ethernet port. A subnet mask may be included to define a range of IP addresses to match.</p> <p>MAC: traffic prioritization is based on the source and (or) destination MAC address of the packet entering the AP's Ethernet port. A mask may be included to define a range of MAC addresses to match. The mask is made up of a hex representation of a series of 1s to start the mask and 0s that end the mask. A 1 may not follow a 0. Thus FF:FF:FF:FF:00:00 is allowed, but FF:00:FF:FF:FF:FF is not. The MAC address is combined with the mask to define the range of allowed MAC addresses.</p>
Details	Represents the details of the Class of Service (CoS) present in the packet entering the AP's Ethernet port.
Priority	Represents the QoS classification rule priority.

AP System page

The AP's System page is used to configure system parameters, services, time settings, SNMP, and Syslog.

Cambium Networks ePMP 2000 ePMP2000_d184b5 Access Point Administrator

Configuration > System

General

Device Name: ePMP2000_d184b5

Webpage Auto Update: 5 sec | min: 2 | max: 20

Web Access: HTTP HTTPS

HTTP Port: 80 min: 1 | max: 65535

SSH Access: Disabled Enabled

Telnet Access: Disabled Enabled

MAC-Telnet Access: Disabled Enabled

MAC-Telnet Protocol: MAC-Telnet MAC-SSH

Network Time Protocol (NTP)

IP Assignment: Static DHCP

Preferred NTP Server: []

Alternate NTP Server: []

Time Zone: (UTC) GMT - Greenwich Mean Time

Location Services

On-board GPS Latitude: 42.05337 degrees

On-board GPS Longitude: -088.02551 degrees

On-board GPS Height: 241.3 meters

Use GPS Coordinates:

Device Latitude: 12.90 degrees | min: -90 | max: 90

Device Longitude: 77.88 degrees | min: -180 | max: 180

Device Height: [] meters | min: -20000 | max: 20000

Device Location:

Simple Network Management Protocol (SNMP)

Read-Only Community String: kreddum-123_234

Read-Write Community String: kreddum-123_234

System Name: kreddum

System Description: kreddum

Traps: Disabled Enabled

Trap Community String: kreddumtrap

Trap Servers:

Server IP	Server Port
Table is empty	

System Logging (Syslog)

Server 1: []

Server 2: []

Server 3: []

Server 4: []

SysLog Mask:

Info Notices

Warnings Errors

Alerts Emergency

cnMaestro

Remote Management: Disabled Enabled

cnMaestro URL: https://qa.cloud.cambiumnetworks.com

Cambium ID: []

Onboarding Key: []

Account Management

Administrator Account: Disabled Enabled

Username: admin

Password: []

Home User Account: Disabled Enabled

Username: home

Password: []

Installer Account: Disabled Enabled

Username: installer

Password: []

Read-Only Account: Disabled Enabled


Username: readonly


Password: []


© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum





Figure 51: Figure 51 AP System page

Table 107: AP System attributes

Attribute	Meaning
General	
Device Name	Specifies the name of the AP.
Webpage Auto Update	Configure the interval for which the device retrieves system statistics for display on the management interface. For example, if this setting is configured to 5 seconds, the statistics and status parameters displayed on the management interface will be refreshed every 5 seconds (default). Webpage Auto Update is a session-only configuration change. It is updated with the <Enter> key and is not savable when using the save button.
Web Access	HTTP: Access to the device management GUI is conducted via HTTP. HTTPS: Access to the device management GUI is conducted via HTTPS.
HTTP Port	If Web Service is set to HTTP , configure the port which the device uses to service incoming HTTP requests for management GUI access.
HTTPS Port	If Web Service is set to HTTPS , configure the port which the device uses to service incoming HTTPS requests for management GUI access.
SSH Access	Disabled: If the SSH port to the device is 'Disabled', access to the device through SSH is not possible. Enabled: If the SSH port to the device is 'Enabled', Cambium engineers can access the device through SSH which enables them to log in to the radio and troubleshoot. SSH port is 'Enabled' by default.
Telnet Access	Disabled: CLI access via telnet is not allowed for the device. Enabled: CLI access via telnet is allowed for the device.
MAC-Telnet Access	Disabled: Disables connections to the radio on the link layer via MAC address from RouterOS or mactelnet-enabled devices. Enabled: Enables connections to the radio on the link layer via MAC address from RouterOS or mactelnet-enabled devices.  Note To use MAC-Telnet the first time, the Administrator account password must be changed on the GUI or the CLI. This password can then be used for MAC-Telnet.
MAC-Telnet Protocol	MAC-Telnet: Use the MAC-Telnet subservice for access MAC-SSH: Use the secured MAC-SSH sub-service for access
Network Time Protocol	
IP Assignment	Static: The device retrieves NTP time data from the servers configured in fields NTP Server IP Address . DHCP: The device retrieves NTP time data from the server IP issued via a network DHCP server.

Attribute	Meaning
Preferred NTP Server	Configure the primary NTP server IP addresses from which the device will retrieve time and date information.
Alternate NTP Server	Configure alternate or secondary NTP server IP addresses from which the device retrieves time and date information.
Time Zone	The Time Zone option may be used to offset the received NTP time to match the operator's local time zone.
Location Services	
On-board GPS Latitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Latitude information from the on-board GPS chip.
On-board GPS Longitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Longitude information from the on-board GPS chip.
On-board GPS Height	On a GPS Synchronized ePMP radio, the field is automatically populated with the Height above sea level information from the on-board GPS chip.
Use GPS Coordinates	On a GPS Synchronized ePMP radio, the Device coordinates can be populated using the information retrieved from the onboard GPS chip. Click the  button to automatically populate the Device Latitude and Device Longitude fields using the coordinates provided by the onboard GPS chip.
Device Latitude	Configure Latitude information for the device in decimal format.
Device Longitude	Configure Longitude information for the device in decimal format.
Device Height	Configure height above sea level for the device in meters.
Device Location	Hyperlink to display the device location in Google Maps
Simple Network Management Protocol (SNMP)	
Read-Only Community String	Specify a control string that can allow a Network Management Station (NMS) such as the Cambium Networks Services Server (CNSS) to read SNMP information. No spaces are allowed in this string. This password will never authenticate an SNMP user or an NMS to read/write access. The Read-only Community String value is clear text and is readable by a packet monitor.
Read-Write Community String	Specify a control string that can allow a Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string.
System Name	Specify a string to associate with the physical module. This parameter can be polled by the Cambium Networks Services Server (CNSS) or an NMS. Special characters are supported.
System Description	Specify a description string to associate with the physical module. This parameter can be polled by the Cambium Networks Services Server (CNSS) or an NMS. Special characters are supported.
Traps	Disabled: SNMP traps for system events are not sent from the device.

Attribute	Meaning
	Enabled: SNMP traps for system events are sent to the servers configured in table Trap Servers .
Trap Community String	Configure an SNMP Trap Community String which is processed by the servers configured in Trap Servers . This string is used by the trap server to decide whether or not to process the traps incoming from the device (i.e. for traps to successfully be received by the trap server, the community string must match).
Trap Servers	The Trap Servers table is used to configure trap destinations for SNMP traps generated by the device.
Server IP	Configure the IP address of each SNMP trap server target.
Server Port	Configure the port to which SNMP traps are sent from the ePMP device.
System Logging (Syslog)	
Server 1-4	Specify up to four syslog servers to which the device sends syslog messages.
SysLog Mask	Configure the levels of syslog messages which the devices send to the servers configured in parameters Server IP 1-4 . <div style="display: flex; align-items: center;">  <div style="background-color: #f4a460; padding: 5px; border: 1px solid black;"> <p>Caution</p> <p>Choose only the syslog levels appropriate for your installation. Excessive logging can cause the device log file to fill and begin overwriting previous entries.</p> </div> </div>
cnMaestro	
Remote Management	When Enabled , the device will be managed by cnMaestro - the Cambium Remote Management System, which allows all Cambium devices to be managed in the cloud.
cnMaestro URL	Configure the URL of cnMaestro. The default value is https://cloud.cambiumnetworks.com .
Cambium-ID	Configure the Cambium ID that the device will use for on-boarding on to cnMaestro.
Onboarding key	Configure the password/key associated with the Cambium-ID that the device will use for on-boarding on to cnMaestro.
Account Management	
(Administrator) Username	Read-only listing of available login levels. <ul style="list-style-type: none"> • ADMINISTRATOR, full read-write permissions. • INSTALLER, permissions to read and write parameters applicable to unit installation and monitoring. • HOME, permissions only to access pertinent information for support purposes. • READONLY has permission to only view the Monitor page.

Attribute	Meaning
(Administrator) Password	Configure a custom password for the Administrator account. The password character display may be toggled using the visibility icon  .
Installer Account	Disabled: The disabled user is not granted access to the device management interface. The administrator user level cannot be disabled. Enabled: The user is granted access to the device management interface.
(Installer) Username	Provide the 'Installer Username' in this box.
(Installer) Password	Configure a custom password to secure the device. Only the 'Administrator' account can override this password. The password character display may be toggled using the visibility icon  .
Home User Account	Disabled: The disabled user is not granted access to the device management interface. Enabled: The user is granted access to the device management interface
(Home) User Username	Provide the Home User 'Username' in this box.
(Home) User Password	Configure a custom password to secure the device to access pertinent information for support purposes only. The password character display may be toggled using the visibility icon  .
Read-Only Account	Disabled: The disabled user is not granted access to the device management interface, even on 'Read-Only' access. Enabled: The user is granted 'Read-Only' access to the device management interface.
(Read-Only) Username	Provide the Read-Only 'Username' in this box.
(Read-Only) Password	Provide the password that can be used for 'Read-Only' access. Password character display may be toggled using the visibility icon  .

AP Network page

The AP's Network page is used to configure system networking parameters and VLAN parameters.

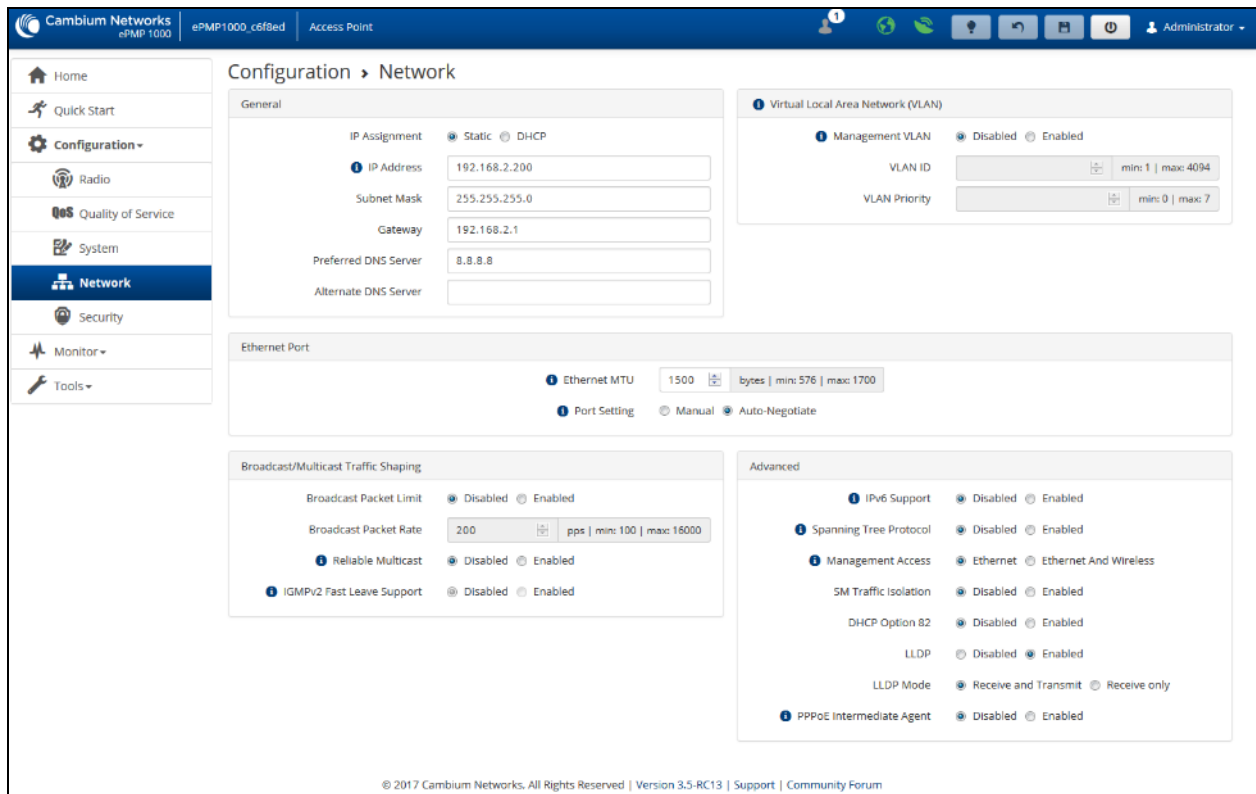




Figure 52: AP Network page

Table 108: AP Network attributes

Attribute	Meaning
General	
IP Assignment	<p>Static: Device management IP addressing is configured manually in fields Device IP Address (LAN), IP Subnet Mask (LAN), Gateway IP Address (LAN), and DNS Server IP Address (LAN).</p> <p>DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters Device IP Address (LAN), IP Subnet Mask (LAN), Gateway IP Address (LAN), and DNS Server IP Address (LAN) are unused.</p>
IP Address	<p>Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>If Device IP address Mode is set to DHCP and the device is unable to retrieve IP address information via DHCP, the device management IP is set to fallback IP 192.168.0.1 (AP mode), 192.168.0.2 (SM mode), 192.168.0.3 (Spectrum Analyzer mode), or the previously-configured static Device IP Address. Units may always be accessed via the Ethernet port with IP 169.254.1.1.</p> </div>

Attribute	Meaning
Subnet Mask	Defines the address range of the connected IP network. For example, if Device IP Address (LAN) is configured to 192.168.2.1 and IP Subnet Mask (LAN) is configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.
Gateway	Configure the IP address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Preferred DNS Server	Configure the primary IP address of the server used for DNS resolution.
Alternate DNS Server	Configure the secondary IP address of the server used for DNS resolution.
IPv6 Assignment	<p>IPv6 Assignment specifies how the IPv6 address is obtained.</p> <p>Static: Device management IP addressing is configured manually in fields IPv6 Address and IPv6 Gateway.</p> <p>DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters IPv6 Address and IPv6 Gateway are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.</p>
IPv6 Address	<p>Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.</p> <p>IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.</p>
IPv6 Gateway	Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Virtual Local Area Network (VLAN)	
Management VLAN	<p>Enabled: The AP management interface can be assigned to a Management VLAN to separate management traffic (remote module management via SNMP or HTTP) from user traffic (such as internet browsing, voice, or video). Once the management interface is enabled for a VLAN, an AP's management interface can be accessed only by packets tagged with a VLAN ID matching the management VLAN ID.</p> <p>A VLAN configuration 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 based on the VLAN architecture. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.</p> <p>Disabled: When disabled, all IP management traffic is allowed to the device.</p>
VLAN ID	Configure this parameter to include the device's management traffic on a separate VLAN network. For example, if MGMT VLAN ID is set to 2, GUI access will only be allowed from IP packets tagged with VLAN ID 2.

Attribute	Meaning
VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. MGMT VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device management traffic.</p> <p>This parameter only takes effect if the MGMT VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the management VLAN originating from the SM. The default value is 0.</p>
Ethernet MTU	<p>Maximum Transmission Unit: the size in bytes of the largest data unit that the device is configured to process. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error. Packets received by the device larger than the configured MTU are dropped.</p>
Port Setting	<p>Manual: The LAN Ethernet port speed and duplex mode can be manually configured.</p> <p>Auto-Negotiate: The AP auto negotiates the LAN Ethernet port speed and duplex mode with the device connected to it.</p>
Port Speed	<p>With “Ethernet Port Configuration” the LAN Ethernet port speed can be forced to 1000 Mbps, 100 Mbps, or 10 Mbps.</p>
Port Duplex Mode	<p>With “Ethernet Port Configuration” the LAN Ethernet port duplex mode can be forced into Full or Half.</p>
Broadcast/Multicast Traffic Shaping	
Broadcast Packet Limit	<p>Enabled: This allows the user to set the Broadcast Packet Rate below. Configure this parameter to limit the number of broadcast packets that will be allowed on the ingress of the radio’s Ethernet port. Set the packets per second value to limit the impact of events such as broadcast storms.</p> <p>Disabled: There is no limit on the amount of broadcast traffic that will be allowed into the ingress of the radio’s Ethernet port.</p>
Broadcast Packet Rate	<p>Set the packets per second value to limit the amount of broadcast traffic that will be allowed on the ingress on the radio’s Ethernet port. The packets per second limit can be set individually on each ePMP radio. The range is 100 to 16000 packets per second. The default is 200.</p>
Reliable Multicast	<p>Enabled: This feature allows ePMP to support IGMP capable devices. Once a multicast group is identified, the AP allows multicast traffic to be sent only to the SMs within the multicast group. The SMs support up to 5 unique multicast groups. Also, when this option is enabled, the multicast traffic is sent to the SMs using the current Downlink MCS rate.</p> <p>Disabled: ePMP will still support IGMP capable devices but the multicast traffic will be sent using MCS 1 on the downlink to all SMs, regardless of the multicast group.</p>
IGMPv2 Fast Leave Support	<p>Disabled: AP will not drop any IGMPv2 Leave packets</p> <p>Enabled: AP will drop/ignore IGMPv2 Leave packets from SMs if there are other SMs downstream still subscribed to the IGMP group.</p>

Attribute	Meaning
Advanced	
IPv6 Support	Systemwide IPv6 Protocol Support. When enabled, appropriate IPv6 modules and services will be loaded.
Spanning Tree Protocol	<p>Disabled: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the AP.</p> <p>Enabled: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the AP, allowing for the prevention of Ethernet bridge loops.</p>
Management Access	<p>Ethernet: Only allow access to the AP's web management interface via a local Ethernet (LAN) connection. In this configuration, the AP's web management interface may not be accessed from over the air (i.e. from a device situated below the SM).</p> <p>Ethernet and Wireless: Allow access to the AP's web management interface via a local Ethernet (LAN) connection and from over the air (i.e. from a device situated below the SM).</p> <div data-bbox="418 814 487 903" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="553 814 1419 940" style="border: 1px solid black; background-color: #f4a460; padding: 5px; margin-top: 10px;"> <p>Caution</p> <p>APs configured with AP Management Access Interface set to LAN and WLAN are susceptible to unauthorized access.</p> </div>
SM Traffic Isolation	<p>Disabled: This is the default mode. When SM isolation is disabled, an SM can communicate with another SM, when both the SM's are associated with the same Access Point (AP).</p> <p>Enabled: When the SM Isolation feature is "Enabled", SM#1 will not be able to communicate with SM#2 (peer-to-peer traffic) when both the SM's are associated with the same Access Point (AP). This feature essentially enables the AP to drop the packets to avoid peer-to-peer traffic scenarios.</p>
DHCP Option 82	<p>Disabled: When 'Disabled', ePMP does not insert the "remote-id" (option ID 0x2) and the "circuit-id" (ID 0x01). DHCP Option 82 is 'Disabled' by default.</p> <p>Enabled: ePMP inserts "remote-id" (option ID 0x2) to be the SM's MAC address and the "circuit-id" (ID 0x01) to be the AP's MAC address. Those two fields are used to identify the remote device and connection from which the DHCP request was received.</p>
LLDP	<p>The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol (as specified in IEEE 802.1AB) used by ePMP for advertising its identity, capabilities, and neighbors on the Ethernet/wired interface.</p> <p>Disabled: ePMP does not Receive or Transmit LLDP packets from/to its neighbors.</p> <p>Enabled: ePMP can Receive LLDP packets from its neighbors and Send LLDP packets to its neighbors, depending on the LLDP Mode configuration below.</p> <div data-bbox="418 1707 487 1785" style="display: inline-block; vertical-align: middle;">  </div> <div data-bbox="553 1701 1419 1816" style="border: 1px solid black; background-color: #a4c6e0; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>LLDP packets are Received/Transmitted ONLY to the neighbors on the Ethernet Interface of the ePMP radio.</p> </div>

Attribute	Meaning
LLDP Mode	<p>Receive and Transmit: ePMP sends and receives LLDP packets to/from its neighbors on the Ethernet/LAN interface.</p> <p>Receive Only: ePMP receives LLDP packets from its neighbors on the Ethernet/LAN interface and discovers them.</p>
PPPoE Intermediate Agent	<p>When enabled, during the PPPoE Discovery phase the AP inserts access loop identification into the PPPoE PADR packets. This mechanism helps the service provider to distinguish between end hosts connected via Ethernet as an access device (typically, home routers situated below an ePMP subscriber device).</p> <p>On the AP, PPPoE Intermediate Agent enables subscriber line identification by tagging Ethernet frames of corresponding users with Vendor-Specific PPPoE Tags “Circuit ID” (defining AP name, frame, slot, port, and VLAN ID information) and “Remote ID” (defining user phone number).</p>

AP Security page

The AP's **Security** page is used to configure system security features including SM authentication and Layer2/Layer3 Firewall rules.



Caution

If a device firewall rule is added with **Action** set to **Deny** and **Interface** set to **LAN** or **WAN** and no other rule attribute are configured, the device will drop all Ethernet or wireless traffic, respectively. Ensure that all firewall rules are specific to the type of traffic which must be denied and that no rules exist in the devices with the only **Action** set to **Deny** and **Interface** set to **LAN** or **WAN**. To regain access to the device, perform a factory default.

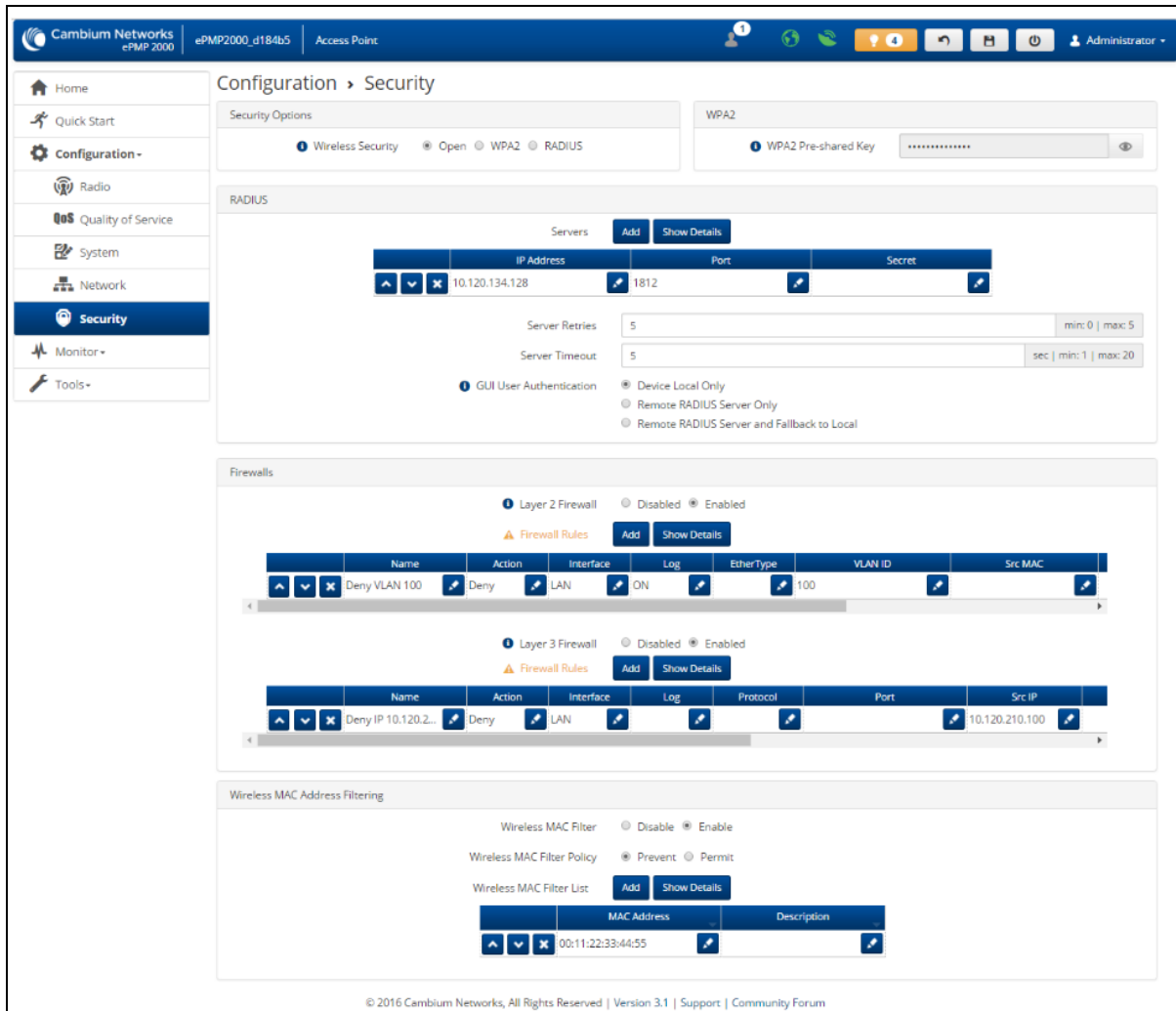


Figure 53: AP Security page

Table 109: AP Security attributes

Attribute	Meaning
Security Options	
Wireless Security	<p>Open: All SMs requesting network entry are allowed registration.</p> <p>WPA2: The WPA2 mechanism provides AES radio link encryption and SM network entry authentication. When enabled, the SM must register using the Authentication Pre-shared Key configured on the AP and SM.</p> <p>RADIUS: Enables the connection to a pre-configured RADIUS server.</p>
WPA2	
WPA2 Pre-shared Key	Configure this key on the AP. Then configure each of the network SMs with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.

Attribute	Meaning
RADIUS	
Servers	<p>For more Radio servers, click Add. Up to 3 Radius servers can be configured on the device with the following attributes:</p> <p>IP Address: IP Address of the Radius server on the network.</p> <p>Port: The Radius server port. Default is 1812.</p> <p>Secret: Secret key that is used to communicate with the Radius server.</p>
Server Retries	The number of times the radio will retry authentication with the configured Radius server before it fails authentication of the SM.
Server Timeout	Timeout between each retry with the configured Radius server before it fails authentication of the SM.
GUI User Authentication	<p>This applies to both the AP and its registered SMs.</p> <p>Device Local Only: The device's GUI authentication is local to the device using one of the accounts configured under Configuration > System > Account Management.</p> <p>Remote RADIUS Server Only: The device's GUI authentication is performed using a RADIUS server.</p> <p>Remote RADIUS Server and Fallback to Local: The device's GUI authentication is performed using a RADIUS server. Upon failure of authentication through a RADIUS server, the authentication falls back to one of the local accounts configured under Configuration->System->Account Management.</p>
Firewalls	
Layer 2 Firewall	<p>Disabled: Modifications to the Layer 2 Firewall Table are not allowed and rules are not enforced.</p> <p>Enabled: Modifications to the Layer 2 Firewall Table are allowed and rules are enforced.</p>
Firewall Rules	The Layer 2 firewall table may be used to configure rules matching layer 2 (MAC layer) traffic which results in forwarding or dropping the traffic over the radio link or Ethernet interface.
Layer 3 Firewall	<p>Disabled: Modifications to the Layer 3 Firewall Table are not allowed and rules are not enforced.</p> <p>Enabled: Modifications to the Layer 3 Firewall Table are allowed and rules are enforced.</p>
Firewall Rules	The Layer 3 firewall table may be used to configure rules matching layer 3 (IP layer) traffic which results in forwarding or dropping the traffic over the radio link or Ethernet interface.
Wireless MAC Address Filtering	
Wireless MAC Filter	<p>Disabled: SMs with any MAC Address are allowed to register to the AP.</p> <p>Enabled: SMs with specific MAC addresses can be allowed (Permit) or denied (Prevent) registration with the AP as configured under the MAC Filter List.</p>

Attribute	Meaning
Wireless MAC Filter Policy	<p>Prevent: All MAC Addresses configured under the MAC Filter List are denied registration to the AP.</p> <p>Permit: Only the MAC Addresses configured under the MAC Filter List are allowed to register to the AP.</p>
Wireless MAC Filter List	Configure the SM's MAC addresses that will be permitted or prevented from registering to the AP.
MAC Address	MAC Address of the SM
Description	Friendly description to identify the SM

AP Monitor menu

Use the **Monitor** menu to access device and network statistics and status information. This section may be used to analyze and troubleshoot network performance and operation.

The **Monitor** menu contains the following pages:

- [AP Performance page](#)
- [AP System page](#)
- [AP Wireless page](#)
- [AP Throughput Chart page](#)
- [AP GPS page](#)
- [AP Network page](#)
- [AP System Log page](#)

AP Performance page

Use the **Performance** page to monitor system status and statistics to analyze and troubleshoot network performance and operation.

Cambridge Networks
eMMP 1000 - r100d Access Point

Home
Quick Start
Configuration+
Monitor-
Performance
System
Wireless
Throughput Chart
GPS
Network
System Log
Tools-

Monitor > Performance

Reset Statistics
Time Since Last Reset: 0000:00:00:23
Reset Stats

Ethernet Statistics - Transmitted

- Total Traffic: 1586 Kbits
- Total Packets: 274
- Packet Errors: 0
- Packet Drops: 0
- Multicast / Broadcast Traffic: 149 Kbits
- Broadcast Packets: 55
- Multicast Packets: 11

Ethernet Statistics - Received

- Total Traffic: 901 Kbits
- Total Packets: 591
- Packet Errors: 0
- Packet Drops: 0
- Multicast / Broadcast Traffic: 693 Kbits
- Broadcast Packets: 227
- Multicast Packets: 222

Wireless Statistics - Downlink

- Total Traffic: 21 Kbits
- Total Packets: 16
- Error Drop Packets: 0
- Capacity Drop Packets: 0
- Retransmission Packets: 0
- Multicast / Broadcast Traffic: 9 Kbit

Wireless Statistics - Uplink

- Total Traffic: 2 Kbits
- Total Packets: 4
- Error Drop Packets: 0
- Multicast / Broadcast Traffic: 0 Kbits
- Broadcast Packets: 1
- Multicast Packets: 0

QoS Statistics

TDD Voice Priority queue

- Total count of transmitted packets: 0
- Total count of received packets: 0
- Total count of dropped packets: 0

TDD Low Priority queue

- Total count of transmitted packets: 2
- Total count of received packets: 2
- Total count of dropped packets: 0

TDD High Priority queue

- Total count of transmitted packets: 105
- Total count of received packets: 105
- Total count of dropped packets: 0

TDD QoS queues

- Total count of transmitted packets: 108
- Total count of received packets: 108
- Total count of dropped packets: 0

System Statistics

- Session Drops: 0
- Device Reboots: 2
- Network Entry Attempts: 1
- Successful Network Entries: 1
- Network Entry Authentication Failures: 0

Subscriber Module Statistics

Subscriber Module Statistics [Show Details](#)

MAC Address	Total Uplink (Kbits)	Total Uplink Packets	Uplink Packet Drops	Total Downlink (Kbits)	Total Downlink Packets	Downlink Packet Drops	Downlink Capacity Packet Drops	Downlink Retransmitted Packets	Downlink Power (dBm)
00:04:5b:05:64:8a	10	20	0	2	2	0	0	0	7

Downlink Packets Per MCS

MCS 15 - 64-QAM 5/6	0 (0%)
MCS 14 - 64-QAM 3/4	0 (0%)
MCS 13 - 64-QAM 2/3	0 (0%)
MCS 12 - 16-QAM 3/4	0 (0%)
MCS 11 - 16-QAM 1/2	0 (0%)
MCS 10 - QPSK 3/4	0 (0%)
MCS 9 - QPSK 1/2	0 (0%)
MCS 7 - 64-QAM 5/6	0 (0%)
MCS 6 - 64-QAM 3/4	0 (0%)
MCS 5 - 64-QAM 2/3	0 (0%)
MCS 4 - 16-QAM 3/4	0 (0%)
MCS 3 - 16-QAM 1/2	0 (0%)
MCS 2 - QPSK 3/4	1 (0.5%)
MCS 1 - QPSK 1/2	186 (99.5%)

Uplink Packets Per MCS

MCS 15 - 64-QAM 5/6	0 (0%)
MCS 14 - 64-QAM 3/4	0 (0%)
MCS 13 - 64-QAM 2/3	0 (0%)
MCS 12 - 16-QAM 3/4	0 (0%)
MCS 11 - 16-QAM 1/2	0 (0%)
MCS 10 - QPSK 3/4	0 (0%)
MCS 9 - QPSK 1/2	14 (29.2%)
MCS 7 - 64-QAM 5/6	0 (0%)
MCS 6 - 64-QAM 3/4	0 (0%)
MCS 5 - 64-QAM 2/3	0 (0%)
MCS 4 - 16-QAM 3/4	0 (0%)
MCS 3 - 16-QAM 1/2	1 (2.1%)
MCS 2 - QPSK 3/4	11 (22.9%)
MCS 1 - QPSK 1/2	22 (45.8%)

Downlink Frame Time

- Total Frame Time Used: 4.4%

© 2017 Cambridge Networks, All Rights Reserved | Version 3.4-RC20 | Support | Community Forum

Figure 54: AP Performance page

Table 110: AP Performance page attributes

Attribute	Meaning
Time Since Last Reset	Time since the stats were last reset.
Ethernet Statistics - Transmitted	
Total Traffic	Total amount of traffic in Kbits transferred from the AP's Ethernet interface.
Total Packets	Total number of packets transferred from the AP's Ethernet interface.
Packet Errors	Total number of packets transmitted out of the AP's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	Total number of packets dropped prior to sending out of the AP's Ethernet interface due to Ethernet setup or filtering issues.
Multicast/Broadcast Traffic	Total amount of multicast and broadcast traffic in Kbits sent via the AP's Ethernet interface.
Broadcast Packets	Total number of broadcast packets sent via the AP's Ethernet interface.
Multicast Packets	Total number of multicast packets sent via the AP's Ethernet interface.
Ethernet Statistics - Received	
Total Traffic	Total amount of traffic in Kbits received by the AP's Ethernet interface.
Total Packets	Total number of packets received by the AP's Ethernet interface.
Packet Errors	Total number of packets received by the AP's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	Total number of packets dropped before sending out of the AP's wireless interface due to Ethernet setup or filtering issues.
Multicast/Broadcast Traffic	Total amount of multicast and broadcast traffic in Kbits received by the AP's Ethernet interface.
Broadcast Packets	Total number of broadcast packets received via the AP's Ethernet interface.
Multicast Packets	Total number of multicast packets received via the AP's Ethernet interface.
Wireless Statistics - Downlink	
Total Traffic	Total amount of traffic transmitted out of the AP's wireless interface in Kbits.
Total Packets	Total number of packets transmitted out of the AP's wireless interface.
Error Drop Packets	Total number of packets dropped after transmitting out of the AP's Wireless interface due to RF errors (No acknowledgment and other RF-related packet error).

Attribute	Meaning
Capacity Drop Packets	Total number of packets dropped after transmitting out of the AP's Wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).
Retransmission Packets	Total number of packets re-transmitted after transmitting out of the AP's Wireless interface due to the packets not being received by SMs.
Multicast / Broadcast Traffic	Total amount of multicast and broadcast traffic transmitted out of the AP's wireless interface in Kbits.
Broadcast Packets	Total number of broadcast packets transmitted out of the AP's wireless interface.
Multicast Packets	Total number of multicast packets transmitted out of the AP's wireless interface.
Wireless Statistics - Uplink	
Total Traffic	Total amount of traffic received via the AP's wireless interface in Kbits.
Total Packets	Total number of packets received via the AP's wireless interface.
Error Drop Packets	Total number of packets dropped before sending out of the AP's Ethernet interface due to RF errors (packet integrity error and other RF-related packet error).
Multicast / Broadcast Traffic	Total amount of multicast and broadcast traffic received on the AP's wireless interface in Kbits.
Broadcast packets	Total number of broadcast packets received on the AP's wireless interface.
Multicast Packets	Total number of multicast packets received on the AP's wireless interface.
QoS Statistics	
TDD Voice Priority Queue	
Total count of transmitted packets	Total count of put packets to Voice queue
Total count of received packets	Total count of get packets from Voice queue
Total count of dropped packets	Total count of dropped packets from Voice queue
TDD High Priority Queue	
Total count of transmitted packets	Total count of put packets to High queue

Attribute	Meaning
Total count of received packets	Total count of get packets from High queue
Total count of dropped packets	Total count of dropped packets from High queue
TDD Low Priority Queue	
Total count of transmitted packets	Total count of put packets to Low queue
Total count of received packets	Total count of get packets from Low queue
Total count of dropped packets	Total count of dropped packets from Low queue
TDD QoS queues	
Total count of transmitted packets	Total count of put packets to all queues
Total count of received packets	Total count of get packets from all queues
Total count of dropped packets	Total count of dropped packets from all queues
System Statistics	
Session Drops	Total number of SM sessions dropped on the AP.
Device Reboots	Total number of reboots of the AP.
Network Entry Attempts	Total number of Network Entry Attempts by all the SMs on the AP.
Successful Network Attempts	Total number of successful network entry attempts.
Network Entry Authentication Failures	Total number of failed Network Entry Attempts by all the SMs on the AP.
Radar (DFS) Detections	Total number of DFS events that were detected by the AP.
Subscriber Module Statistics	
MAC Address	MAC Address of the SM connected to the AP.
Total Uplink	Total amount of traffic received via the AP's wireless interface from this SM in Kbits.
Total Uplink Packets	Total number of packets received via the AP's wireless interface from this SM.

Attribute	Meaning
Uplink Packet Drops	Total number of packets dropped before sending out of the AP's Ethernet interface due to RF errors (packet integrity error and other RF-related packet error) from this SM.
Total Downlink	Total amount of traffic transmitted out of the AP's wireless interface in Kbits.
Total Downlink Packets	Total number of packets transmitted out of the AP's wireless interface.
Downlink Packet Drops	Total number of packets dropped after transmitting out of the AP's Wireless interface due to RF errors (No acknowledgment and other RF-related packet error).
Downlink Capacity Packet Drops	Total number of packets dropped after transmitting out of the AP's Wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).
Downlink Retransmitted Packets	Total number of packets re-transmitted after transmitting out of the AP's Wireless interface due to the packets not being received by the SM.
Downlink Power	The transmit power of the AP for the downlink packets to the SM.
Downlink Packets per MCS	
MCS 0 through MCS 15	Number of packets (and percentage of total packets) transmitted out of the AP's wireless interface for every modulation mode used by the AP's transmitter, based on radio conditions.
Uplink Packets per MCS	
MCS 0 through MCS 15	Number of packets (and percentage of total packets) received on the AP's wireless interface for every modulation mode, based on radio conditions.
Downlink Frame Time	
Total Frame Time Used	Percentage of frame time used in the downlink.
Uplink Frame Time	
Total Frame Time Used	Percentage of frame time used in the uplink.

AP System page

Use the **System Status** page to reference key system information.

Cambium Networks ePMP 2000 ePMP2000_d184b5 Access Point Administrator

Monitor > System

Hardware Version	ePMP 2000
Serial number (MSN)	E6RM001MBJFW
Firmware Version	U-Boot 9557_PX 1.1.4.c (Nov 3 2016 - 16:29:29)
Software Version	3.1
Software Version (Active Bank)	3.1
Software Version (Inactive Bank)	3.0.1
Device-Agent Version	2.53
Date and Time	15 Nov 2016, 16:28:41 GMT
System Uptime	6 minutes, 55 seconds
Wireless MAC Address	00:04:56:D1:84:B6
Ethernet MAC Address	00:04:56:D1:84:B5
DFS Status	Not Available
Sync Source Status	GPS Sync Up
Contains FCC ID(s):	N/A
Read-Only Users	0
Read-Write Users	1
Factory Reset Via Power Sequence	Disabled
cnMaestro Connection Status	Connected to qa.cloud.cambiumnetworks.com
cnMaestro Account ID	KREDDUM_CNSNGQA

© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 55: AP System Status page

Table 111: AP System Status page attributes

Attribute	Meaning
Hardware Version	Board hardware version information.
Serial Number (MSN)	Serial Number information.
Firmware Version	U-Boot version information.
Software Version (Active Bank)	The currently operating version of software on the ePMP device.
Software Version (Inactive Bank)	The backup software version on the ePMP device was used upon failure of the active bank. Two software upgrades in sequence will update both the Active Software Bank Version and the Inactive Software Bank Version .
Device-Agent Version	The operating version of the device agent, which is used for communication with cnMaestro.
Date and Time	Current date and time, subject to time zone offset introduced by the configuration of the device Time Zone parameter. Until a valid NTP server is configured, this field will display the time configured from the factory.
System Uptime	The total system uptime since the last device reset.
Wireless MAC Address	The hardware address of the device's wireless interface.
Ethernet MAC Address	The hardware address of the device LAN (Ethernet) interface.
DFS Status	<p>N/A: DFS operation is not required for the region configured in parameter Country Code.</p> <p>Channel Availability Check: Before transmitting, the device must check the configured Frequency Carrier for radar pulses for 60 seconds). If no radar pulses are detected, the device transitions to state In-Service Monitoring.</p> <p>In-Service Monitoring: Radio is transmitting and receiving normally while monitoring for radar pulses that require a channel move.</p> <p>Radar Signal Detected: The receiver has detected a valid radar pulse and is carrying out detect-and-avoid mechanisms (moving to an alternate channel).</p> <p>In-Service Monitoring at Alternative Channel: The radio has detected a radar pulse and has moved the operation to a frequency configured in DFS Alternative Frequency Carrier 1 or DFS Alternative Frequency Carrier 2.</p> <p>System Not In Service due to DFS: The radio has detected a radar pulse and has failed channel availability checks on all alternative frequencies. The non-occupancy time for the radio frequencies in which radar was detected is 30 minutes.</p>
Sync Source Status	Displays the current source (GPS, CMM, or Internal) of sync timing for the AP.
Read-Only Users	Displays the number of active Read-Only users logged into the radio.

Attribute	Meaning
Read-Write Users	Displays the number of active Read-Write users logged into the radio.
Factory Reset Via Power Sequence	<p>Enabled: When Enabled under Tools > Backup/Restore > Reset Via Power Sequence, it is possible to reset the radio's configuration to factory defaults using the power cycle sequence explained under Resetting ePMP to factory defaults by power cycling.</p> <p>Disabled: When Disabled, it is not possible to factory default the radio's configuration using the power cycle sequence.</p>
cnMaestro Connection Status	The current management status of the device concerning the Cambium Cloud Server. When Enabled under Configuration > System , the device will be managed by the Cambium Remote Management System, which allows all Cambium devices to be managed from the Cambium Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Cloud Server.

AP Wireless page

Use the **Wireless** Status page to reference key information about the radio's wireless interface and connected SMs.

The screenshot shows the Cambium Networks ePMP 2000 interface. The top navigation bar includes the logo, device ID (ePMP2000_d1f2df), and the role (Access Point). The sidebar on the left has a 'Wireless' section highlighted. The main content area shows the following wireless status information:

- Operating Frequency: 5550 MHz
- Operating Channel Bandwidth: 40 MHz
- Transmitter Output Power: 0 dBm
- Device Initialization Status: Successful
- Registered Subscriber Modules: 19
- Ethernet Status: 1000 Mbps / Full
- Wireless Status: Up
- Country: Other

Below this summary is a table titled 'Registered Subscriber Modules' with a 'Show Detail' button. The table lists 19 subscriber modules with the following columns: Address, IP Address, Device Name, SM Distance (miles), Session Time (hh:mm:ss), RSSI (dBm) Downlink / Uplink, SNR (dB) Downlink / Uplink, MCS Downlink / Uplink, Downlink Quality, Downlink Capacity, MRR Profile, MRR Rate (kbps) Downlink / Uplink, and Antenna Selected.

Address	IP Address	Device Name	SM Distance (miles)	Session Time (hh:mm:ss)	RSSI (dBm) Downlink / Uplink	SNR (dB) Downlink / Uplink	MCS Downlink / Uplink	Downlink Quality	Downlink Capacity	MRR Profile	MRR Rate (kbps) Downlink / Uplink	Antenna Selected
00:0A:D9	10.120.224.107	ePMP1000_c00ad8	0	00:55:44	-45 / -72	45 / 26	15 / 15	100%	100%	0	10000 / 10000	V-4*H-6*
00:0E:3F	10.120.224.110	ePMP1000_c00e3e	0	00:55:41	-31 / -60	59 / 36	15 / 15	100%	100%	0	10000 / 10000	V-4*H-6*
00:0E:0F	10.120.224.115	ePMP1000_c00e0e	0	00:55:37	-43 / -69	47 / 26	7 / 15	100%	40%	0	10000 / 10000	V-3*H-3*
00:0B:63	10.120.224.112	ePMP1000_c00b62	0	00:55:36	-50 / -72	40 / 24	15 / 15	100%	100%	0	10000 / 10000	V-4*H-3*
00:0E:4E	10.120.224.114	ePMP1000_c00e4d	0	00:55:35	-29 / -57	61 / 39	15 / 15	100%	100%	0	10000 / 10000	Sector
00:0B:CC	10.120.224.111	ePMP1000_c00bcb	0	00:55:33	-45 / -72	45 / 25	7 / 15	100%	40%	0	10000 / 10000	V-4*H-6*
00:0A:EE	10.120.224.117	ePMP1000_c00aed	0.093	00:55:25	-28 / -54	82 / 41	7 / 15	100%	40%	0	10000 / 10000	Sector
00:0D:F1	10.120.224.113	ePMP1000_c00df0	0	00:55:22	-28 / -54	82 / 42	7 / 15	100%	40%	0	10000 / 10000	Sector
00:0E:5D	10.120.224.109	ePMP1000_c00e5c	0	00:55:20	-27 / -53	83 / 43	15 / 15	100%	100%	0	10000 / 10000	V-4*H-6*
00:0E:66	10.120.224.108	ePMP1000_c00e65	0	00:55:19	-45 / -72	45 / 25	15 / 14	100%	100%	0	10000 / 10000	V-4*H-6*

Figure 56: AP Wireless Status page (ePMP 2000 – List View)

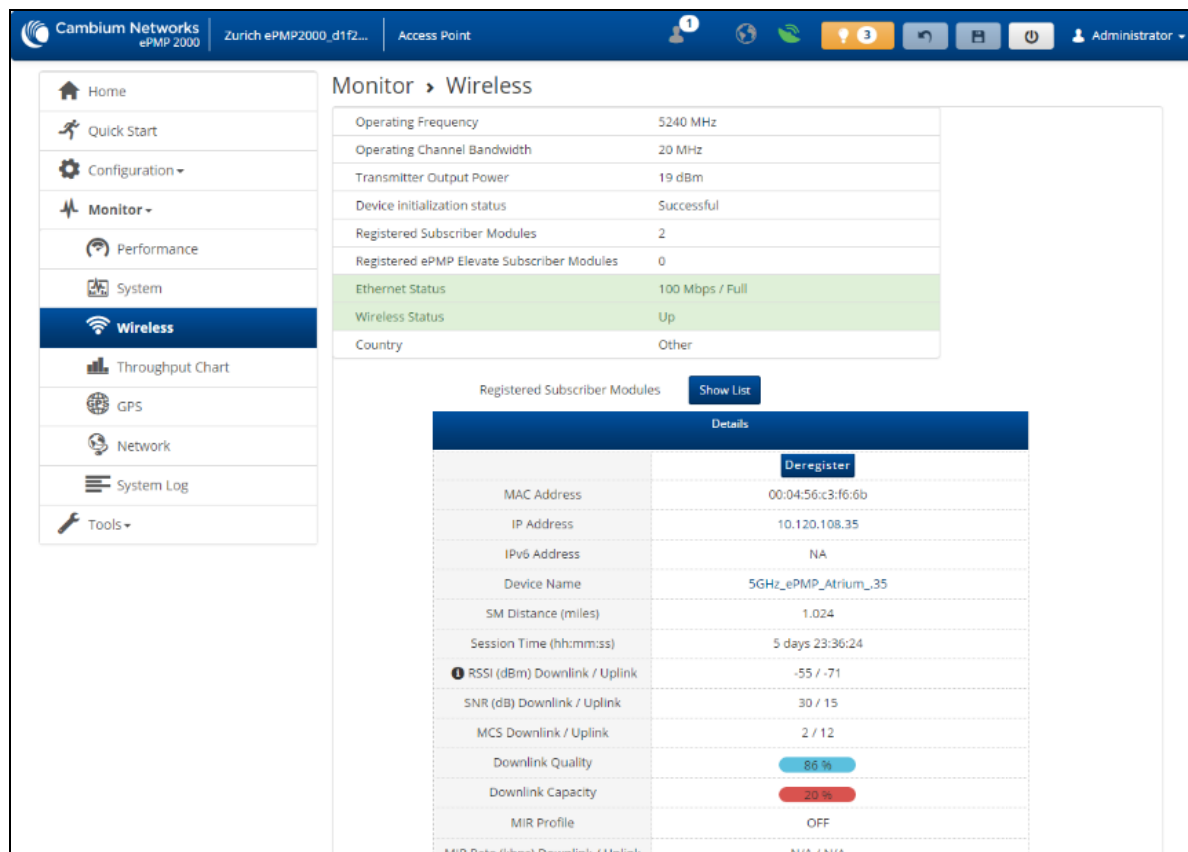



Figure 57: AP Wireless Status page (ePMP 1000 – Detail View)

Table 112: AP Wireless Status page attributes

Attribute	Meaning
Operating Frequency	The current frequency at which the AP is operating.
Operating Channel Bandwidth	The current channel size at which the AP is transmitting and receiving.
Transmitter Output Power	The current power level at which the AP is transmitting.
Device Initialization Status	This field indicates the status of the device initialization. Values are Successful and Error code for a fail case. Please pay attention that in fail case the device cannot be used in operating mode due to a major hardware problem.
Registered Subscriber Modules	The total number of SMs that are currently registered to the AP.

Attribute	Meaning
Ethernet Interface	Up: The Ethernet (LAN) interface is functioning properly. Down: The Ethernet (LAN) interface has encountered an error and is not servicing traffic.
Wireless Interface	Up: The radio (WAN) interface is functioning properly. Down: The radio (WAN) interface has encountered an error and is not servicing traffic.
Country	The current country code at which the AP is operating.
Registered Subscriber Modules	Use the Registered Subscriber Modules table to monitor registered SMs, their key RF status, and statistics information.
	Clicking this button deregisters the SM from the AP
MAC Address	The MAC address of the SM wireless interface.
IP Address	The IPv4 address of the SM wireless interface.
IPv6 Address	The IPv6 address of the SM wireless interface.
Device Name	Device Name of the SM
SM Distance (miles)	Distance of the SM from the AP
Session Time	Time duration for which the SM has been registered and in session with the AP.
RSSI (dBm) Downlink / Uplink	Current receive signal strength of the AP at the SM, in the downlink and the current receive signal strength of the SM at the AP, in the uplink. The downlink RSSI is an estimation. For accurate downlink RSSI, please refer to the SM's Dashboard page.
SNR (dB) Downlink / Uplink	Current Signal-to-Noise of the SM in the downlink and uplink
MCS Downlink / Uplink	Current MCS at which the SM is operating on the downlink and uplink
Downlink Quality	The downlink quality based on the current MCS and PER (Packet Error Rate) for this SM
Downlink Capacity	The downlink capacity is based on the current DL MCS concerning the highest supported MCS (MCS15). Not available in ePTP Master mode.
MIR Profile	Current MIR profile assigned to this SM "SERVER" indicates that the MIR values are assigned by the RADIUS server
MIR Rate (kbps) Downlink / Uplink	Current downlink and uplink MIR assigned to this SM in kbps

Attribute	Meaning
Antenna Selected	<p>Indicates the antenna for which uplink communication is conducted, Sector or Smart Antenna.</p> <p>V -4° H 3°</p> <p>When Smart Antenna is displayed, an indicator of the angle (in degrees) of the antenna pattern is also displayed. The V value represents vertical polarity and the H value represents horizontal polarity, both relative to boresight.</p>

AP Throughput Chart page

Use the Throughput page to reference a line chart visual representation of system throughput over time. The blue line indicates downlink throughput and the orange line indicates uplink throughput. The X-axis may be configured to display data over seconds, minutes, or hours, and the Y-axis is adjusted automatically based on average throughput. Hover over data points to display details.

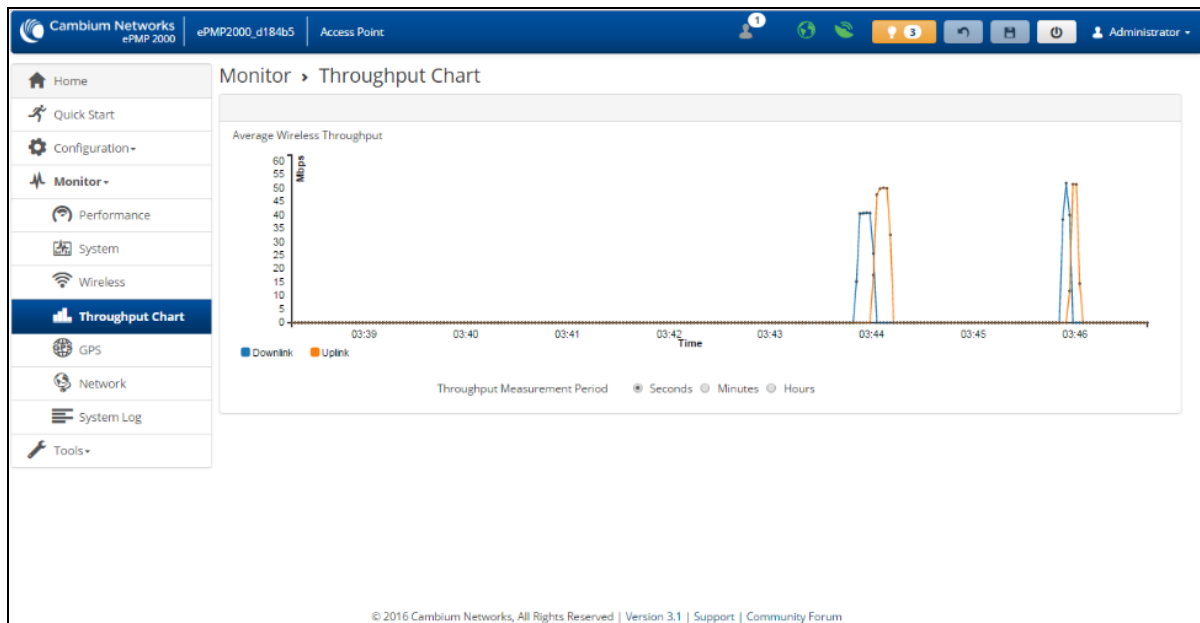


Figure 58: AP Throughput Chart page

Table 113: AP Throughput Chart page attributes

Attribute	Meaning
Throughput Measurement Period	Adjust the X-axis to display throughput intervals in seconds, minutes, or hours.

AP GPS page

Use the GPS Status page to reference key information about the radio's configured GPS coordinates.

The screenshot shows the 'Monitor > GPS Status' page. The top navigation bar includes 'Cambium Networks ePMP 2000', 'ePMP2000_d184b5', 'Access Point', and 'Administrator'. The left sidebar contains navigation options: Home, Quick Start, Configuration, Monitor (selected), Performance, System, Wireless, Throughput Chart, GPS, Network, System Log, and Tools. The main content area displays the following GPS status information:

On-board GPS Latitude	42.05337 degrees
On-board GPS Longitude	-088.02551 degrees
On-board GPS Height	241.3 meters
GPS Time (Greenwich Mean Time)	16:40:21
GPS Firmware Version	AXN_3.20_8174
Satellites Tracked	10
Satellites Visible	18

Below this summary is a 'Satellites' section with a 'Show Details' button and a table listing tracked and visible satellites:

ID	Signal-to-Noise Ratio	Status
5	44	Tracked
18	38	Tracked
13	42	Tracked
2	41	Tracked
15	42	Tracked
25	37	Tracked
29	40	Tracked
20	38	Tracked
21	45	Tracked
26	40	Tracked
51	38	Visible
65	0	Visible
88	0	Visible
87	16	Visible
72	22	Visible
66	0	Visible
81	16	Visible
80	0	Visible

© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 59: AP GPS Status page

Table 114: AP GPS Status page attributes

Attribute	Meaning
On-board GPS Latitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Latitude information from the on-board GPS chip.
On-board GPS Longitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Longitude information from the on-board GPS chip.
On-board GPS Height	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device height above sea level from the onboard GPS chip.

Attribute	Meaning
GPS Time (Greenwich Mean Time)	On a GPS Synchronized ePMP radio, the field is automatically populated with the time from the onboard GPS chip.
GPS Firmware version	On a GPS Synchronized ePMP radio, the field indicates the current firmware version of the onboard GPS chip.
Satellites Tracked	On a GPS Synchronized ePMP radio, the field indicates the number of satellites current tracked by the onboard GPS chip.
Satellites Visible	On a GPS Synchronized ePMP radio, the field indicates the number of satellites visible to the on-board GPS chip.
Satellites	The Satellites table provides information about each satellite that is visible or tracked along with the Satellite ID and Signal to Noise Ratio (SNR) of the satellite.
ID	Represents the Satellite ID.
Signal-to-Noise Ratio	This is an expression of the carrier signal quality concerning signal noise.
Status	Status of each Satellite available.

AP Network page

Use the AP Network Status page to reference key information about the device network status.

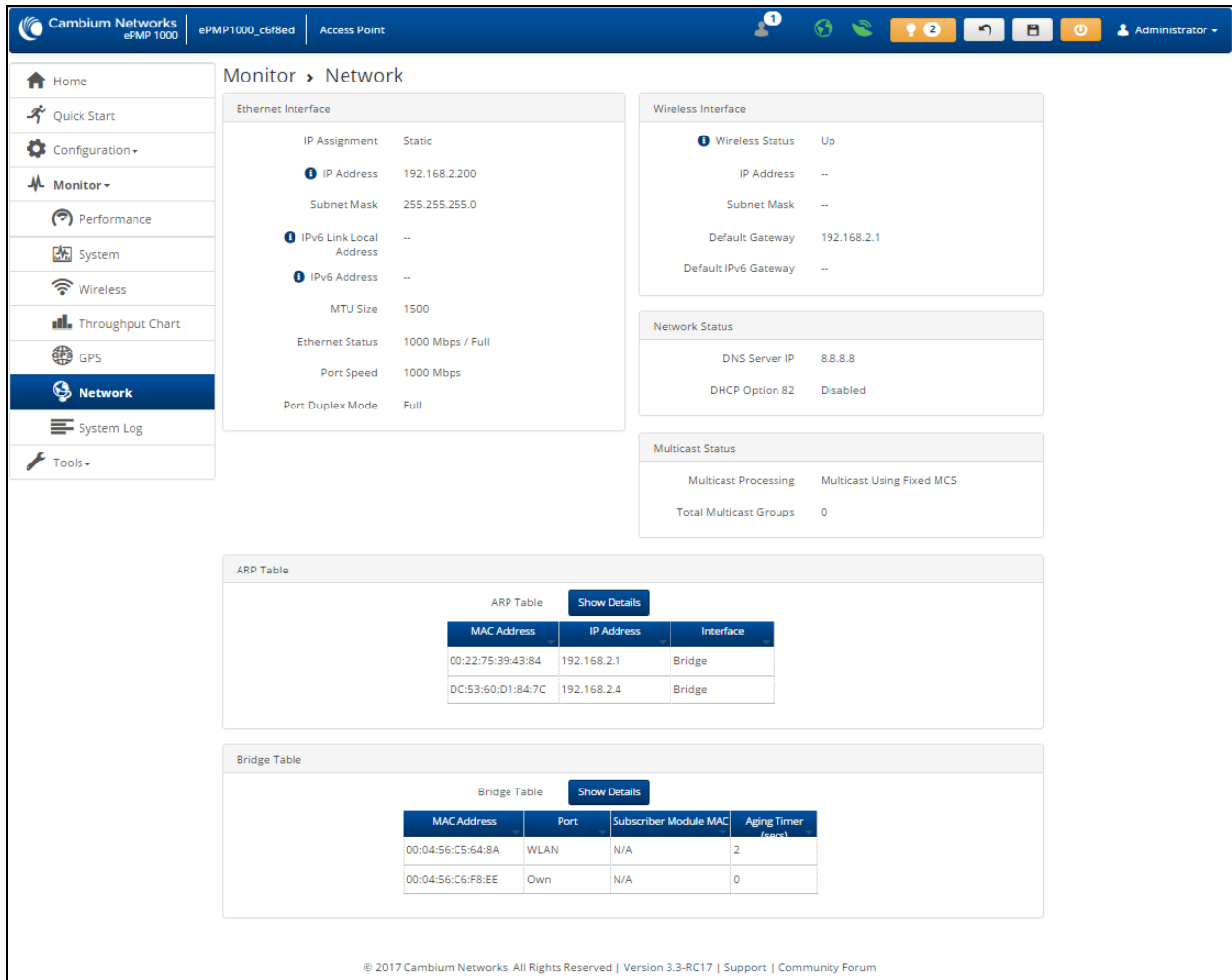


Figure 60: AP Network Status page

Table 115: AP Network Status page attributes

Attribute	Meaning
Ethernet Status	
IP Assignment	Static: Device management IP addressing is configured manually in fields Device IP Address (LAN), IP Subnet Mask (LAN), Gateway IP Address (LAN), and DNS Server IP Address (LAN). DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters Device IP Address (LAN), IP Subnet Mask (LAN), Gateway IP Address (LAN), and DNS Server IP Address (LAN) are unused.
IP Address	The current IP Address mode of the device (static or DHCP).
Subnet Mask	The currently configured device IP subnet mask.

Attribute	Meaning
IPv6 Link Local Address	A link-local address is required for the IPv6-enabled interface (applications may rely on the link-local address even when there is no IPv6 routing). The IPv6 link-local address is comparable to the auto-configured IPv4 address 169.254.0.0/16.
IPv6 Address	The IPv6 address for device management.
MTU Size	The currently configured Maximum Transmission Unit for the AP's Ethernet (LAN) interface. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Status	Up: The device's Ethernet interface is functioning and passing data. Down: The device Ethernet interface has encountered an error disallowing full operation. Reset the device to reinitiate the Ethernet interface.
Port Speed	The current Ethernet port speed of the radio.
Port Duplex Mode	The current Ethernet port duplex mode of the radio.
Wireless Status	
Wireless Interface	Up: The device wireless interface is functioning and passing data Down: The device's wireless interface has encountered an error disallowing full operation. Reset the device to reinitiate the wireless interface.
IP address	Currently unused.
Subnet Mask	Currently unused.
Default Gateway	The IP address that is currently assigned.
Network Status	
DNS Server IP	Represents the IP address of the DNS Server.
DHCP Option 82	Enabled: ePMP inserts "remote-id" (option ID 0x02) to be SM's MAC address and the "circuit-id" (ID 0x01) to be the AP's MAC address. Those two fields are used to identify the remote device and connection where the DHCP request was received and the DHCP server can assign an IP address accordingly. Disabled: When 'Disabled', AP passes the bootP traffic unaffected. DHCP Option 82 is 'Disabled' by default.
Multicast Status	
Multicast Processing	Displays the rate at which multicast traffic is sent on the downlink. Multicast Using Fixed MCS: Multicast traffic is sent to the SMs on the downlink at MCS 1. Multicast Using Best MCS: Multicast traffic is converted to unicast and sent to the SMs at the current MCS capability on the downlink.

Attribute	Meaning
Total Multicast Groups	Displays the current number of multicast groups that the AP has identified from IGMP devices connected to the registered SMS.
ARP Table	
MAC Address	MAC Address of the devices on the bridge.
IP Address	IP Address of the devices on the bridge.
Interface	Interface on which the AP identified the devices on.
Bridge Table	
MAC address	The hardware address of the AP.
Port	The port to which the device is connected.
Subscriber Module MAC	MAC Address for one of the connected SMS.
Aging Timer (secs)	Time set for the MAC addresses in the Bridge table.

AP System Log page

Use the AP System Log page to view the device system log and to download the log file to the accessing PC/device.

The screenshot shows the Cambium Networks ePMP 2000 web interface. The top navigation bar includes the Cambium Networks logo, the device ID 'ePMP2000_d184b5', and the title 'Access Point'. The left sidebar contains a menu with options: Home, Quick Start, Configuration, Monitor (selected), Performance, System, Wireless, Throughput Chart, GPS, Network, System Log (highlighted), and Tools. The main content area is titled 'Monitor > System Log'. It features a 'Syslog Display' toggle switch set to 'Enabled'. Below the toggle is a 'Syslog File' section with a scrollable log of system events. The log entries include:


```
Nov 15 15:10:14 ePMP2000_d184b5 user_absent[172.26.120.156]: sessions: kill_session_by_name: aa5919e5fb203c3a095d29c9268cc95e
Nov 15 15:10:14 ePMP2000_d184b5 user_absent[172.26.120.156]: sessions: kill_session_by_name: eb94781eeba70acd6fbd28a6de88951a
Nov 15 15:10:42 ePMP2000_d184b5 admin[172.26.120.156]: web_interface: User 'admin' is logged in...
```

 A 'Download' button is located below the log. At the bottom of the page, the copyright notice reads: '© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum'.

Figure 61: AP System Log page

Table 116: AP System Log attributes

Attribute	Meaning
Syslog Display	Enabled: The system log file is displayed on the management GUI. Disabled: The system log file is hidden on the management GUI.
Download	Use this button to download the full system log file to a connected PC or device.

AP Tools menu

The AP **Tools** menu provides several options for upgrading device software, configuration backup/restore, analyzing RF spectrum, testing device throughput, and running ping and traceroute tests.

- [AP Software Upgrade page](#)
- [AP Backup/Restore page](#)
- [AP Backup/Restore page](#)
- [AP eDetect page](#)
- [AP Spectrum Analyzer page](#)
- [AP Automatic Channel Selection page](#)
- [AP eAlign page](#)
- [AP Wireless Link Test page](#)
- [AP Ping page](#)
- [AP Traceroute page](#)

AP Software Upgrade page



Caution

Please read the Release Notes associated with each software release for special notices, feature updates, resolved software issues, and known software issues.

The Release Notes may be accessed at the [Cambium Support Center](#).

Use the AP **Software Upgrade** page to update the device radio software to take advantage of new software features and improvements.

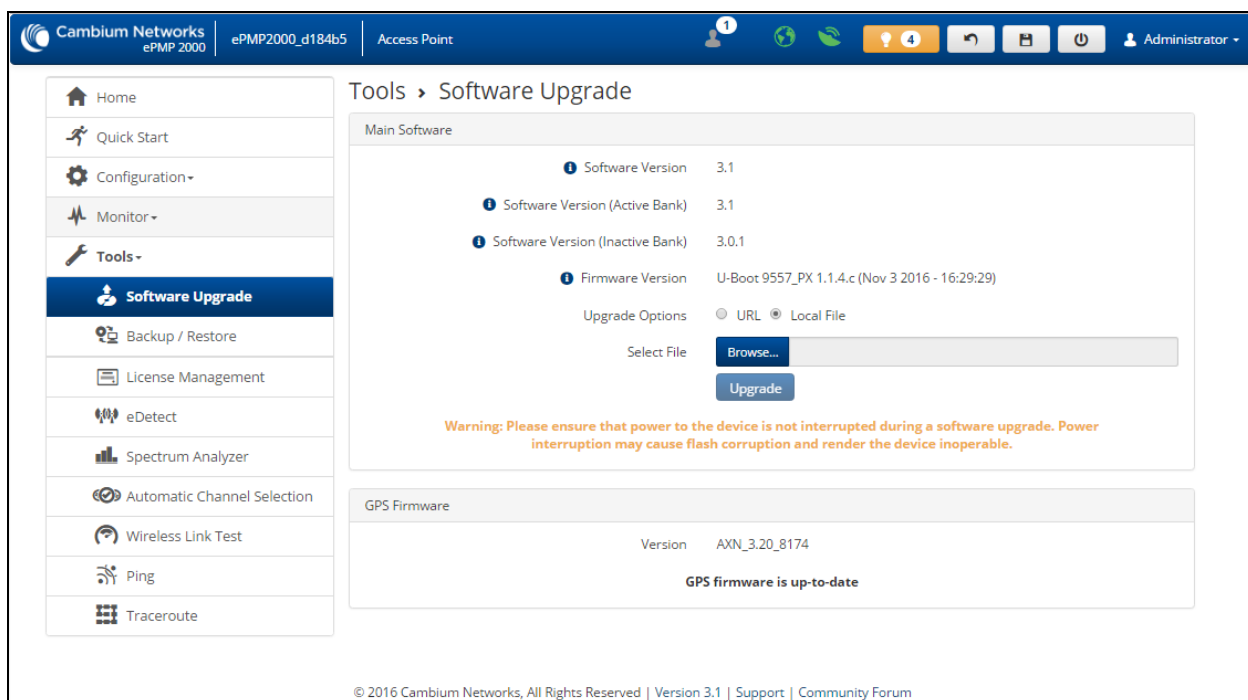


Figure 62: AP Software Upgrade page

Table 117: AP Software Upgrade attributes

Attribute	
Main Software	
Software Version	ePMP boards that do not have an onboard GPS have one bank of flash memory which contains a version of the software. The version of the software last upgraded onto the Flash memory is present on this bank of flash memory. This software will be used by the AP when the AP is rebooted.
Software Version (Active Bank)	ePMP boards that have an onboard GPS have two banks of flash memory which each contain a version of the software. The version of the software last upgraded onto the Flash memory is made the Active Bank. This software will be used by the AP when the AP is rebooted.
Software Version (Inactive Bank)	ePMP boards that have an onboard GPS have two banks of flash memory which each contain a version of the software. The version of the software that was the Active Bank is made the Inactive Bank when another version of the software is upgraded onto the Flash memory. The Inactive Bank of the software will be used by the SM in case the Active Bank cannot be used due to a failure condition.
Firmware Version	The current U-Boot version.

Attribute	
Upgrade Options	<p>URL: A web server may be used to retrieve software upgrade packages (downloaded to the device via the webserver). For example, if a web server is running at IP address 192.168.2.1 and the software upgrade packages are located in the home directory, an operator may select an option From URL and configure the Software Upgrade Source field to http://192.168.2.1/<software_upgrade_package>.</p> <p>Local File: Click Browse to select the local file containing the software upgrade package.</p>
Select File	Click Browse to select a local file (located on the device accessing the web management interface) for upgrading the device software.
GPS Firmware	
Firmware Version	<p>The current firmware of the on-board GPS chip (AXN_1.51_2801 or AXN_3.20_8174).</p> <p>(1st Generation ePMP 1000 - Units purchased 2015 and prior) After upgrading, this version should show as AXN_1.51_2838.</p> <p>(2nd Generation ePMP 1000 and ePMP 2000 - Units purchased 2016 and after) After upgrading, this version should show as AXN_5.1_8174.</p>
Upgrade Options	<p>URL: A web server may be used to retrieve GPS firmware upgrade packages (downloaded to the device via the webserver). For example, if a web server is running at IP address 192.168.2.1 and the firmware upgrade packages are located in the home directory, an operator may select the option From URL and configure the GPS Firmware Upgrade Source field to http://192.168.2.1/<firmware_upgrade_package>.</p> <p>Local File: Click Browse to select the local file containing the GPS firmware upgrade package.</p> <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>If the “GPS Firmware Version” under Monitor=>GPS Status shows “NOT AVAILABLE”, it means that the on-board GPS chip has locked up. A power cycle of the ePMP unit is required to restore the connectivity to the chip before performing the GPS firmware upgrade.</p> </div>
Select File	<p>Click Browse to select a local file (located on the device accessing the web management interface) for upgrading the on-board GPS chip firmware.</p> <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>Use the same package that is used to upgrade the device’s software. The new GPS firmware is part of the software upgrade packages.</p> </div>

To upgrade the device software from a local file (or network-accessible file), follow this procedure:

Procedure:

1. Download the software upgrade packages from <https://support.cambiumnetworks.com/files/epmp>
2. Clear the accessing browser cache.
3. On the device GUI, navigate to **Tools > Software Upgrade**.

4. Select the **Software Upgrade Source** which represents the location of your software upgrade packages.
5. Based on the configuration of **Software Upgrade Source**, enter either the **Software Upgrade Source** or click the **Browse** button and locate the software package.
6. Click **Upgrade**.
7. When the upgrade completes successfully, click the **Reset** icon.

To upgrade the GPS firmware from a local file (or network-accessible file), follow this procedure:

Procedure:

1. Download the software upgrade packages from <https://support.cambiumnetworks.com/files/epmp>
2. Clear the accessing browser cache.
3. On the device GUI, navigate to **Tools > Software Upgrade**.
4. Select the **Upgrade Options** under **GPS Firmware** which represents the location of your software upgrade packages.
5. Based on the configuration of **GPS Firmware Source**, enter either the **Upgrade Source** or click the **Browse** button and locate the firmware package.
6. Click Upgrade.
7. When the upgrade completes successfully, click the **Reset** icon.

AP Backup/Restore page

Use the AP Backup/Restore page to perform the following functions:

- Back up the configuration in either text (.json) format or binary (.bin) format.
- Restore the configuration of using a configuration file that was previously backed up.
- Reset the device to its factory default configuration. For more factory defaulting methods, see:
 - [Using the device external reset button](#)
 - [Resetting ePMP to factory defaults by power cycling](#)

AP License Management page

The AP's License Management page is used to:

- Install licensing for ePMP Elevate subscriber access allotments
- Convert the AP from Lite (10 subscribers) to Full (120 subscribers)
- Configure the Country Code ETSI-locked devices

Beginning with Software Release 3.5.1, there are two types of ePMP Elevate license management mechanisms available on the ePMP device - Flexible and Fixed, described below:

Flexible Licensing

With Flexible Licensing, your licenses are stored in a license server and can be shared among all your Access Points. Each Access Point will only use as many licenses as it has connected subscribers. When a subscriber disconnects, a license is returned to the pool and can be used by any other Access Point.

In order to use Flexible Licensing, your Access Points must:

- be able to make HTTPS requests out to the Internet,
- be running firmware version 3.5 or greater,
- have an accurate NTP time source.

[Use Flexible Licensing →](#)

Fixed Licensing

With Fixed Licensing, you will generate a license key for a specific MAC address, and load that license key into the Access Point. The license key represents the number of Elevate Subscribers that can be supported by that Access Point. The license key may not be transferred to any other Access Point.

You should use Fixed Licensing if your Access Points:

- are unable to make HTTPS requests to the Internet, or
- are running firmware version 3.4.1 or earlier, or
- don't have an accurate NTP time source.

[Use Fixed Licensing →](#)

Figure 63: AP ePMP Elevate license management options



Note

Country Code configuration for ETSI locked device and Full Capacity Keys for AP Lite devices are available only via Fixed License Management.



Note

To use flexible licensing, the AP must have DNS server access to be able to resolve URLs (and communicate with the license server). Also, the AP must have a valid, accurate time server (NTP) connection.

The screenshot shows the 'Tools > License Management' page in the Cambium Networks ePMP 1000 web interface. The page is split into two main sections: Flexible License Management and Fixed License Management.

Flexible License Management:

- License Server Agent:** Disabled (radio button) / Enabled (radio button)
- Cloud Licensing ID:** [Redacted]
- Connection Status:** Connected. ePMP Elevate Subscriber Module Limit synced with License Server
- Enable Proxy:** Disabled (radio button) / Enabled (radio button)
- Proxy Server IP Address:** [Redacted]
- Proxy Server Port:** 8080 (min: 1 | max: 65535)
- Refresh Requests Failed:** 0
- Update Requests Failed:** 0
- NTP Status:** NTP Enabled, Date and Time is obtained from NTP Server
- Date and Time:** 09 Jul 2018, 14:41:54 GMT
- ePMP Elevate Subscriber Module Limit:** 1

Fixed License Management:

- Local License Key:** [Redacted]
- Version:** Not received
- MAC address:** Not received
- Country Code:** Not received
- Subscriber Module Limit:** 120 (Unlocked)
- Signature:** Unknown

At the top of the page, there is a warning message: "ePMP Elevate License: ePMP Access Point will not support ePMP Elevate Subscriber Module registration unless a local License Key is obtained or License Server enabled with appropriate Cloud Licensing ID."

Figure 64: AP License Management page

Table 118: AP License Management attributes

Attribute	Meaning
Flexible License Management	
License Server Agent	<p>Disabled: No communication with the License Server is established</p> <p>Enabled: Enables License Server functionality to obtain the number of allowed ePMP Elevate SMs to be connected to the AP</p>
Cloud Licensing ID	This field represents a Cambium Networks customer identification used for AP identification on the License Server. This identifier is generated upon License Entitlement activation at the Cambium Networks web-based Support Center.
Connection Status	The Connection Status displays the License Server process state when License Server Agent is Enabled . This status may also be referenced on the device Home page.
Enable Proxy	<p>Disabled: The AP must have a valid internet connection to reach the license server</p> <p>Enabled: A proxy server is specified for license server access from a private network</p>
Proxy Server IP Address	Specify the IP address of the proxy server used for internet access from a private network
Proxy Server Port	Specify the port used on the proxy server for internet access from a private network
Refresh Requests Failed	The number of failed refresh (polling) requests to the License Server. The ePMP Elevate Subscriber Module Limit resets to 1 after the 3 rd failed refresh request.
Update Requests Failed	The number of failed update (licensing information transfer) requests to the License Server. The ePMP Elevate Subscriber Module Limit resets to 1 after the 5 th failed updated request.
NTP Status	Represents whether or not the current time and date have been retrieved from the configured NTP server
ePMP Elevate Subscriber Module Limit	The number of ePMP Elevate devices allowed to register to the AP
Fixed License Management	
Local License Key	The "License Key" is obtained from support.cambiumnetworks.com and must be entered into this field to enable additional functionality (registration capacity, ePMP Elevate support) of the ePMP device.
Version	Specifies the licensing version scheme for the License Key
MAC address	The MAC Address is extracted from the License Key and must match the MAC Address of this device for the licenses to be enacted.

Attribute	Meaning
Country Code	A two-character value representing the licensed country
Subscriber Module Limit	ePMP Lite / Force 110 devices are limited to 10 SMs in AP TDD mode. SM Limit will display Unlocked if a license is present which allows no limit of SMs to register to the device in AP TDD mode.
Signature	A valid License Key must have a valid signature included. The status is displayed after a License Key is entered and saved. Licenses can only be used if the signature is valid.

AP eDetect page

The eDetect tool (not available in ePTP Master mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP, on the current operating channel. When the tool is run, the ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS. Use the AP eDetect page to perform the following functions:

- Collect information about interferers system-wide on the AP and the SMs connected to it to display on the APs GUI.
- Collect information about interferers locally at the AP only to display on the AP's GUI.

The screenshot shows the Cambium Networks ePMP 2000 web interface. The top navigation bar includes the Cambium Networks logo, the device model 'ePMP2000_d184b5', and the role 'Access Point'. The user is logged in as 'Administrator'. The left sidebar contains various navigation options, with 'eDetect' highlighted. The main content area is titled 'Tools > eDetect' and shows the following configuration and results:

- eDetect**
 - Detecting Device:** AP AP/SMs
 - Detection Duration:** 30 (sec | min: 10 | max: 120)
 - Start/Stop:** Stop
 - Export to CSV:** Export
 - Status:** Running ...
 - SSID:** Cambium-AP
- Detection Results:**


Interferers' MAC	Interferers' SSID	Interferers' RSSI (dBm)
MAC: 00:04:56:C0:26:D8	RSSI (dBm): -54	RATE: MCS-15 (No interferers)
MAC: 00:04:56:D1:84:B6	RSSI (dBm): -63	RATE: MCS-1 (No interferers)
MAC: 00:04:56:FB:28:BB	RSSI (dBm): -56	RATE: MCS-15 (No interferers)

© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 65: AP eDetect page

Table 119: AP eDetect attributes

Attribute	Meaning
Detecting Device	AP: Choosing this option will collect information about interferers local to the AP.

Attribute	Meaning
	AP/SMs: Choosing this option collect information about interferers system-wide i.e. interferers local to the AP as well as interferers at the SMs connected to the AP.
Detection Duration	Configure the duration for which the AP (and SMs) scan for interferers.  <div style="background-color: #f4a460; padding: 5px; margin-left: 20px;"> Caution During the scanning period, the AP continues servicing the SMs under it, and there is no outage (unlike running a Spectrum Analyzer). There may be a negligible degradation in overall sector throughput. </div>
Start/Stop	Use to start or stop the interference detection.
Export to CSV	Choose this option to export the detection results to .csv format.
Status	Current status of the Interference Detection tool.
SSID	The current configured name/SSID of the AP.
Detection Results	Use the Detection Results table to monitor interferers at the AP and the registered SMs and their key RF parameters.
Device Instant Health	This is an indicator of the device's health in terms of channel conditions in the presence of interferer(s). Green: Indicates that the channel is relatively clean and has good C/I levels (>25dB). The interference level is low. Yellow: Indicates that the channel has moderate or intermittent interference (C/I between 10dB and 25dB). Red: Indicates that the channel has high interference and poor C/I levels (<10dB).
Device MAC	The MAC address of the AP and/or SMs wireless interface.
Device RSSI (dBm)	The Received Signal Strength Indicator, which is a measurement of the power level being received by the device's antenna.
Device MCS	Modulation and Coding Scheme - indicates the modulation mode used for the radio's receiver side, based on radio conditions (MCS 1-7, 9-15).
Interferers' MAC	The MAC address of the interferer's wireless interface.
Interferers' RSSI (dBm)	The Received Signal Strength Indicator, which is a measurement of the interferer's power level being received by the device's antenna.
Interferers' MCS	Modulation and Coding Scheme - indicates the modulation mode used by the interferer, based on radio conditions (MCS 1-15).



Note

The system is operational when the eDetect tool is initiated. The detection is done during the transmission period within the TDD frame. The AP may detect another AP on its back sector as an interferer when it is using the same frequency carrier in a GPS Synchronized system. Also, since the detection happens when the system is operational, there may be a negligible degradation in overall sector throughput when run from the AP.

AP Spectrum Analyzer page

Use the AP Spectrum Analyzer page to download the spectrum analyzer tool.

To download the spectrum analyzer tool, the AP **Device Mode** must be set to **Spectrum Analyzer**.

Java Runtime Environment is required to run the AP spectrum analyzer.



Caution

Conducting spectrum analysis causes the AP to enter scan mode and the AP drops all RF connections.

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

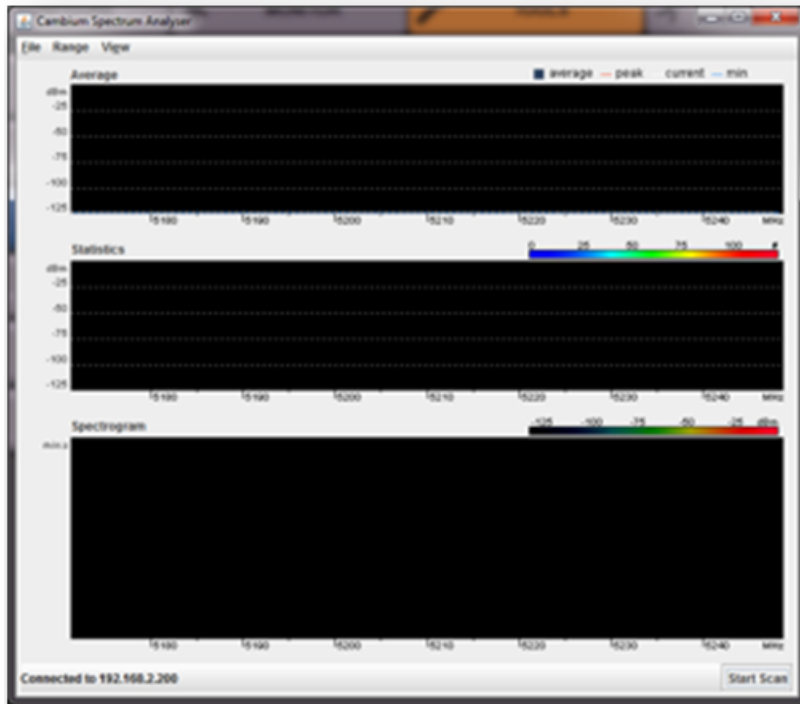
To conduct a spectrum analysis, follow this procedure:

Required Software:

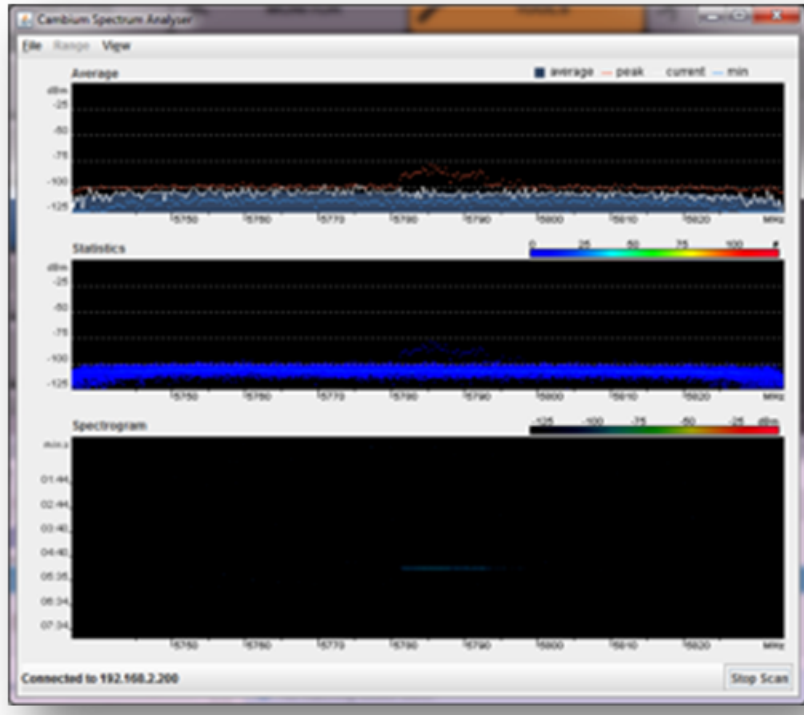
- Java Run-time Environment (JRE)

Procedure:

1. On the AP GUI, navigate to **Configuration > Radio**
2. Change the Radio Mode to Spectrum Analyzer.
3. Click the **Save** button.
4. Click the **Reset** button.
5. Log in to the AP GUI and navigate to **Tools => Spectrum Analyzer**.
6. Click Download Spectrum Analyzer Tool.
7. Locate the folder to which the spectrum analyzer tool was saved and double-click on file csa.jnlp to launch the tool.
8. If a security warning window appears, check the box next to "I accept the risk and want to run this application".
9. In the security warning window, click **Run**
The spectrum analyzer interface is displayed



10. Click **Range** to configure the range of frequencies to scan.
11. Display of the average, peak, current, and minimum power levels for the configured range Click **Start Scan** to begin scanning
12. Spectrogram display of the energy levels detected throughout the configured range, over time
Statistical display of the number of times each frequency in the range was scanned.



Once the scanning completes, follow these steps to return the device to AP operation:

Procedure:

1. In the spectrum analyzer application, click **Stop Scan**.
2. Close the spectrum analyzer application by clicking **File > Exit**.
3. On the AP GUI, navigate to **Configure > Radio**.
4. Configure Device Mode to AP.
5. Click the **Save** button.
6. Click the **Reset** button.

AP Automatic Channel Selection page

Use the Automatic Channel Selection page to use the Automatic Channel Selection feature to allow the AP to choose the best channel possible under the current RF environment. This feature is not available when the AP is in ePTP Master mode.

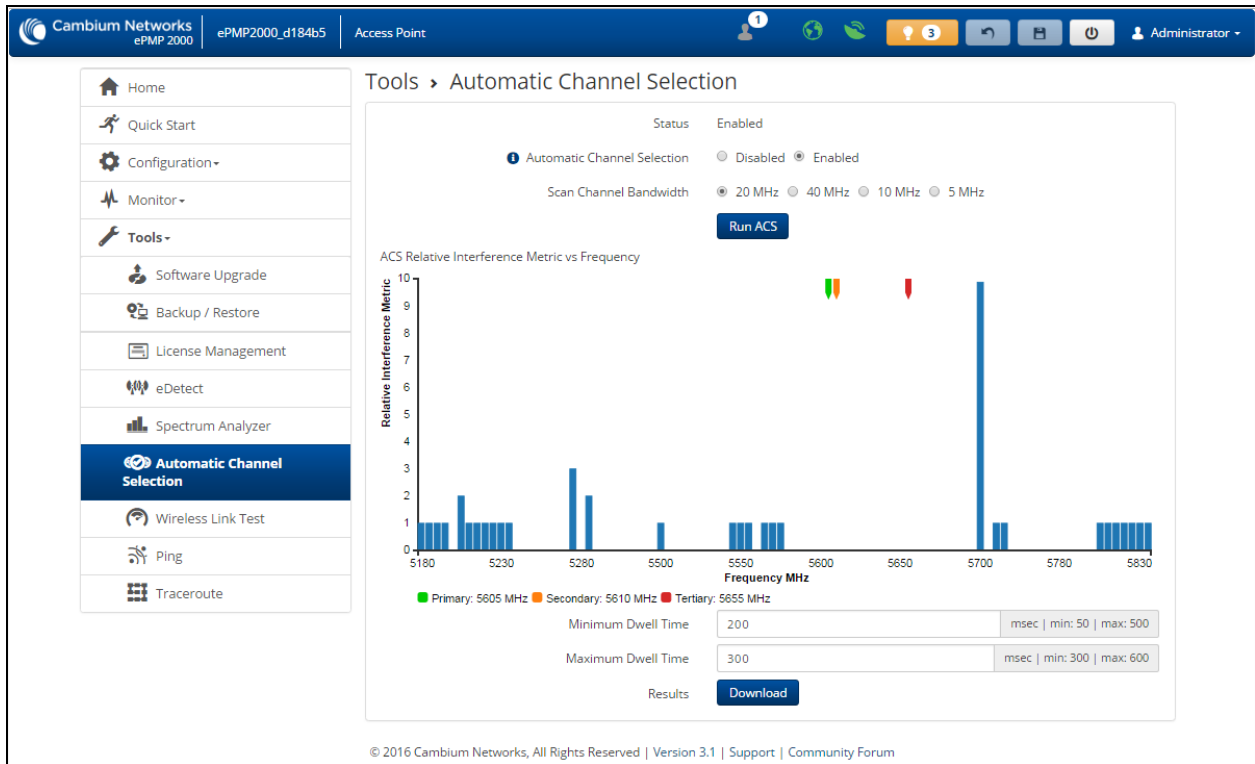


Figure 66: AP Automatic Channel Selection

Table 120: Automatic Channel Selection

Attribute	Meaning
Automatic Channel Selection	<p>Enabled: This enables the Automatic Channel Selection (ACS) feature. ACS allows the radio to scan the entire band (governed by the Country setting) and chooses a channel with the lowest channel occupancy i.e. lowest interference level. To run the ACS feature (once enabled), the radio will have to be rebooted or manually triggered using Tools->Automatic Channel Selection. When ACS is running, the radio measures the occupancy level of the channel (measured in terms of an internal interference metric) and uses an algorithm to decide to choose the best channel within the band. The channel chosen is not based just on the occupancy level channel but also on the occupancy level of adjacent channels.</p> <p>Disabled: ACS is disabled and the operator should configure a Frequency Carrier manually.</p> <div data-bbox="397 1556 467 1633" style="float: left; margin-right: 10px;"> </div> <div data-bbox="532 1556 1419 1831" style="border: 1px solid black; padding: 5px;"> <p>Note</p> <p>The channel bandwidth configured before enabling and running ACS will be used to automatically select a channel. For example: If the operator manually configured a channel bandwidth of 20MHz, ACS will scan and choose a channel of 20MHz wide channel. To switch ACS to 40MHz or other channel bandwidth, the operator should disable ACS, manually configure 40MHz or desired channel bandwidth on the radio, then enable and run ACS.</p> </div>

Attribute	Meaning
Scan Channel Bandwidth	Configure the channel size for which the radio needs to scan the band.
Minimum Dwell Time	Configure the minimum time in milliseconds for which the radio needs to scan a channel to measure channel occupancy or interference levels. Default is 200 ms.
Maximum Dwell Time	Configure the maximum time in milliseconds for which the radio needs to scan a channel to measure channel occupancy or interference levels. Default is 300 ms.
Results	Click this button to download the most recent ACS results in .csv format.

AP eAlign page

Use the eAlign page to aid with link alignment.



Note

A valid link to an SM is required to provide meaningful RSSI measurements.



Figure 67: AP eAlign

Table 121: eAlign

Attribute	Meaning
Operating Frequency	The current frequency at which the AP is operating.

Attribute	Meaning
Registered SM MAC Address	The MAC address of the SM that is registered to the AP.
Current RSSI	Current RSSI value measured on the uplink by the AP's receiver.
Peak RSSI	Peak RSSI value measured by the AP's receiver from the time the user navigated to the eAlign page.
Reset Measurements	Click this button to reset all current measurements.



Caution

ePMP supports Automatic Transmit Power Control (ATPC) where the SMs are instructed by the AP to adjust their Tx power in order for the SM's signal (UL RSSI) to arrive at the AP at a predetermined RSSI level (configurable on the AP under **Configuration > Radio > Power Control > Subscriber Module Target Receive Level**). This feature is beneficial to keep the overall noise floor in the sector to an acceptable level and is critical for deploying a GPS Synchronized system. However, the feature negates the purpose of eAlign measurements on the AP since, during the alignment, the SM may constantly change its Tx power. It is recommended to turn off ATPC and set the SM's Tx power to maximum allowable power during alignment.

While aligning the link using eAlign, please follow these steps:

Procedure:

1. On the SM, set **Configuration > Radio > Power Control > Tx Power Manual Limit** to **Max Tx Output Power**.
2. Set **Configuration > Radio > Power Control > Transmitter Output Power** to **30 dBm** (or maximum value allowed by regulations).
3. Click the **Save** button.
4. Perform link alignment using **eAlign**.
5. Once alignment is complete, set **Configuration > Radio > Power Control > Tx Power Manual Limit** back to **Auto**.
6. Click the **Save** button.

AP Wireless Link Test page

Use the AP Wireless Link Test page to conduct a simple test of AP wireless throughput to any one of the connected SMs. This allows users to determine the throughput that can be expected on a particular link without having to use external tools.

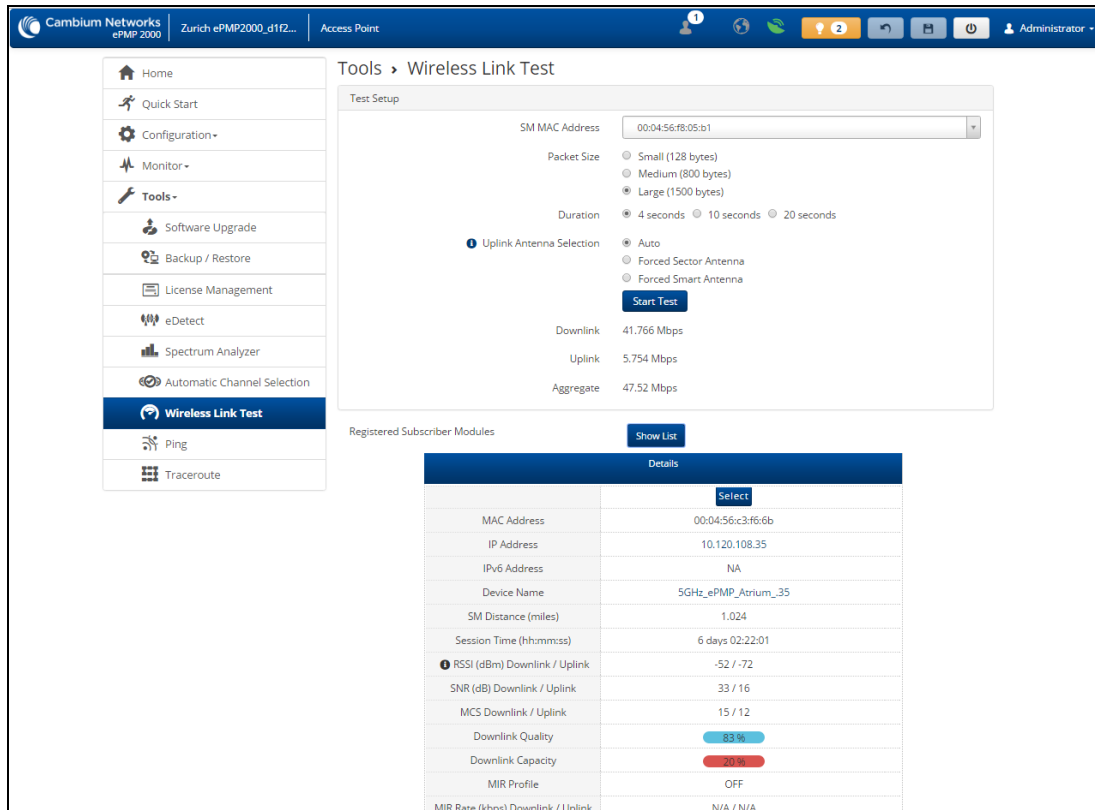


Figure 68: AP Wireless Link Test

Table 122: AP Wireless Link Test attributes

Attribute	Meaning
Test Setup	
SM MAC Address	Enter the MAC Address of one of the connected SMs or simply click the Select button of the SM desired in the “Registered Subscriber Modules” list.
Packet Size	Choose the Packet Size to use for the throughput test.
Duration	Choose the time duration in seconds to use for the throughput test.
Uplink Antenna Selection	Uplink Antenna Selection specifies the antenna to be used in the uplink for the wireless link test. The antenna cannot be forced if it is already configured to Forced Sector Antenna or Forced Smart Antenna in section Configuration > Radio .
Downlink	This field indicates the result of the throughput test on the downlink, in Mbps.
Uplink	This field indicates the result of the throughput test on the uplink, in Mbps.
Aggregate	This field indicates the result of the aggregate throughput on the link, in Mbps. Displayed only when Downlink/Uplink Ratio is set to 75/25, 50/50 or 30/70.
Registered Subscriber Modules	Use the Registered Subscriber Modules table to monitor registered SMs and their key RF status and statistics information. Click Select on the SM that is desired to be used in the throughput test.

AP Ping page

Use the AP Ping page to conduct a simple test of AP IP connectivity to other devices which are reachable from the network. If no ping response is received or if “Destination Host Unreachable” is reported, the target may be down, there may be no route back to the AP, or there may be a failure in the network hardware (i.e. DNS server failure).

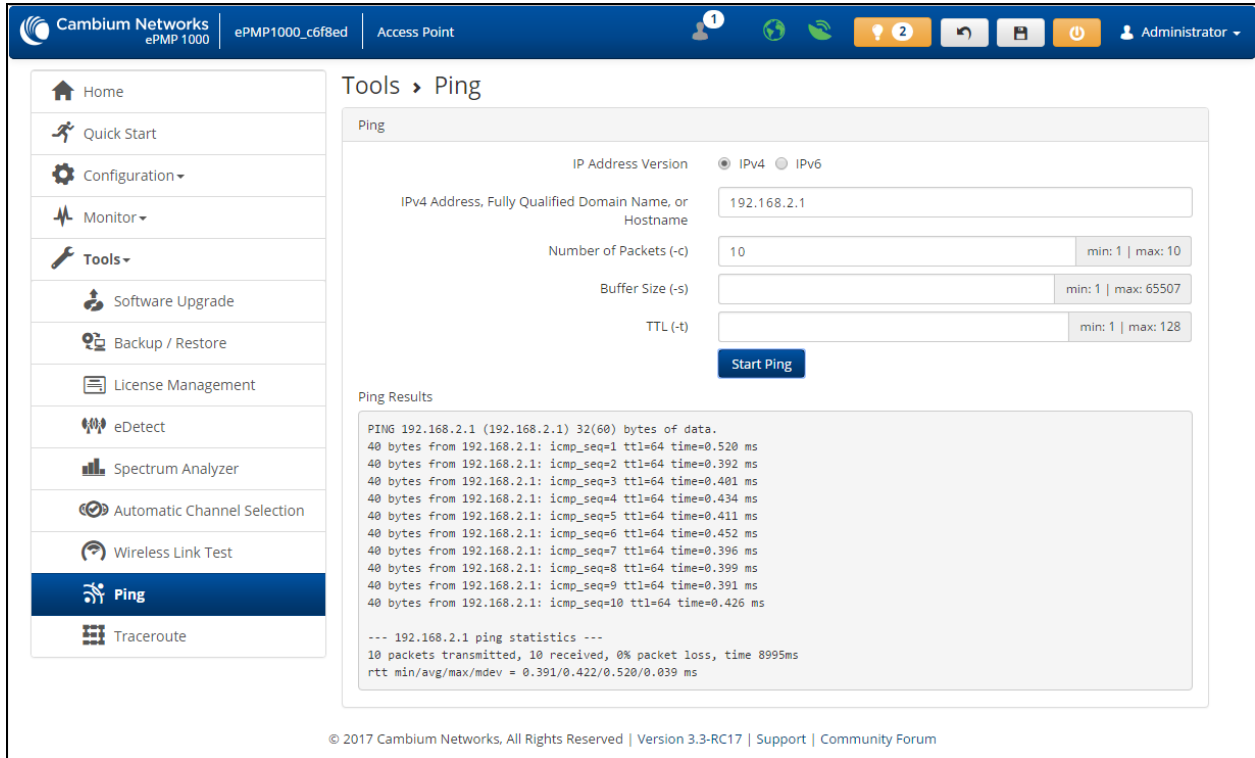


Figure 69: AP Ping page

Table 123: AP Ping attributes

Attribute	Meaning
Ping	
IP Address Version	IPv4: The ping test is conducted via IPv4 protocol. IPv6: The ping test is conducted via IPv6 protocol.
IP Address	Enter the IP address of the ping target.
Number of packets (-c)	Enter the total number of ping requests to send to the target.
Buffer size (-s)	Enter the number of data bytes to be sent.
TTL (-t)	Set the IP Time-To-Live (TTL) for multicast packets. This flag applies if the ping target is a multicast address.
Ping results	Results of the Ping test are displayed in the box.

AP Traceroute page

Use the AP Traceroute page to display the route (path) and associated diagnostics for IP connectivity between the AP and the destination specified.

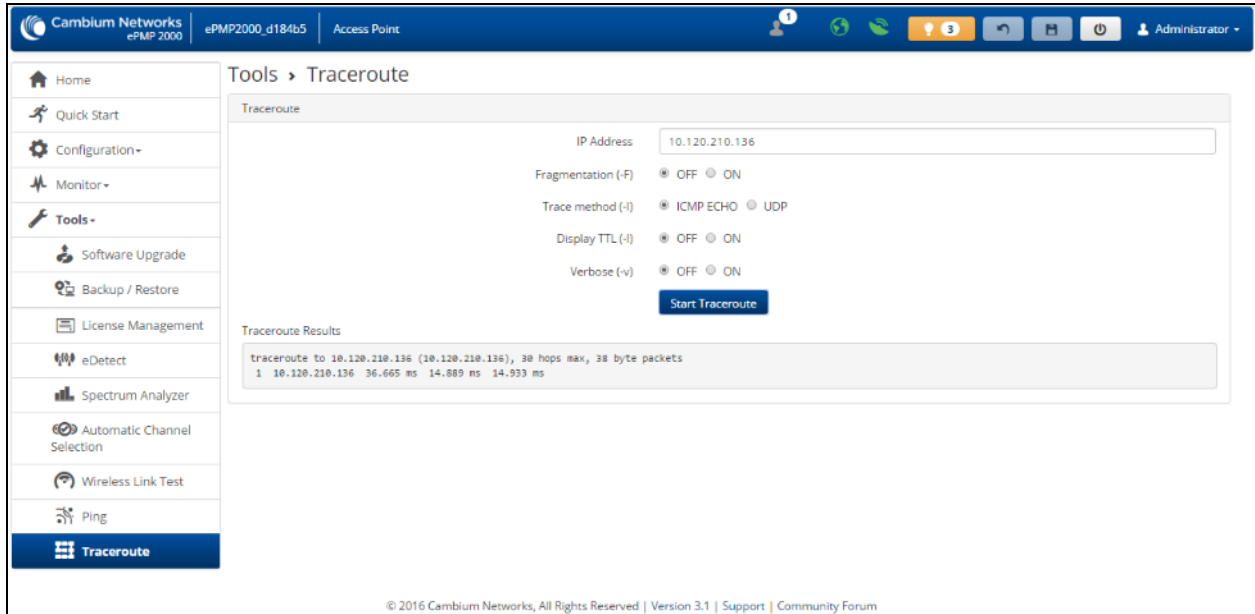


Figure 70: AP Traceroute page

Table 124: AP Traceroute attributes

Attribute	Meaning
Traceroute	
IP Address	Enter the IP address of the target of the traceroute diagnostic.
Fragmentation (-F)	ON: Allow source and target to fragment probe packets. OFF: Do not fragment probe packets (on the source or target).
Trace method (-l)	ICMP ECHO: Use ICMP ECHO for traceroute probes. UDP: Use UDP for traceroute probes.
Display TTL (-l)	ON: Display TTL values for each hop on the route. OFF: Suppress display of TTL values for each hop on the route.
Verbose (-v)	ON: ICMP packets other than TIME_EXCEEDED and UNREACHABLE are displayed in the output. OFF: Suppress display of extraneous ICMP messaging.
Traceroute Results	Traceroute test results are displayed in the box.

Using the SM menu options

Use the menu navigation bar in the top and left panels to navigate to each web page. The functional area that may be accessed from each menu option is listed under [Table 103 Functional areas accessed from each AP menu option](#). Some of the parameters are only displayed for specific system configurations.

Table 125: Functional areas accessed from each SM menu option

Menu option	Menu Details
Quick Start	Configuring SM units using the Quick Start menu
Configuration	SM Configuration menu
Radio	SM Radio page
Quality of Service	SM Quality of Service page
System	SM System page
Network	SM Network page
Security	SM Security page
Monitor	SM Monitor menu
Performance	SM Performance page
System Status	SM System page
Wireless Status	SM Wireless page
Throughput Chart	SM Throughput Chart page
Network Status	SM Network page
System Log	SM System Log page
Tools	SM Tools menu
Software Upgrade	SM Software Upgrade page
Backup / Restore	SM Backup / Restore page
eDetect	SM eDetect page
Spectrum Analyzer	SM Spectrum Analyzer page
eAlign	SM eAlign page
Wireless Link Test	SM Wireless Link Test page
Ping	SM Ping page
Traceroute	SM Traceroute page

SM Configuration menu

Use the **Configuration** menu to access all applicable device configuration parameters. It contains the following pages:

- [SM Radio page](#)
- [SM Quality of Service page](#)
- [SM System page](#)
- [SM Network page](#)
- [SM Security page](#)

SM Radio page

Use the Radio page to configure the device radio interface parameters.



Caution

Modifying radio parameters may result in a wireless outage. Plan configuration modifications accordingly.

The screenshot displays the 'Configuration > Radio' page for a Cambium Networks ePMP 1000 device. The interface is divided into several sections:



- General:** Radio Mode is set to 'Subscriber Module'. Driver Mode is 'TDD'. Country is 'Follow AP's Country'. Range Unit is 'Miles'.
- Preferred APs:** A table with columns for SSID, Wireless Security, and WPA2 Pre-shared Key. The table is currently empty.
- Subscriber Module Scanning:** Scan Channel Bandwidth is set to 40 MHz. A 'Radio Frequency 40 MHz Scan List' is shown with a grid of checkboxes for frequencies from 4930 MHz to 5855 MHz in 5 MHz increments.
- Power Control:** Max Tx Power is 'Auto'. Transmitter Output Power is 30 dBm. Antenna Gain is 13 dBi. Network Entry RSSI Threshold is -80 dBm. Network Entry SNR Threshold is 0 dB. Uplink Antenna Selection is 'Auto'.
- Scheduler:** Uplink Max Rate is 'MCS 15 - 64-QAM 5/6'.

© 2017 Cambium Networks. All Rights Reserved | Version 3.3-RC16 | Support | Community Forum

Figure 71: SM Radio page (TDD or ePTP Slave mode)

Table 126: SM Radio Configuration attributes (TDD mode or ePTP Slave mode)

Attribute	Meaning
General	

Attribute	Meaning
Radio Mode	This parameter controls the function of the device – All ePMP devices may be configured to operate as an Access Point (AP) , Subscriber Module (SM) , or as a Spectrum Analyzer .
Driver Mode	This parameter controls the wireless mode of operation of the SM. TDD: The SM is operating in the proprietary TDD mode and will only connect to another ePMP Access Point. Standard WiFi: The SM is operating in the Standard 802.11n WiFi mode and will be able to connect to any Access Point operating in standard 802.11n WiFi mode. ePTP Slave: The SM is operating as a Slave in point-to-point mode. The AP and the system do not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode.
Country	The SM automatically inherits the Country Code setting of the AP (except for US-locked devices). Country settings affect the radios in the following ways: <ul style="list-style-type: none"> • Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain) • DFS operation is enabled based on the configured country code, if applicable • Frequency selection is based on local regulatory limits
Range Unit	The unit of measurement used for reporting Distance from AP .
Preferred AP List	
Preferred APs	The Preferred AP List is comprised of a list of up to 16 APs to which the SM sequentially attempts registration. For each AP configured, if authentication is required, enter a Pre-shared Key associated with the configured AP SSID . When the SM is in Standard WiFi mode, the SMs will actively probe the SSIDs in this list to find APs with hidden SSIDs.
Subscriber Module Scanning	
Scan Channel Bandwidth	Click the  button to unselect all channel bandwidths. The SM will not scan for any frequencies. Click the  button to select all channel bandwidths. The SM will scan all channel bandwidths, i.e. 5 MHz, 10 MHz, 20 MHz, and 40 MHz. Alternately choose individual channel bandwidth tabs and/or frequencies within each channel bandwidth tab for a customized scan list.
Power Control	
Max Tx Power	Auto: The Access Point can control, using ATPC (Automatic Transmit Power Control), the TX power of the SM up to the maximum capability of the SM's transmitter (based on regulatory limits).

Attribute	Meaning
	Manual: The Access Point can control the TX power of the SM up to the value configured in the Transmitter Output Power field below.
Transmitter Output Power	When Manual is selected, the SM will not transmit higher than the configured value in the field. Determines the maximum output power of the transmitter. The actual output power may be lower due to Automatic Transmit Power Control (ATPC), where the AP instructs the SM to lower its power to meet the SM target Receive Level configured on the AP.
Antenna Gain	This value represents the amount of gain introduced by the unit's internal antenna. This parameter is read-only for Integrated radios.
Network Entry RSSI Threshold	Set this parameter to the minimum Received Signal Strength Indicator (RSSI) at the SM required for the SM to attempt registration to an AP. For example, if the AP RSSI Threshold is set to -80 dBm, and the SM is receiving the AP signal at -85 dBm (RSSI = -85 dBm), the SM will not attempt to register to the AP.
Network Entry SNR Threshold	Set this parameter to the minimum Signal-to-Noise Ratio (SNR) at the SM required for the SM to attempt registration to an AP. For example, if the AP SNR Threshold is set to 30 dB and the SM is calculating its DL SNR as 25 dB, the SM will not attempt to register to the AP.
Uplink Antenna Selection	<p>Uplink Antenna Selection specifies the antenna to be used in the uplink. This parameter is specific to SMs registered to ePMP 2000 APs configured with an optional Smart Antenna.</p> <p>Auto: The AP decides which antenna to use (sector or Smart Antenna) for uplink communications based on internal quality metrics.</p> <p>Forced Sector Antenna: The AP uses the Sector Antenna for uplink communications with SMs configured with this option</p> <p>Forced Smart Antenna: The AP uses the smart antenna for uplink communications with SMs configured with this option</p> <div data-bbox="393 1255 1424 1528" style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p>Note</p> <p>If the AP is configured with Uplink Antenna Selection set to Auto and an SM is set to Forced Sector Antenna or Forced Smart Antenna, the SM setting will be enforced.</p> <p>If the AP is configured with Uplink Antenna Selection set to Forced Sector Antenna or Forced Smart Antenna and an SM is set to a conflicting Forced setting, the AP's setting will be enforced.</p> </div>
Scheduler	
Uplink Max Rate	Configure the MCS (Modulation and Coding Scheme) rate beyond which the radio's scheduler should not exceed when transmitting data traffic on the uplink. This is useful in situations where there are high variance and unpredictability in the interference present in the environment causing packet loss. Reducing the max rate to a lower MCS (than the default MCS 15) may help in these situations. Reducing the Uplink Max Rate will result in reduced throughput capacity of the SM in the uplink. Not available when SM is in ePTP Slave or Standard WiFi mode.

Cambium Networks ePMP 1000 ePMP1000_SM Subscriber Module Administrator

- Home
- Quick Start
- Configuration
 - Radio**
 - System
 - Network
 - Security
 - Monitor
 - Tools

Configuration > Radio

General

Radio Mode * Access Point Subscriber Module Spectrum Analyzer

Driver Mode TDD Standard WiFi ePTP Slave

Fallback Country

Range Unit Miles Kilometers

Preferred APs

Preferred APs [Add new AP](#) [Show Details](#)

SSID	Wireless Security	WPA2 Pre-shared Key
Table is empty		

Subscriber Module Scanning

Scan Channel Bandwidth 5 MHz 10 MHz 40 MHz 20 MHz

20 MHz Scan List 40 MHz Scan List

Radio Frequency 40 MHz Scan List [Unselect All](#) [Select All](#)

<input type="checkbox"/> 4930 MHz	<input type="checkbox"/> 4935 MHz	<input type="checkbox"/> 4940 MHz	<input type="checkbox"/> 4945 MHz	<input type="checkbox"/> 4950 MHz	<input type="checkbox"/> 4955 MHz	<input type="checkbox"/> 4960 MHz	<input type="checkbox"/> 4965 MHz
<input type="checkbox"/> 4970 MHz	<input type="checkbox"/> 4975 MHz	<input type="checkbox"/> 4980 MHz	<input type="checkbox"/> 4985 MHz	<input type="checkbox"/> 4990 MHz	<input type="checkbox"/> 4995 MHz	<input type="checkbox"/> 5000 MHz	<input type="checkbox"/> 5005 MHz
<input type="checkbox"/> 5010 MHz	<input type="checkbox"/> 5015 MHz	<input type="checkbox"/> 5020 MHz	<input type="checkbox"/> 5025 MHz	<input type="checkbox"/> 5030 MHz	<input type="checkbox"/> 5035 MHz	<input type="checkbox"/> 5040 MHz	<input type="checkbox"/> 5045 MHz
<input type="checkbox"/> 5050 MHz	<input type="checkbox"/> 5055 MHz	<input type="checkbox"/> 5060 MHz	<input type="checkbox"/> 5065 MHz	<input type="checkbox"/> 5070 MHz	<input type="checkbox"/> 5075 MHz	<input type="checkbox"/> 5080 MHz	<input type="checkbox"/> 5085 MHz
<input type="checkbox"/> 5090 MHz	<input type="checkbox"/> 5095 MHz	<input type="checkbox"/> 5100 MHz	<input type="checkbox"/> 5105 MHz	<input type="checkbox"/> 5110 MHz	<input type="checkbox"/> 5115 MHz	<input type="checkbox"/> 5120 MHz	<input type="checkbox"/> 5125 MHz
<input type="checkbox"/> 5130 MHz	<input type="checkbox"/> 5135 MHz	<input type="checkbox"/> 5140 MHz	<input type="checkbox"/> 5145 MHz	<input type="checkbox"/> 5150 MHz	<input type="checkbox"/> 5155 MHz	<input type="checkbox"/> 5160 MHz	<input type="checkbox"/> 5165 MHz
<input type="checkbox"/> 5170 MHz	<input type="checkbox"/> 5175 MHz	<input type="checkbox"/> 5180 MHz	<input type="checkbox"/> 5185 MHz	<input type="checkbox"/> 5190 MHz	<input type="checkbox"/> 5195 MHz	<input type="checkbox"/> 5200 MHz	<input type="checkbox"/> 5205 MHz
<input type="checkbox"/> 5210 MHz	<input type="checkbox"/> 5215 MHz	<input type="checkbox"/> 5220 MHz	<input type="checkbox"/> 5225 MHz	<input type="checkbox"/> 5230 MHz	<input type="checkbox"/> 5235 MHz	<input type="checkbox"/> 5240 MHz	<input type="checkbox"/> 5245 MHz
<input type="checkbox"/> 5250 MHz	<input type="checkbox"/> 5255 MHz	<input type="checkbox"/> 5260 MHz	<input type="checkbox"/> 5265 MHz	<input type="checkbox"/> 5270 MHz	<input type="checkbox"/> 5275 MHz	<input type="checkbox"/> 5280 MHz	<input type="checkbox"/> 5285 MHz
<input type="checkbox"/> 5290 MHz	<input type="checkbox"/> 5295 MHz	<input type="checkbox"/> 5300 MHz	<input type="checkbox"/> 5305 MHz	<input type="checkbox"/> 5310 MHz	<input type="checkbox"/> 5315 MHz	<input type="checkbox"/> 5320 MHz	<input type="checkbox"/> 5325 MHz
<input type="checkbox"/> 5330 MHz	<input type="checkbox"/> 5335 MHz	<input type="checkbox"/> 5340 MHz	<input type="checkbox"/> 5345 MHz	<input type="checkbox"/> 5350 MHz	<input type="checkbox"/> 5355 MHz	<input type="checkbox"/> 5360 MHz	<input type="checkbox"/> 5365 MHz
<input type="checkbox"/> 5370 MHz	<input type="checkbox"/> 5375 MHz	<input type="checkbox"/> 5380 MHz	<input type="checkbox"/> 5385 MHz	<input type="checkbox"/> 5390 MHz	<input type="checkbox"/> 5395 MHz	<input type="checkbox"/> 5400 MHz	<input type="checkbox"/> 5405 MHz
<input type="checkbox"/> 5410 MHz	<input type="checkbox"/> 5415 MHz	<input type="checkbox"/> 5420 MHz	<input type="checkbox"/> 5425 MHz	<input type="checkbox"/> 5430 MHz	<input type="checkbox"/> 5435 MHz	<input type="checkbox"/> 5440 MHz	<input type="checkbox"/> 5445 MHz
<input type="checkbox"/> 5450 MHz	<input type="checkbox"/> 5455 MHz	<input type="checkbox"/> 5460 MHz	<input type="checkbox"/> 5465 MHz	<input type="checkbox"/> 5470 MHz	<input type="checkbox"/> 5475 MHz	<input type="checkbox"/> 5480 MHz	<input type="checkbox"/> 5485 MHz
<input type="checkbox"/> 5490 MHz	<input type="checkbox"/> 5495 MHz	<input type="checkbox"/> 5500 MHz	<input type="checkbox"/> 5505 MHz	<input type="checkbox"/> 5510 MHz	<input type="checkbox"/> 5515 MHz	<input type="checkbox"/> 5520 MHz	<input type="checkbox"/> 5525 MHz
<input type="checkbox"/> 5530 MHz	<input type="checkbox"/> 5535 MHz	<input type="checkbox"/> 5540 MHz	<input type="checkbox"/> 5545 MHz	<input type="checkbox"/> 5550 MHz	<input type="checkbox"/> 5555 MHz	<input type="checkbox"/> 5560 MHz	<input type="checkbox"/> 5565 MHz
<input type="checkbox"/> 5570 MHz	<input type="checkbox"/> 5575 MHz	<input type="checkbox"/> 5580 MHz	<input type="checkbox"/> 5585 MHz	<input type="checkbox"/> 5590 MHz	<input type="checkbox"/> 5595 MHz	<input type="checkbox"/> 5600 MHz	<input type="checkbox"/> 5605 MHz
<input type="checkbox"/> 5610 MHz	<input type="checkbox"/> 5615 MHz	<input type="checkbox"/> 5620 MHz	<input type="checkbox"/> 5625 MHz	<input type="checkbox"/> 5630 MHz	<input type="checkbox"/> 5635 MHz	<input type="checkbox"/> 5640 MHz	<input type="checkbox"/> 5645 MHz
<input type="checkbox"/> 5650 MHz	<input type="checkbox"/> 5655 MHz	<input checked="" type="checkbox"/> 5700 MHz	<input type="checkbox"/> 5665 MHz	<input type="checkbox"/> 5670 MHz	<input type="checkbox"/> 5675 MHz	<input type="checkbox"/> 5680 MHz	<input type="checkbox"/> 5685 MHz
<input type="checkbox"/> 5690 MHz	<input type="checkbox"/> 5695 MHz	<input type="checkbox"/> 5705 MHz	<input type="checkbox"/> 5710 MHz	<input type="checkbox"/> 5715 MHz	<input type="checkbox"/> 5720 MHz	<input type="checkbox"/> 5725 MHz	<input type="checkbox"/> 5730 MHz
<input type="checkbox"/> 5730 MHz	<input type="checkbox"/> 5735 MHz	<input type="checkbox"/> 5740 MHz	<input type="checkbox"/> 5745 MHz	<input type="checkbox"/> 5750 MHz	<input type="checkbox"/> 5755 MHz	<input type="checkbox"/> 5760 MHz	<input type="checkbox"/> 5765 MHz
<input type="checkbox"/> 5770 MHz	<input type="checkbox"/> 5775 MHz	<input type="checkbox"/> 5780 MHz	<input type="checkbox"/> 5785 MHz	<input type="checkbox"/> 5790 MHz	<input type="checkbox"/> 5795 MHz	<input type="checkbox"/> 5800 MHz	<input type="checkbox"/> 5805 MHz
<input type="checkbox"/> 5810 MHz	<input type="checkbox"/> 5815 MHz	<input type="checkbox"/> 5820 MHz	<input type="checkbox"/> 5825 MHz	<input type="checkbox"/> 5830 MHz	<input type="checkbox"/> 5835 MHz	<input type="checkbox"/> 5840 MHz	<input type="checkbox"/> 5845 MHz
<input type="checkbox"/> 5850 MHz	<input type="checkbox"/> 5855 MHz						

Power Control

Transmitter Output Power dBm | min: -24 | max: 30

Antenna Gain dBi | min: 0 | max: 40

Network Entry RSSI Threshold dBm | min: -100 | max: -20

Scheduler

Distance to AP miles | min: 1 | max: 32



Advanced

RTS Threshold | min: 1 | max: 2346

© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 72: SM Radio page (Standard WiFi mode)

Table 127: SM Radio Configuration attributes (Standard WiFi mode)

Attribute	Meaning
General	
Radio Mode	This parameter controls the function of the device – All ePMP devices may be configured to operate as an Access Point (AP) , Subscriber Module (SM) , or as a Spectrum Analyzer .
Driver Mode	This parameter controls the wireless mode of operation of the SM. TDD: The SM is operating in the proprietary TDD mode and will only connect to another ePMP Access Point. Standard WiFi: The SM is operating in the Standard 802.11n WiFi mode and will be able to connect to any Access Point operating in standard 802.11n WiFi mode. ePTP Slave: The SM is operating as a Slave in point-to-point mode. The AP and the system do not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode.
Fallback Country	The SM automatically inherits the Country Code setting of the AP (except for US-locked devices). Fallback Country is used by the SM if the AP does not provide a Country Code to the SM during registration and affect the radios in the following ways: <ul style="list-style-type: none"> • Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain) • DFS operation is enabled based on the configured country code, if applicable • Frequency selection is based on local regulatory limits
Range Unit	The unit of measurement used for configuring Distance to AP .
Preferred AP List	
Preferred APs	The Preferred AP List is comprised of a list of up to 16 APs to which the SM sequentially attempts registration. For each AP configured, if authentication is required, enter a Pre-shared Key associated with the configured AP SSID .
Subscriber Module Scanning	
Scan Channel Bandwidth	Click the  button to unselect all channel bandwidths. The SM will not scan for any frequencies. Click the  button to select all channel bandwidths. The SM will scan all channel bandwidths, i.e. 5 MHz, 10 MHz, 20 MHz, and 40 MHz. Alternately choose individual channel bandwidth tabs and/or frequencies within each channel bandwidth tab for a customized scan list.

Attribute	Meaning
Power Control	
Tx Power Manual Limit	<p>Auto: The Access Point can control, using ATPC (Automatic Transmit Power Control), the TX power of the SM up to the maximum capability of the SM's transmitter (based on regulatory limits).</p> <p>Max Tx Output Power: The Access Point can control the TX power of the SM up to the value configured in the Transmitter Output Power field below.</p>
Transmitter Output Power	The SM will not transmit higher than the configured value in the field. Determines the maximum output power of the transmitter. The actual output power may be lower due to Automatic Transmit Power Control (ATPC), where the AP instructs the SM to lower its power to meet the SM target Receive Level configured on the AP.
Antenna Gain	This value represents the amount of gain introduced by the unit's internal antenna. This parameter is read-only for Integrated radios.
Network Entry RSSI Threshold	Set this parameter to the minimum Received Signal Strength Indicator (RSSI) at the SM required for the SM to attempt registration to an AP. For example, if the AP RSSI Threshold is set to -80 dBm, and the SM is receiving the AP signal at -85 dBm (RSSI = -85 dBm), the SM will not attempt to register to the AP.
Scheduler	
Distance to AP	In Standard WiFi mode, this parameter represents cell coverage radius. SMs outside the configured radius will not achieve optimal throughput. It is recommended to configure Distance to AP to match the actual physical maximum range of the farthest subscriber . This must be configured to match the range of the farthest subscriber on all SMs under the AP regardless of their respective distance from the AP.
Advanced	
RTS Threshold	Configure the RTS packet size threshold for uplink data transmission. The range is between 0-2347 octets. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold. If the packet size that the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. Otherwise, the data frame gets sent immediately.

SM Quality of Service page

The ePMP platform supports three QoS priority levels (not available in ePTP Master mode) using air fairness, priority-based starvation avoidance scheduling algorithm.

Ordering of traffic amongst the priority levels is based on a percentage of total link throughput. In other words, all priorities receive some throughput so that low priority traffic is not starved from transmission. In effect, the greatest amount of throughput is guaranteed to the VOIP priority level, then High, then Low.

Priority Level	ePMP Traffic Priority Label
Highest Priority	VOIP (only utilized when VOIP Enable is set to Enabled)
Medium Priority	High
Lowest Priority	Low

By default, all traffic passed over the air interface is low priority. The SM's Quality of Service page may be utilized to map traffic to certain priority levels using QoS classification rules. The rules included in the table are enforced starting with the first row of the table.



Caution

Each additional traffic classification rule increases device CPU utilization. Careful network traffic planning is required to efficiently use the device processor.

The ePMP platform also supports radio data rate-limiting (Maximum Information Rate, or MIR) based on the configuration of the MIR table. Operators may add up to 16 MIR profiles on the AP, each with unique limits for uplink and downlink data rates. The SM field **MIR Profile Setting** is used to configure the appropriate MIR profile for limiting the SM's data rate.

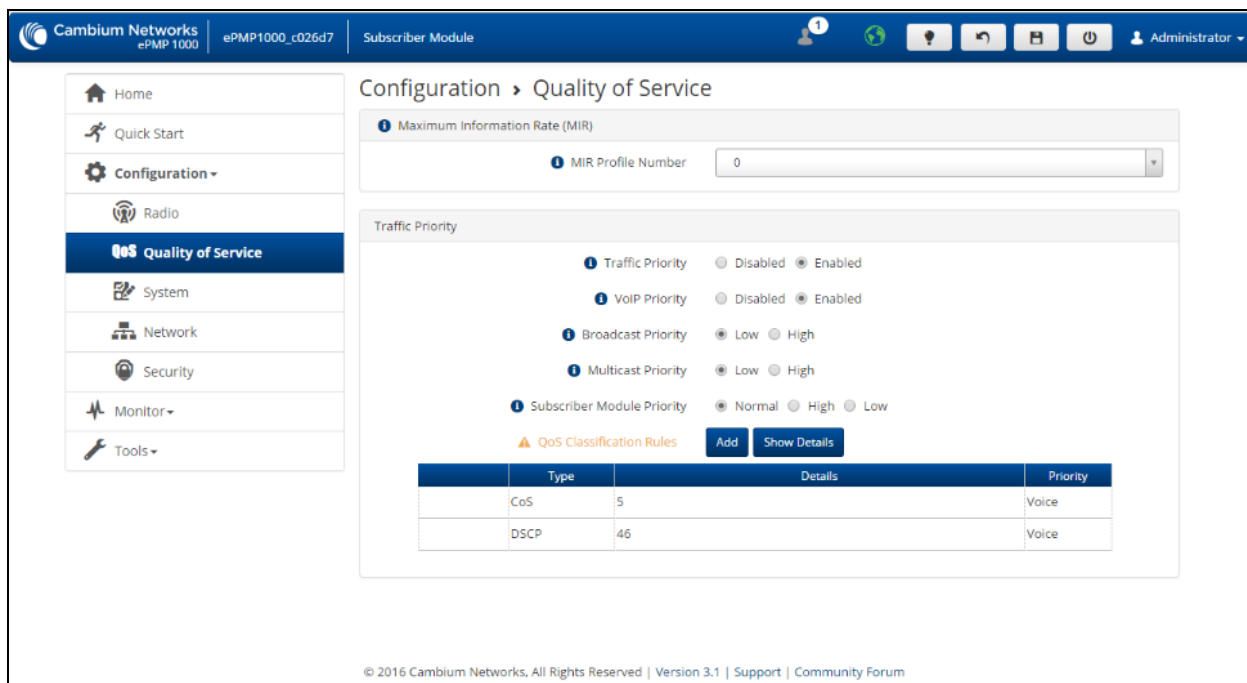


Figure 73: SM Quality of Service page

Table 128: SM Quality of Service attributes

Attribute	Meaning
Maximum Information Rate (MIR)	
MIR Profile Number	Configure the desired MIR (Maximum Information Rate) profile for SM operation. This profile must be configured on the AP else the default profile (0) is used.
Traffic Priority	
Traffic Priority	<p>Enabled: The QoS Classification Rules table is editable and is utilized by the device to classify traffic.</p> <p>Disabled: The QoS Classification Rules table is greyed-out and all traffic is sent at one priority level.</p>

Attribute	Meaning
VoIP Priority	<p>Enabled: When enabled, two entries are automatically added to the first and second rows of the QoS Classification Rules table, one with Rule Type CoS (5) and one with Rule Type DSCP (46). The addition of these rules ensures that VoIP traffic passed over the radio downlink is given the highest priority. The CoS and DSCP values may be modified to accommodate non-standard VoIP equipment.</p>
Broadcast Priority	<p>Low Priority: All Broadcast traffic sent over the uplink is prioritized as low priority and is delivered to the AP after scheduled high priority and VoIP traffic.</p> <p>High Priority: All Broadcast traffic sent over the uplink is prioritized as a high priority and is scheduled for delivery to the AP before low priority traffic but after VoIP traffic.</p>
Multicast Priority	<p>Low Priority: All Multicast traffic sent over the uplink is prioritized as low priority and is delivered to the AP after scheduled high priority and VoIP traffic.</p> <p>High Priority: All Multicast traffic sent over the uplink is prioritized as a high priority and is scheduled for delivery to the AP before low priority traffic but after VoIP traffic.</p>
Subscriber Module Priority	<p>Normal: SM gives priority to the packets as defined in the rules which could be "Low", "High", or "VoIP". "Normal" priority will allow data to be added to the appropriate "High", "Low", and "VoIP" queues based on the QoS rules. This is the default setting. If no rule is defined for a packet, then the packet priority will be "Low".</p> <p>High: SM places all data other than VoIP in the "High" queue. It will be given higher priority than SMs configured with "Low" and "Normal" when there is contention for bandwidth under the AP.</p> <p>Low: "Low" priority will place all data that is not VoIP in the "Low" priority queue. It will be given lower priority than SMs configured with "High" when there is contention for bandwidth under the same AP.</p> <p>"VoIP" queue is the highest priority queue followed by the "High" queue and then by the "Low" queue. Higher priority queues have preference over lower priority queues, but will not starve them.</p>
QoS Classification Rules	<p>The QoS Classification Rules table contains all of the rules enforced by the device when passing traffic over the radio downlink. Traffic passed through the device is matched against each rule in the table; when a match is made the traffic is sent over the radio link using the priority defined in column Traffic Priority.</p>
Type	<p>DSCP: Differentiated Services Code Point; traffic prioritization is based on the 6-bit Differentiated Services field in the IP header present in the packet entering the Ethernet port.</p> <p>CoS: Class of Service; traffic prioritization is based on the 3-bit header present in the 802.1Q VLAN-tagged Ethernet frame header in the packet entering the SM's Ethernet port.</p> <p>VLAN ID: Traffic prioritization is based on the VLAN ID of the packet entering the SM's Ethernet port.</p>

Attribute	Meaning
	<p>EtherType: Traffic prioritization is based on a 2 octet Ethertype field in the Ethernet frame entering the SM's Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame.</p> <p>IP: Traffic prioritization is based on the source and/or destination IP addresses of the packet entering the SM's Ethernet port. A subnet mask may be included to define a range of IP addresses to match.</p> <p>MAC: Traffic prioritization is based on the source and/or destination MAC addresses of the packet entering the SM's Ethernet port. A mask may be included to define a range of MAC addresses to match. The mask is made up of a hex representation of a series of 1s to start the mask and 0s that end the mask. A 1 may not follow a 0. Thus, FF:FF:FF:FF:00:00 is allowed, but FF:00:FF:FF:FF:FF is not. The MAC address is combined with the mask to define the range of allowed MAC addresses.</p>
Details	The Rule Details column is used to further configure each classification rule specified in column Rule Type .
Priority	<p>High: Traffic entering the SM's Ethernet port is prioritized as "high priority" for sending over the radio link (traffic will be sent after VOIP-classified traffic but before Low-classified traffic).</p> <p>Low: Traffic entering the SM's Ethernet port is prioritized as "low priority" for sending over the radio link (traffic will be sent after VOIP-classified and High-classified traffic is sent).</p>

SM System page

The SM's System page is used to configure system parameters, services, time settings, SNMP, and syslog.

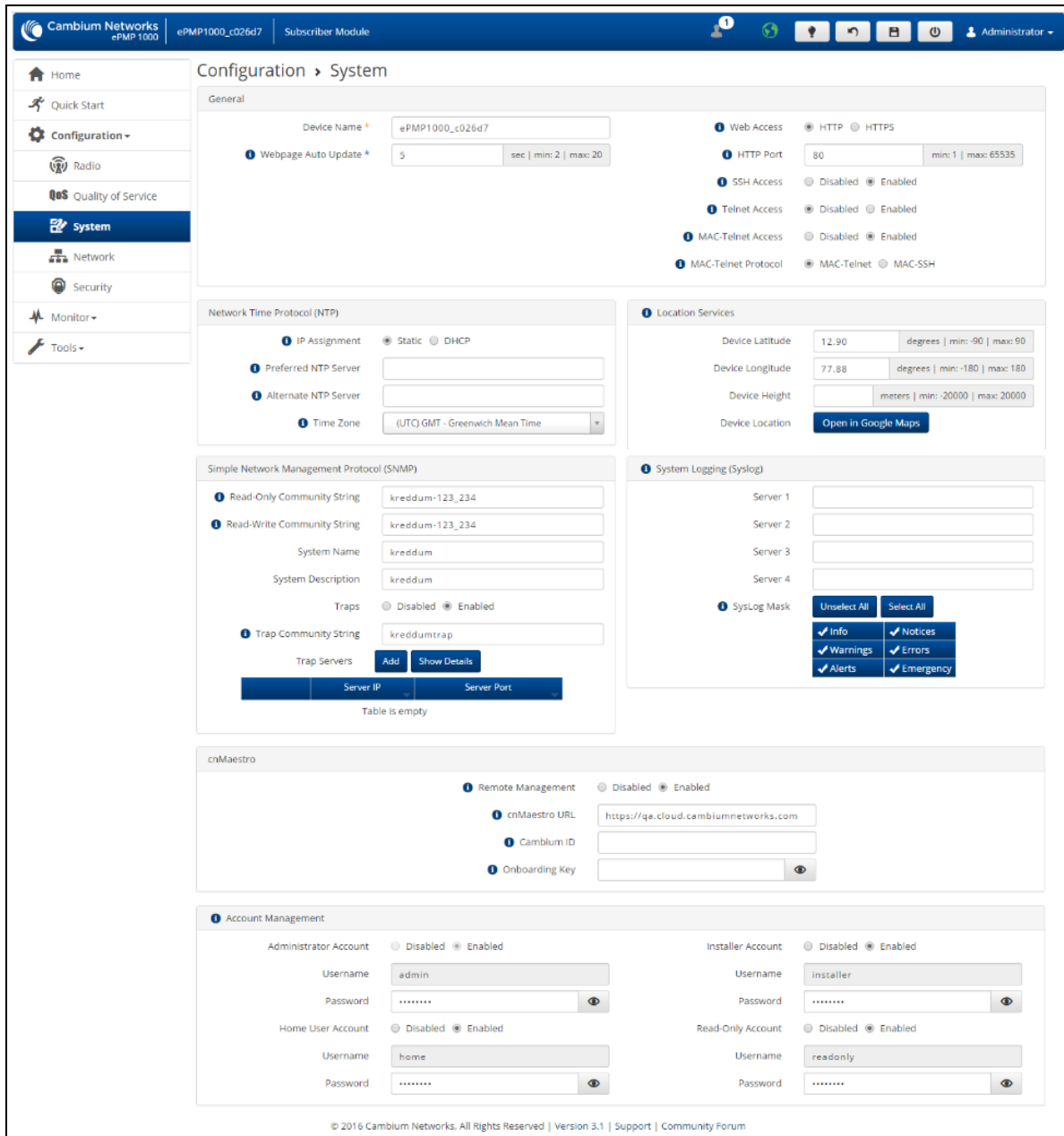




Figure 74: SM System page


Table 129: SM System attributes

Attribute	Meaning
General	
Device Name	The Device Name is used to identify the SM on the network and can be retrieved by an NMS such as the Cambium Network Services Server (CNSS).

Attribute	Meaning
Webpage Auto Update	Configure the interval for which the device retrieves system statistics for display on the management interface. For example, if this setting is configured to 5 seconds, the statistics and status parameters displayed on the management interface will be refreshed every 5 seconds (default). Webpage Auto Update is a session-only configuration change. It is updated with the <Enter> key and is not savable when using the save button.
Web Access	<p>HTTP: Access to the device management GUI is conducted via HTTP.</p> <p>HTTPS: Access to the device management GUI is conducted via HTTPS.</p>
HTTP Port	If Web Service is set to HTTP , configure the port which the device uses to service incoming HTTP requests for management GUI access.
HTTPS Port	If Web Service is set to HTTPS , configure the port which the device uses to service incoming HTTPS requests for management GUI access.
SSH Access	<p>Disabled: If the SSH port to the device is 'Disabled', access to the device through SSH is not possible.</p> <p>Enabled: If the SSH port to the device is 'Enabled', Cambium engineers can access the device through SSH which enables them to log in to the radio and troubleshoot. SSH port is 'Enabled' by default.</p>
Telnet Access	<p>Disabled: CLI access via telnet is not allowed for the device.</p> <p>Enabled: CLI access via telnet is allowed for the device.</p>
MAC-Telnet Access	<p>Disabled: Disables connections to the radio on the link layer via MAC address from RouterOS or mactelnet-enabled devices.</p> <p>Enabled: Enables connections to the radio on the link layer via MAC address from RouterOS or mactelnet-enabled devices.</p> <div data-bbox="457 1201 526 1276" style="display: inline-block; vertical-align: middle;"> </div> <div data-bbox="597 1201 1417 1344" style="border: 1px solid black; background-color: #e6f2ff; padding: 5px; margin-left: 10px;"> <p>Note</p> <p>To use MAC-Telnet the first time, the Administrator account password must be changed on the GUI or the CLI. This password can then be used for MAC-Telnet.</p> </div>
MAC-Telnet Protocol	<p>MAC-Telnet: Use the MAC-Telnet subservice for access</p> <p>MAC-SSH: Use the secured MAC-SSH sub-service for access</p>
Network Time Protocol (NTP)	
IP Assignment	<p>Static: The device retrieves NTP time data from the servers configured in fields Preferred NTP Server and Alternate NTP Server.</p> <p>DHCP: The device retrieves NTP time data from the server IP issued via a network DHCP server.</p>
Preferred NTP Server	Configure primary NTP server IP address from which the device retrieves time and date information.

Attribute	Meaning
Alternate NTP Server	Configure secondary or alternate NTP server IP address from which the device retrieves time and date information.
Time Zone	The Time Zone option may be used to offset the received NTP time to match the operator's local time zone.
Location Services	
Device Latitude	Configure Latitude information for the device in decimal format.
Device Longitude	Configure Longitude information for the device in decimal format.
Device Height	Configure the Height above sea level for the device, in meters.
Device Location	Hyperlink to display the device location on Google Maps
Simple Network Management Protocol (SNMP)	
Read-Only Community String	Specify a community string that allows a Network Management Station (NMS) such as the Cambium Networks Services Server (CNSS) to read SNMP information. No spaces are allowed in this string. This password will never authenticate an SNMP user or an NMS to read/write access. The SNMP Read-only Community String value is clear text and is readable by a packet monitor.
Read-Write Community String	Specify a community string that allows a Network Management Station (NMS) to not only read SNMP information but also write SNMP values that are defined as writeable in the radio. No spaces are allowed in this string.
System Name	Specify a string to associate with the physical module. This parameter can be polled by the Cambium Networks Services Server (CNSS) or an NMS. Special characters are supported.
System Description	Specify a description string to associate with the physical module. This parameter can be polled by the Cambium Networks Services Server (CNSS) or an NMS. Special characters are supported.
Traps	Disabled: With this setting, the radio does not send traps Enabled: Setting this enables the radio to send SNMP traps to the configured SNMP Trap Server.
Trap Community String	Specify a control string to match the Trap Community String on the SNMP Trap server. No spaces are allowed in this string.
Trap Servers	The SNMP Trap Servers table contains all of the SNMP Trap servers the radio can send SNMP traps. Configure the IP Address which the device uses to send SNMP traps.
Server IP	Specify up to four SNMP Trap Servers to which the device will send SNMP traps.
Server Port	Configure port which the device uses to send SNMP traps.
System Logging (Syslog)	
Server 1-4	Specify up to four syslog servers to which the device sends syslog messages.

Attribute	Meaning
SysLog Mask	Configure the levels of syslog messages which the devices send to the servers configured in parameters Syslog Server IP 1-4
cnMaestro	
Remote Management	When Enabled , the device will be managed by cnMaestro - the Cambium Remote Management System, which allows all Cambium devices to be managed in the cloud.
cnMaestro URL	Configure the URL of cnMaestro. The default value is https://cloud.cambiumnetworks.com .
Cambium ID	Configure the Cambium ID that the device will use for on-boarding on to cnMaestro.
Onboarding key	Configure the password/key associated with the Cambium-ID that the device will use for on-boarding on to cnMaestro.
Account Management	
(Administrator) Username	Read-only listing of available login levels. <ul style="list-style-type: none"> ADMINISTRATOR, full read-write permissions. INSTALLER, permissions to read and write parameters applicable to unit installation and monitoring. HOME USER, permissions only to access pertinent information for support purposes. READONLY, permissions only to view the Monitor page.
(Administrator) Password	Configure a custom password configuration for each user to secure the device. The password character display may be toggled using the visibility icon  .
Installer Account	Disabled: The disabled user is not granted access to the device management interface. The administrator user level cannot be disabled. Enabled: The user is granted access to the device management interface.
(Installer) Username	Read-only listing of available login levels: <ul style="list-style-type: none"> INSTALLER, permissions to read and write parameters applicable to unit installation and monitoring. HOME USER, permissions only to access pertinent information for support purposes. READONLY, permissions only to view the Monitor page.
(Installer) Password	Configure a custom password configuration for each user to secure the device. The password character display may be toggled using the visibility icon  .

Attribute	Meaning
Home User Account	<p>Disabled: The disabled user is not granted access to the device management interface. The administrator user level cannot be disabled.</p> <p>Enabled: The user is granted access to the device management interface.</p>
(Home) User Username	<p>Read-only listing of available login levels:</p> <ul style="list-style-type: none"> • HOME USER, permissions only to access pertinent information for support purposes. • READONLY, permissions only to view the Monitor page.
(Home) User Password	<p>Configure a custom password configuration for each user to secure the device.</p> <p>The password character display may be toggled using the visibility icon .</p>
Read-Only Account	<p>Disabled: The disabled user is not granted access to the device management interface. The administrator user level cannot be disabled.</p> <p>Enabled: The user is granted access to the device management interface.</p>
(Read-Only) Username	READONLY, permissions only to view the Monitor page.
(Read-Only) Password	Configure a custom password configuration for each user to secure the device.

SM Network page

The SM's **Network** page is used to configure system networking parameters and VLAN parameters. Parameter availability is based on the configuration of the **SM Network Mode** parameter.

Cambium Networks ePMP 1000 ePMP1000_SM Subscriber Module Administrator

Configuration > Network

General

Network Mode * NAT Bridge Router

Wireless IP Assignment Static DHCP

Wireless IP Address 192.168.0.2

Wireless Subnet Mask 255.255.255.0

Wireless Gateway

Preferred DNS Server

Alternate DNS Server

Wireless IPv6 Assignment Static DHCPv6

Wireless IPv6 Address

Wireless IPv6 Gateway

Ethernet Port Security Disabled Enabled

Secure MAC Limit 5 min: 1 | max: 254

MAC Aging Time 300 seconds | min: 0 | max: 1440

Ethernet Interface

IP Address 10.1.1.254

Subnet Mask 255.255.255.0

IPv6 Address

DHCP Server Disabled Enabled

DHCP Start IP 10.1.1.1 ip | min: 10.1.1.1

DHCP End IP 10.1.1.10 ip | max: 10.1.1.254

Preferred DHCP DNS Server

Alternate DHCP DNS Server

DHCP Lease Time 24 hours | min: 1 | max: 24

Separate Wireless Management Interface

Separate Management IP Disabled Enabled

IP Assignment Static DHCP

IP Address

Subnet Mask 255.255.255.0

Gateway

IPv6 Assignment Static DHCPv6

IPv6 Address

IPv6 Gateway

Separate Management VLAN Disabled Enabled

VLAN ID min: 1 | max: 4094

VLAN Priority min: 0 | max: 7

Virtual Local Area Network (VLAN)

VLAN (Management + Data) Disabled Enabled

VLAN ID 4 min: 1 | max: 4094

VLAN Priority min: 0 | max: 7

Ethernet Port

Ethernet MTU 1500 bytes | min: 576 | max: 1700

Ethernet Port Disabled Enabled

Port Setting Manual Auto-Negotiate

Auxiliary Port Disabled Enabled

Auxiliary Port Setting Manual Auto-Negotiate

Auxiliary Port PoE Disabled Enabled

Port Forwarding

UPnP IGMP Disabled Enabled

NAT PMP (PCP) Disabled Enabled

Data Port Forwarding Disabled Enabled

Point-to-Point Protocol over Ethernet (PPPoE)

PPPoE Disabled Enabled

Service Name temp

Access Concentrator Cambium

Authentication ALL PAP CHAP

Username admin

Password *****

MTU Size 1492 bytes | min: 576 | max: 1492

Keep Alive Time 10 min: 0 | max: 180

MSS Clamping Disabled Enabled

De-Militarized Zone (DMZ)

DMZ Disabled Enabled

IP Address

Advanced

IPv6 Support Disabled Enabled

Spanning Tree Protocol Disabled Enabled

DHCP Server Below SM Disabled Enabled

NAT Helper For SIP Disabled Enabled

LLDP Disabled Enabled

LLDP Mode Receive and Transmit Receive only

Figure 75: SM Network page, NAT mode

Table 130: SM Network attributes, NAT mode


Attribute	Meaning
General	
Network Mode	<p>NAT: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination).</p> <p>Bridge: The SM acts as a switch and packets are forwarded or filtered based on their MAC destination address.</p> <p>Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.</p>
Wireless IP Assignment	<p>Static: Wireless IP address is configured manually in fields Wireless IP Address, Wireless IP Subnet Mask, Wireless Gateway IP Address, Preferred DNS IP Address, and Alternate DNS IP Address.</p> <p>DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server.</p>
Wireless IP Address	Wireless Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Wireless Subnet Mask	Defines the address range of the connected IP network. For example, if Wireless IP Address is configured to 192.168.2.1 and Wireless IP Subnet Mask is configured to 255.255.255.0, the device wireless interface will belong to subnet 192.168.2.X.
Wireless Gateway	Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Preferred DNS Server	Configure The IP address of the preferred server used for DNS resolution.
Alternate DNS Server	Configure The IP address of the alternate server used for DNS resolution.
Wireless IPv6 Assignment	<p>Wireless IPv6 Assignment specifies how the IPv6 address for the wireless interface is obtained.</p> <p>Static: Device management IP addressing is configured manually in fields Wireless IPv6 Address and Wireless IPv6 Gateway.</p> <p>DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters Wireless IPv6 Address and Wireless IPv6 Gateway are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.</p>
Wireless IPv6 Address	<p>Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit (wireless interface) on a network.</p> <p>IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.</p>

Attribute	Meaning
Wireless IPv6 Gateway	Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Ethernet Port Security	<p>Disabled: When disabled, any number of devices (MAC Addresses) can connect via the SM's Ethernet (LAN) port.</p> <p>Enabled: When enabled, the number of devices (MAC Addresses) that can connect via the SM's Ethernet (LAN) port can be restricted with the fields below.</p>
Secure MAC Limit	Specify the maximum number of unique devices (MAC Addresses) that can connect via the SM's Ethernet (LAN) port. The range is 1 - 254 devices.
MAC Aging Time	Specify the aging timer in seconds. The aging timer will determine the duration for which the SM will maintain the MAC Address in its bridge table. The timer is restarted any time traffic from a specific MAC address is received on the LAN port. Once the timer expires, the MAC Address is removed from the SM's bridge table.
Ethernet Interface	
IP Address	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Subnet Mask	Defines the address range of the connected IP network. For example, if Device IP Address (LAN) is configured to 192.168.2.1 and IP Subnet Mask (LAN) is configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.
IPv6 Address	<p>Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit (Ethernet interface) on a network.</p> <p>IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.</p>
Gateway	Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
DHCP Server	<p>Disabled: Use this setting when SM is in NAT mode, if there is an existing DHCP Server below the SM handing out IP Addresses or if all devices below the SM will be configured with static IP Addresses.</p> <p>Enabled: Use this setting when SM is in NAT mode, to use the SM's local/onboard DHCP server to hand out IP addresses to its clients.</p>
DHCP Start IP	Configure the first address which will be issued to a DHCP client. Upon additional DHCP requests, the DHCP Start IP is incremented until the Local DHCP End IP is reached.
DHCP End IP	Configure the highest IP address in the DHCP pool that can be issued to a DHCP client.
Preferred DHCP DNS Server	Configure the primary DNS Server IP address which will be used to configure DHCP clients (if Local DHCP Server is set to Enabled).

Attribute	Meaning
Alternate DHCP DNS Server	Configure the secondary DNS Server IP address which will be used to configure DHCP clients (if Local DHCP Server is set to Enabled).
DHCP Lease Time	Configure the time for which a DHCP IP address is leased. When the lease time expires, the DHCP client must renew IP addresses via DHCP request.
DHCP Clients	The DHCP Client List table identifies hardware situated below the SM which shall be issued DHCP IP addressing information. The SM acts as a DHCP server, responding to requests from hardware connected to the SM.
MAC	Configure the physical address of the device which will retrieve DHCP IP addressing information from the SM.
IP	Configure the IP address which will be assigned to the device.
Name	Configure a logical name for the device configured (i.e. VoIP Phone1, or Network Camera1).
Separate Wireless Management Interface	
Separate Management IP	Disabled: When disabled, the Wireless IP is the management interface for the SM. Enabled: When enabled, the IP Address below is the management interface for the SM.
IP Assignment	Static: Separate Wireless Management Interface is configured manually in fields IP Address, Subnet Mask and Gateway. DHCP: Management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server.
IP Address	Configure the IP address that will be used to access the SM's management interface when in NAT mode. The Wireless IP (public IP) will not allow management access.
Subnet Mask	Defines the address range of the connected IP network. For example, if IP Address is configured to 192.168.2.1 and Subnet Mask is configured to 255.255.255.0, the device's wireless interface will belong to subnet 192.168.2.X.
Gateway	Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
IPv6 Assignment	IPv6 Assignment specifies how the IPv6 address for the separate wireless interface is obtained. Static: Device management IP addressing is configured manually in fields IPv6 Address and IPv6 Gateway. DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters IPv6 Address and IPv6 Gateway are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.

Attribute	Meaning
IPv6 Address	<p>Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit (separate wireless interface) on a network.</p> <p>IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.</p>
IPv6 Gateway	<p>Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.</p>
Separate Management VLAN	<p>Enabled: A VLAN configuration 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 based on the VLAN architecture. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security. When the SM is in NAT mode, the Separate Wireless Management VLAN configuration applies to management data.</p> <p>Disabled: When disabled, the SM does not have a unique management VLAN.</p>
VLAN ID	<p>Configure this parameter to include the device's management traffic on a separate VLAN network.</p>
VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. Data VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device's management data.</p> <p>This parameter only takes effect if the Separate Wireless Management VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for management traffic on the configured VLAN ID originating from the SM. The default value is 0.</p>
Virtual Local Area Management (VLAN)	
VLAN (Management + Data)	<p>Enabled: A VLAN configuration 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 based on the VLAN architecture. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security. When the SM is in NAT or Router mode, the VLAN configuration applies to both management and user data.</p> <p>Disabled: When disabled, all IP management and data traffic is allowed to the device.</p>
VLAN ID	<p>Configure this parameter to include the device's management and user traffic on a separate VLAN network.</p>
VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. Data VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device's user and management data.</p>

Attribute	Meaning
	This parameter only takes effect if the VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the configured VLAN ID originating from the SM. The default value is 0.
Ethernet Port	
Ethernet MTU	Maximum Transmission Unit; the size in bytes of the largest data unit that the device is configured to process. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Port	Disabled: The primary Ethernet port is disabled. Enabled: The primary Ethernet port is enabled.
Port Setting	Manual: The LAN Ethernet port speed and duplex mode can be manually configured. Auto-negotiate: The AP auto negotiates the LAN Ethernet port speed and duplex mode with the device connected to it.
Port Speed	With “Ethernet Port Configuration” set to Manual, the LAN Ethernet port speed can be forced to 1000 Mbps (only GPS Synchronized radio), 100 Mbps, or 10 Mbps.
Port Duplex Mode	With “Ethernet Port Configuration” set to Manual, the LAN Ethernet port duplex mode can be forced to Full or Half.
Auxiliary Port	Disabled: When disabled, the LAN Auxiliary port on the SM is shut down. Enabled: When enabled, the LAN Auxiliary port on the SM is up and able to bridge traffic with the primary Ethernet port. The default value is Enabled.
Auxiliary Port Setting	Manual: The LAN Auxiliary port speed and duplex mode can be manually configured. Auto-negotiate: The AP auto negotiates the LAN Auxiliary port speed and duplex mode with the device connected to it.
Auxiliary Port Speed	With “Auxiliary Port Configuration” set to Manual, the LAN Auxiliary port speed can be forced to 1000 Mbps (only GPS Synchronized radio), 100 Mbps, or 10 Mbps.
Auxiliary Port Duplex Mode	With “Auxiliary Port Configuration” set to Manual, the LAN Auxiliary port duplex mode can be forced to Full or Half.
Auxiliary Port PoE	Disabled: When disabled, the LAN Auxiliary port on the SM will not provide proprietary PoE out. The default value is Disabled . Enabled: When enabled, the LAN Auxiliary port on the SM will provide proprietary PoE out to power external PoE devices such as another ePMP radio or a PoE camera.
Port Forwarding	
Port Forwarding	The SM port forwarding functionality may be used to configure the SM to route external network services to an internal IP address so that end devices (situated below the SM) are reachable from external networks.

Attribute	Meaning
	 <div style="background-color: #f4a460; padding: 5px; border: 1px solid black; margin-left: 20px;"> <p>Caution</p> <p>Opening ports for forwarding may introduce a network security risk.</p> </div>
UPnP IGD	<p>Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise-class devices. With UPnP IGD and PCP protocols, ePMP will support explicit dynamic port mappings.</p> <p>Enable UPnP IGD (Internet Gateway Device) to allow the ePMP device to use the IGD profile for UPnP support.</p>
NAT PMP (PCP)	<p>The PCP (Port Control Protocol) allows an IPv6 or IPv4 host to control how incoming IPv6 or IPv4 packets are translated and forwarded by a Network Address Translator (NAT) or simple firewall, and also allows a host to optimize its outgoing NAT keepalive messages. PCP was standardized as a successor to the NAT Port Mapping Protocol (NAT-PMP), with which it shares similar protocol concepts and packet formats.</p> <p>Enable this parameter to allow the ePMP device to use PCP protocol for UPnP support.</p>
Data Port Forwarding	<p>The Data Port Forwarding Table is used to define which range of wireless ports are forwarded to a LAN (SM local network) IP address below the SM.</p>
Protocol	<p>UDP: Packet forwarding decisions are based on UDP packets.</p> <p>TCP: Packet forwarding decisions are based on TCP packets.</p>
Port Begin	<p>Configure the beginning of the range of wireless ports to match for forwarding to LAN IP.</p>
Port End	<p>Configure the end of the range of wireless ports to match for forwarding to LAN IP.</p>
Forwarding IP	<p>Configure the LAN IP of the device situated below the SM which receives the packets forwarded based on the Separate Management IP Port Forwarding Table configuration.</p>
Mapped Port	<p>Configure the port of the device situated below the SM which receives the packets forwarded based on the Data Port Forwarding Table configuration.</p>
Separate Management IP Port Forwarding	<p>The Separate Management IP Port Forwarding Table is used to define which range of wireless ports from which Management traffic on the Separate Management IP is forwarded to a LAN (SM local network) IP address below the SM.</p>
Protocol	<p>UDP: Packet forwarding decisions are based on UDP packets.</p> <p>TCP: Packet forwarding decisions are based on TCP packets.</p>
Port Begin	<p>Configure the beginning of the range of wireless ports to match for forwarding to LAN IP.</p>

Attribute	Meaning
Port End	Configure the end of the range of wireless ports to match for forwarding to LAN IP.
Forwarding IP	Configure the LAN IP of the device situated below the SM which receives the packets forwarded based on the Separate Management IP Port Forwarding Table configuration.
Mapped Port	Configure the port of the device situated below the SM which receives the packets forwarded based on the Separate Management IP Port Forwarding Table configuration.
Point-to-Point Protocol over Ethernet (PPPoE)	
PPPoE	Point-to-Point Protocol over Ethernet: Used for Encapsulating PPP frames inside Ethernet frames.
Service Name	An optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the SM accepts the first service option that comes back from the Access Concentrator specified below, if any. This is limited to 32 characters.
Access Concentrator	An optional entry to set a specific Access Concentrator to connect to for the PPPoE session. If this is blank, the SM accepts the first Access Concentrator which matches the service name (if specified). This is limited to 32 characters.
Authentication	ALL: This means that CHAP authentication will be attempted first, then PAP authentication. The same password is used for both types. CHAP: This means that CHAP authentication will be attempted. PAP: This means that PAP authentication will be attempted.
Username	This is the CHAP/PAP username that is used. This is limited to 32 characters.
Password	This is the CHAP/PAP password that is used. This is limited to 32 characters.
MTU Size	Maximum Transmission Unit; the size in bytes of the largest data unit that the device is configured to process inside the PPPoE tunnel. This field allows the operator to specify the largest MTU value to use in the PPPoE session if PPPoE MSS Clamping is Enabled. The user will be able to enter an MTU value up to 1492. However, if the MTU determined in LCP negotiations is less than this user-specified value, the SM uses the smaller value as its MTU for the PPPoE link.
Keep Alive Time	Configure the Keep Alive Time to allow the radio to keep the PPPoE session up after establishment. As an example, if this field is set to 5, the PPPoE client will send a keep-alive message to the PPPoE server every 5 seconds. If there is no acknowledgment, it sends the 'Keep alive' message to the server 4 more times (for a total of 5 times) before tearing down the PPPoE session. Setting this to 12 will mean the keep-alive message will be sent every 12 seconds and when there is no acknowledgment, the client will try for a total of 12 times every 12 seconds before tearing down the PPPoE session.
MSS Clamping	Disabled: The SM PPPoE session allows any MTU size determined by other devices in the PPPoE session during the LCP negotiations.

Attribute	Meaning
	<p>Enabled: The SM PPPoE session enforces a max MTU size determined by the PPPoE MTU Size setting for all devices in the PPPoE session during the LCP negotiations unless one of the devices enforces an MTU setting that is smaller in value.</p>
De-Militarized Zone (DMZ)	
DMZ	<p>Disabled: Packets arriving on the Wireless Interface destined for the Ethernet side of the network are dropped if a session does not exist between the Source IP (Wireless) and Destination IP (Ethernet). By default, NAT requires the sessions to be initiated from the Ethernet side before a packet is accepted from the Wireless to the Wired side."</p> <p>Enabled: Any packets with an unknown destination port (not associated to an existing session or not defined in the port forwarding rules) is automatically sent to the device configured with DMZ IP Address."</p>
IP Address	<p>Configure the IP address of an SM-connected device that is allowed to provide network services to the wide-area network.</p>
Advanced	
IPv6 Support	<p>System-wide IPv6 Protocol Support. When enabled, appropriate IPv6 modules and services will be loaded.</p>
ARP-NAT	<p>ARP-NAT or Wireless Client Bridging is a special MAC address translation mechanism. It is similar to NAT for IP networks, except it works one layer deeper. Instead of translating IP network addresses, the ePMP device translates between the MAC hardware addresses on both sides of the interface. If a device on the wired side of the router makes an ARP request for the MAC address of an IP on the wireless side, then the ePMP device forwards the request as if it came from the ePMP device. When the response comes back, it translates the address again. Instead of passing back the real MAC (which resides on the wireless network), the ePMP device gives its own wired MAC address. Then, when it receives frames for IP addresses on the wireless network, it forwards them through (conducted on both sides of the bridge).</p> <p>ARP-NAT is configured on the SM in section Configuration > Network > Advanced.</p> <div data-bbox="451 1388 516 1465" style="display: inline-block; vertical-align: middle;"> </div> <div data-bbox="581 1381 1424 1499" style="border: 1px solid black; background-color: #e6f2ff; padding: 5px; margin-left: 20px;"> <p>Note</p> <p>PPPoE Client on PCs connected to the SM is not supported and throughput decreases when the ARP-NAT feature is enabled.</p> </div>
Spanning Tree Protocol	<p>Disabled: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the SM.</p> <p>Enabled: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the SM, allowing for the prevention of Ethernet bridge loops.</p>
DHCP Server Below SM	<p>Disabled: This blocks the DHCP server connected to the SM's LAN side from handing out IP addresses to DHCP clients above the SM (wireless side).</p>

Attribute	Meaning
	<p>Enabled: This allows DHCP servers connected to the SM’s LAN side to assign IP addresses to DHCP clients above the SM (wireless side). This configuration is typical in PTP links.</p>
NAT Helper For SIP	<p>Disabled: When disabled, the SM does not perform any deep packet manipulation on the SIP request packet from a SIP Client.</p> <p>Enabled: When enabled, the SM in NAT mode replaces the Source IP within the SIP request to the Wireless IP of the SM. Please note that this translation is oftentimes handled by the SIP server so this option may not always be needed.</p>
LLDP	<p>The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol (as specified in IEEE 802.1AB) used by ePMP for advertising its identity, capabilities, and neighbors on the Ethernet/wired interface.</p> <p>Disabled: ePMP does not Receive or Transmit LLDP packets from/to its neighbors.</p> <p>Enabled: ePMP can Receive LLDP packets from its neighbors and Send LLDP packets to its neighbors, depending on the LLDP Mode configuration below.</p>
LLDP Mode	<p>Receive and Transmit: ePMP sends and receives LLDP packets to/from its neighbors on the Ethernet/LAN interface.</p> <p>Receive Only: ePMP receives LLDP packets from its neighbors on the Ethernet/LAN interface and discovers them.</p>

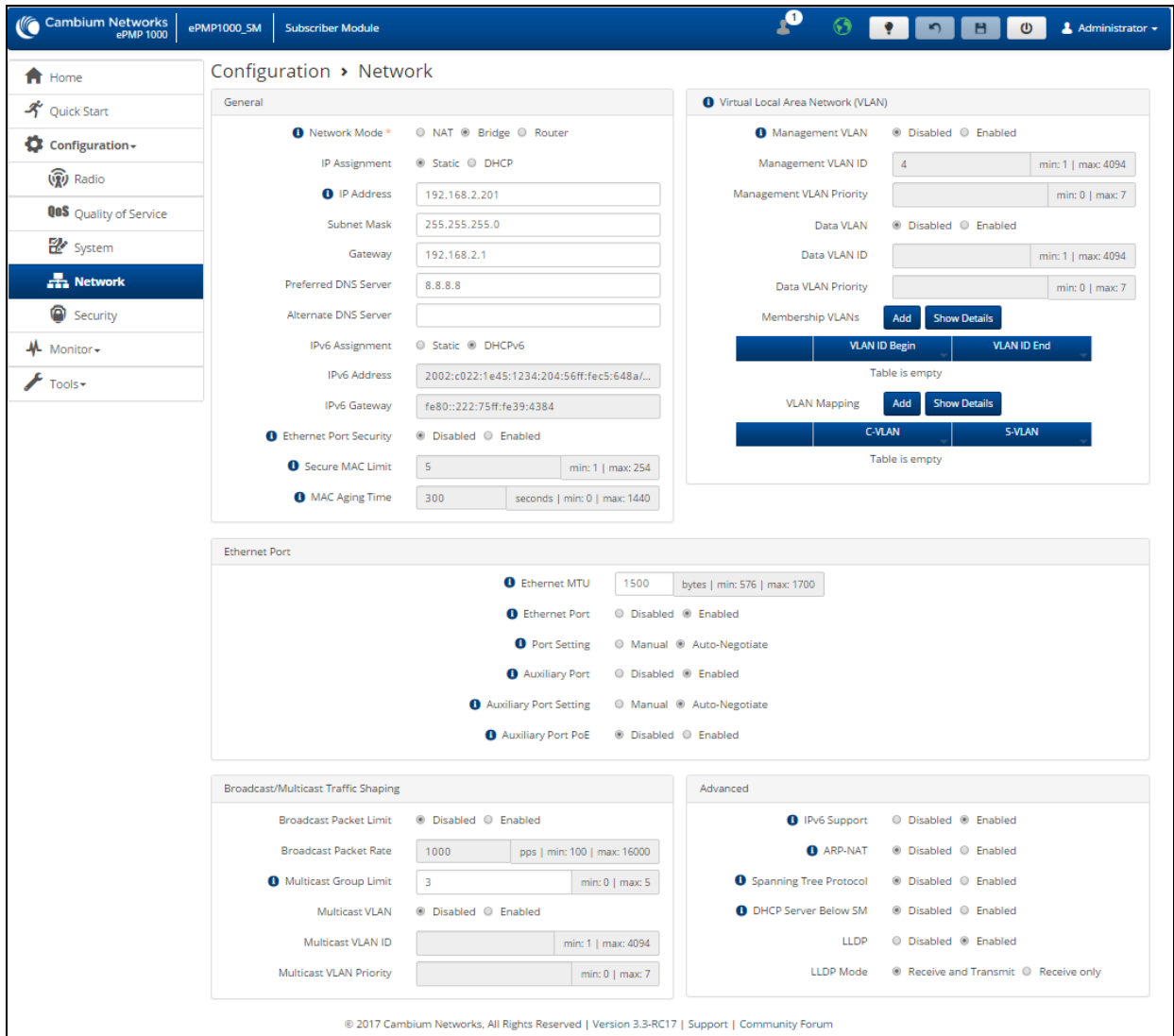





Figure 76: SM Network page, Bridge mode

Table 131: SM Network attributes, Bridge mode


Attribute	Meaning
General	
Network Mode	<p>NAT: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination).</p> <p>Bridge: The SM acts as a switch and packets are forwarded or filtered based on their MAC destination address.</p> <p>Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.</p>

Attribute	Meaning
IP Assignment	<p>Static: Device management IP addressing is configured manually in fields IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server.</p> <p>DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are unused.</p>
IP Address	<p>Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.</p> <div data-bbox="410 531 548 821" style="border: 1px solid black; padding: 5px;">  <p>Note</p> <p>If Device IP address Mode is set to DHCP and the device is unable to retrieve IP address information via DHCP, the device management IP is set to fall back to IP 192.168.0.1 (AP mode), 192.168.0.2 (SM mode), 192.168.0.3 (Spectrum Analyzer mode) or the previously-configured static Device IP Address. Units may always be accessed via the Ethernet port with IP 169.254.1.1. 169.254.1.1 is a local IP and is independent of the NAT local subnet or the wireless IP.</p> </div>
Subnet Mask	<p>Defines the address range of the connected IP network. For example, if IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.</p>
Gateway	<p>Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.</p>
Preferred DNS Server	<p>Configure the IP address of the preferred server used for DNS resolution.</p>
Alternate DNS Server	<p>Configure the IP address of the alternate server used for DNS resolution.</p>
IPv6 Assignment	<p>IPv6 Assignment specifies how the IPv6 address is obtained.</p> <p>Static: Device management IP addressing is configured manually in fields IPv6 Address and IPv6 Gateway.</p> <p>DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters IPv6 Address and IPv6 Gateway are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.</p>
IPv6 Address	<p>Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.</p> <p>IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.</p>
IPv6 Gateway	<p>Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.</p>

Attribute	Meaning
Ethernet Port Security	<p>Disabled: When disabled, any number of devices (MAC Addresses) can connect via the SM's Ethernet (LAN) port.</p> <p>Enabled: When enabled, the number of devices (MAC Addresses) that can connect via the SM's Ethernet (LAN) port can be restricted with the fields below.</p>
Secure MAC Limit	Specify the maximum number of unique devices (MAC Addresses) that can connect via the SM's Ethernet (LAN) port. The range is 1 - 254 devices.
MAC Aging Time	Specify the aging timer in seconds. The aging timer will determine the duration for which the SM will maintain the MAC Address in its bridge table. The timer is restarted any time traffic from a specific MAC address is received on the LAN port. Once the timer expires, the MAC Address is removed from the SM's bridge table.
Virtual Local Area Network (VLAN)	
Management VLAN	<p>Enabled: The SM management interface can be assigned to a Management VLAN to separate management traffic (remote module management via SNMP or HTTP) from user traffic (such as internet browsing, voice, or video). Once the management interface is enabled for a VLAN, an SM's management interface can be accessed only by packets tagged with a VLAN ID matching the management VLAN ID.</p> <p>A VLAN configuration establishes a logical group within the network. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security.</p> <p>Disabled: When disabled, all untagged IP management traffic is allowed to the device.</p>
Management VLAN ID	Configure this parameter to include the device's management traffic on a separate VLAN network. For example, if MGMT VLAN ID is set to 2, GUI access will only be allowed from frames tagged with VLAN ID 2. This parameter only takes effect if the MGMT VLAN parameter is enabled.
Management VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. MGMT VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device's management traffic.</p> <p>This parameter only takes effect if the MGMT VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the management VLAN originating from the SM. The default value is 0.</p>
Data VLAN	<p>Enabled: A VLAN tag will be added to all untagged traffic entering the SM's LAN port before sending it to the AP and remove tags in the opposite direction from traffic (tagged with Data VLAN ID) entering on the SM's WAN port before sending to the SM's LAN port.</p> <p>Disabled: When disabled, no changes are made to untagged traffic passing through the SM.</p>

Attribute	Meaning
Data VLAN ID	Configure this parameter to include this VLAN tag to all untagged traffic entering on the SM's LAN port before sending it to the AP and remove tags in the opposite direction from traffic (tagged with Data VLAN ID) entering on the SM's WAN port before sending to the SM's LAN port.
Data VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. Data VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to device user data.</p> <p>This parameter only takes effect if the Data VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the Data VLAN originating from the SM. The default value is 0.</p>
Membership VLANs	Configure the Membership VLAN Table to include the SM in one or more VLANs. When the SM receives a packet tagged from either the Ethernet (LAN) or Wireless (WAN) side with a VLAN ID which is contained in the Membership VLAN Table, the packet is forwarded and sent out to the other interface. When the SM receives a packet tagged with a VLAN ID that is not present in the Membership VLAN Table, the frame is dropped (assuming there is at least one VLAN ID present in the Membership VLAN table or configured as a Data VLAN).
VLAN ID Begin	Configure the first VLAN ID for the VLAN range.
VLAN ID End	Configure the last VLAN ID for the VLAN range.
VLAN Mapping	Configure the VLAN Mapping Table to map the C-VLAN of traffic ingressing the Ethernet (LAN) port of the SM to an S-VLAN before being forwarded to the air interface on the UL. In the DL direction, the SM will automatically un-map the S-VLAN to the C-VLAN before forwarding the tagged packets to the Ethernet (LAN) interface of the SM.
C-VLAN	<p>Configure the C-VLAN ID of the tagged traffic for which the mapping needs to occur.</p> <div style="display: flex; align-items: center;">  <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p>Note</p> <p>The C-VLAN ID must be entered in the SM VLAN Membership VLAN table.</p> </div> </div>
S-VLAN	<p>Configure the S-VLAN ID to which the tagged traffic needs to be mapped to.</p> <div style="display: flex; align-items: center;">  <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p>Note</p> <p>The S-VLAN ID must be entered in the SM VLAN Membership VLAN table.</p> </div> </div>
Ethernet Port	
Ethernet MTU	Maximum Transmission Unit; the size in bytes of the largest data unit that the device is configured to process. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Port	Disabled: The primary Ethernet port is disabled.

Attribute	Meaning
	Enabled: The primary Ethernet port is enabled.
Port Setting	Manual: The LAN Ethernet port speed and duplex mode can be manually configured. Auto-negotiate: The AP auto negotiates the LAN Ethernet port speed and duplex mode with the device connected to it.
Port Speed	With “Ethernet Port Configuration”, the LAN Ethernet port speed can be forced to 1000 Mbps (only GPS Sync'd radio), 100 Mbps, or 10 Mbps.
Port Duplex Mode	With “Ethernet Port Configuration”, the LAN Ethernet port duplex mode can be forced to Full or Half.
Auxiliary Port	Disabled: When disabled, the LAN Auxiliary port on the SM is shut down. Enabled: When enabled, the LAN Auxiliary port on the SM is up and able to bridge traffic with the primary Ethernet port. The default value is Enabled.
Auxiliary Port Setting	Manual: The LAN Auxiliary port speed and duplex mode can be manually configured. Auto-negotiate: The AP auto negotiates the LAN Auxiliary port speed and duplex mode with the device connected to it.
Auxiliary Port Speed	With “Auxiliary Port Configuration” set to Manual, the LAN Auxiliary port speed can be forced to 1000 Mbps (only GPS Synchronized radio), 100 Mbps, or 10 Mbps.
Auxiliary Port Duplex Mode	With “Auxiliary Port Configuration” set to Manual, the LAN Auxiliary port duplex mode can be forced to Full or Half.
Auxiliary Port PoE	Disabled: When disabled, the LAN Auxiliary port on the SM will not provide proprietary PoE out. The default value is Disabled. Enabled: When enabled, the LAN Auxiliary port on the SM will provide proprietary PoE out to power external PoE devices such as another ePMP radio or a PoE camera.
Broadcast/Multicast Traffic Shaping	
Broadcast Packet Limit	Enabled: This allows the user to set the Broadcast Packet Rate below. Configure this parameter to limit the number of broadcast packets that will be allowed on the ingress of the radio's Ethernet port. Set the packets per second value to limit the impact of events such as broadcast storms. Disabled: There is no limit on the amount of broadcast traffic that will be allowed into the ingress of the radio's Ethernet port.
Broadcast Packet Rate	Set the packets per second value to limit the amount of broadcast traffic that will be allowed on the ingress on the radio's Ethernet port. The packets per second limit can be set individually on each ePMP radio. The range is 100 to 16000 packets per second. The default is 1000.
Multicast Group Limit	Configure the maximum number of simultaneous multicast groups that the SM will allow from devices below it. The default is 3.
Multicast VLAN	Enabled: A VLAN tag will be added to all untagged multicast traffic entering the SM's LAN port before sending it to the AP and remove tags in the opposite direction from traffic (tagged with Multicast VLAN ID) entering on the SM's WAN port before sending to the SM's LAN port.

Attribute	Meaning
	Disabled: When disabled, no changes are made to untagged multicast traffic passing through the SM.
Multicast VLAN ID	Configure this parameter to include this VLAN tag to all untagged multicast traffic entering on the SM's LAN port before sending it to the AP and remove tags in the opposite direction from multicast traffic (tagged with Multicast VLAN ID) entering on the SM's WAN port before sending to the SM's LAN port.
Multicast VLAN Priority	ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. Multicast VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device's multicast data. This parameter only takes effect if the Multicast VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the Multicast VLAN originating from the SM. The default value is 0.
Advanced	
Spanning Tree Protocol	Disabled: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the SM. Enabled: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the SM, allowing for the prevention of Ethernet bridge loops.
DHCP Servers Below SM	Disabled: This blocks the DHCP server connected to the SM's LAN side from handing out IP addresses to DHCP clients above the SM (wireless side). Enabled: This allows DHCP servers connected to the SM's LAN side to assign IP addresses to DHCP clients above the SM (wireless side). This configuration is typical in PTP links.
NAT Helper For SIP	Disabled: When disabled, the SM does not perform any deep packet manipulation on the SIP request packet from a SIP Client. Enabled: When enabled, the SM in NAT mode replaces the Source IP within the SIP request to the Wireless IP of the SM. Please note that this translation is oftentimes handled by the SIP server so this option may not always be needed.
LLDP	The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol (as specified in IEEE 802.1AB) used by ePMP for advertising its identity, capabilities, and neighbors on the Ethernet/wired interface. Disabled: ePMP does not Receive or Transmit LLDP packets from/to its neighbors. Enabled: ePMP can Receive LLDP packets from its neighbors and Send LLDP packets to its neighbors, depending on the LLDP Mode configuration below.  Note LLDP packets are Received/Transmitted ONLY to the neighbors on the Ethernet Interface of the ePMP radio.
LLDP Mode	Receive and Transmit: ePMP sends and receives LLDP packets to/from its neighbors on the Ethernet/LAN interface.

Attribute	Meaning
	Receive Only: ePMP receives LLDP packets from its neighbors on the Ethernet/LAN interface and discovers them.

Cambium Networks ePMP 1000 ePMP1000_c026d7 Subscriber Module Administrator

Configuration > Network

General

- Network Mode: NAT Bridge Router
- Wireless IP Assignment: Static DHCP
- Wireless IP Address:
- Wireless Subnet Mask:
- Wireless Gateway:
- Preferred DNS Server:
- Alternate DNS Server:
- Ethernet Port Security: Disabled Enabled
- Secure MAC Limit: min: 1 | max: 254
- MAC Aging Time: seconds | min: 0 | max: 1440

Ethernet interface

- IP Address:
- Subnet Mask:
- DHCP Server: Disabled Enabled
- DHCP Start IP: ip | min: 10.1.1.1
- DHCP End IP: ip | max: 10.1.1.254
- Preferred DHCP DNS Server:
- Alternate DHCP DNS Server:
- DHCP Lease Time: hours | min: 1 | max: 24

DHCP Clients:

MAC	IP
Table is empty	

Static Routes

Static Routes: Disabled Enabled

IP Aliases

IP Aliases: Disabled Enabled

Separate Wireless Management Interface

- Separate Management IP: Disabled Enabled
- IP Assignment: Static DHCP
- IP Address:
- Subnet Mask:
- Gateway:
- Separate Management VLAN: Disabled Enabled
- VLAN ID: min: 1 | max: 4094
- VLAN Priority: min: 0 | max: 7

Virtual Local Area Network (VLAN)

- VLAN (Management + Data): Disabled Enabled
- VLAN ID: min: 1 | max: 4094
- VLAN Priority: min: 0 | max: 7

Ethernet Port

- Ethernet MTU: bytes | min: 576 | max: 1700
- Ethernet Port: Disabled Enabled
- Port Setting: Manual Auto-Negotiate
- Auxiliary Port: Disabled Enabled
- Auxiliary Port Setting: Manual Auto-Negotiate
- Auxiliary Port PoE: Disabled Enabled

Point-to-Point Protocol over Ethernet (PPPoE)

- PPPoE: Disabled Enabled
- Service Name:
- Access Concentrator:
- Authentication: ALL PAP CHAP
- Username:
- Password:
- MTU Size: bytes | min: 576 | max: 1492
- Keep Alive Time: min: 0 | max: 180
- MSS Clamping: Disabled Enabled

Advanced

- Spanning Tree Protocol: Disabled Enabled
- DHCP Server Below SM: Disabled Enabled
- NAT Helper For SIP: Disabled Enabled
- LLDP: Disabled Enabled
- LLDP Mode: Receive and Transmit Receive only


© 2016 Cambium Networks, All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 77: SM Network page, Router mode

Table 132: SM Network attributes, Router mode


Attribute	Meaning
General	
Network Mode	<p>NAT: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination).</p> <p>Bridge: The SM acts as a switch and packets are forwarded or filtered based on their MAC destination address.</p> <p>Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.</p>
Wireless IP Assignment	<p>Static: Wireless IP address is configured manually in fields Wireless IP Address, Wireless IP Subnet Mask, Wireless Gateway IP Address, Preferred DNS IP Address, and Alternate DNS IP Address.</p> <p>DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server.</p>
Wireless IP Address	Wireless Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Wireless Subnet Mask	Defines the address range of the connected IP network. For example, if Wireless IP Address is configured to 192.168.2.1 and Wireless IP Subnet Mask is configured to 255.255.255.0, the device wireless interface will belong to subnet 192.168.2.X.
Wireless Gateway	Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Preferred DNS Server	Configure The IP address of the preferred server used for DNS resolution.
Alternate DNS Server	Configure The IP address of the alternate server used for DNS resolution.
Ethernet Port Security	<p>Disabled: When disabled, any number of devices (MAC Addresses) can connect via the SM's Ethernet (LAN) port.</p> <p>Enabled: When enabled, the number of devices (MAC Addresses) that can connect via the SM's Ethernet (LAN) port can be restricted with the fields below.</p>
Secure MAC Limit	Specify the maximum number of unique devices (MAC Addresses) that can connect via the SM's Ethernet (LAN) port. The range is 1 - 254 devices.
MAC Aging Time	Specify the aging timer in seconds. The aging timer will determine the duration for which the SM will maintain the MAC Address in its bridge table. The timer is restarted any time traffic from a specific MAC address is received on the LAN port. Once the timer expires, the MAC Address is removed from the SM's bridge table.
Ethernet Interface	

Attribute	Meaning
IP Address	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Subnet Mask	Defines the address range of the connected IP network. For example, if Device IP Address (LAN) is configured to 192.168.2.1 and IP Subnet Mask (LAN) is configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.
DHCP Server	<p>Disabled: Use this setting when SM is in NAT mode, if there is an existing DHCP Server below the SM handing out IP Addresses or if all devices below the SM will be configured with static IP Addresses.</p> <p>Enabled: Use this setting when SM is in NAT mode, to use the SM's local/onboard DHCP server to hand out IP addresses to its clients.</p>
DHCP Start IP	Configure the first address which will be issued to a DHCP client. Upon additional DHCP requests, the DHCP Start IP is incremented until the Local DHCP End IP is reached.
DHCP End IP	Configure the highest IP address in the DHCP pool that can be issued to a DHCP client.
Preferred DHCP DNS Server	Configure the primary DNS Server IP address which will be used to configure DHCP clients (if Local DHCP Server is set to Enabled).
Alternate DHCP DNS Server	Configure the secondary DNS Server IP address which will be used to configure DHCP clients (if Local DHCP Server is set to Enabled).
DHCP Lease Time	Configure the time for which a DHCP IP address is leased. When the lease time expires, the DHCP client must renew IP addresses via DHCP request.
DHCP Clients	The DHCP Client List table identifies hardware situated below the SM which shall be issued DHCP IP addressing information. The SM acts as a DHCP server, responding to requests from hardware connected to the SM.
MAC	Configure the physical address of the device which will retrieve DHCP IP addressing information from the SM.
IP	Configure the IP address which will be assigned to the device.
Name	Configure a logical name for the device configured (i.e. VoIP Phone1, or Network Camera1).
Static Routes	
Route	<p>When Enabled, it allows the operator to create static routes that will apply to both the Wireless and Ethernet interface of the SM.</p> <p>This allows operators to configure a custom table of explicit paths between networks. Static routing is often used as a method to reduce the overhead of processing dynamic routes through a network when the specific path is known (or, it is simpler to define a specific path). Static routing is also used as a backup when dynamic routing protocols fail to complete a route from one network to another.</p> <p>In router mode, the Static Routes table is referenced by the SM to forward/filter packets to a particular destination configured by the user based on the IP addressing information contained in the table.</p>

Attribute	Meaning
	<p>Since static routes do not change with network changes, it is recommended to only use static routes for simple network paths which are not prone to frequent changes (requiring updates to the routes configured on the ePMP SM).</p> <p>It is important to consider each hop in a static route's path to ensure that the routing equipment has been configured to statically or dynamically route packets to the proper destination. Otherwise, the network communication will fail.</p> <div style="display: flex; align-items: center;">  <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px;"> <p>Note</p> <p>Network Address Translation (NAT) is not performed when the SM is in Router mode.</p> </div> </div>
Target Network IP	Configure the target subnet/network's IP address to which the SM should route the packets.
Subnet Mask	Configure the subnet mask for the Target Network IP address.
Gateway	Configure the gateway to which packets that match the Target Network IP Address and Subnet Mask are sent.
Description	Provide a description to easily identify the static route and its purpose.
Separate Wireless Management Interface	
Separate Management IP	<p>Disabled: When disabled, the Wireless IP is the management interface for the SM.</p> <p>Enabled: When enabled, the IP Address below is the management interface for the SM.</p>
IP Assignment	<p>Static: Separate Wireless Management Interface is configured manually in fields IP Address, Subnet Mask and Gateway.</p> <p>DHCP: Management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server.</p>
IP Address	Configure the IP address that will be used to access the SM's management interface when in NAT mode. The Wireless IP (public IP) will not allow management access.
Subnet Mask	Defines the address range of the connected IP network. For example, if IP Address is configured to 192.168.2.1 and Subnet Mask is configured to 255.255.255.0, the device's wireless interface will belong to subnet 192.168.2.X.
Gateway	Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Separate Management VLAN	<p>Enabled: A VLAN configuration 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 based on the VLAN architecture. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security. When the SM is in NAT mode, the Separate Wireless Management VLAN configuration applies to management data.</p> <p>Disabled: When disabled, the SM does not have a unique management VLAN.</p>

Attribute	Meaning
VLAN ID	Configure this parameter to include the device's management traffic on a separate VLAN network.
VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. Data VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device's management data.</p> <p>This parameter only takes effect if the Separate Wireless Management VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for management traffic on the configured VLAN ID originating from the SM. The default value is 0.</p>
Virtual Local Area Management (VLAN)	
VLAN (Management + Data)	<p>Enabled: A VLAN configuration 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 based on the VLAN architecture. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security. When the SM is in NAT or Router mode, the VLAN configuration applies to both management and user data.</p> <p>Disabled: When disabled, all IP management and data traffic is allowed to the device.</p>
VLAN ID	Configure this parameter to include the device's management and user traffic on a separate VLAN network.
VLAN Priority	<p>ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. Data VLAN Priority represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to the device's user and management data.</p> <p>This parameter only takes effect if the VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the configured VLAN ID originating from the SM. The default value is 0.</p>
IP Aliases	
IP aliases	<p>When Enabled, IP aliases allow the operator to associate more than one IP address to the Ethernet interface of the SM.</p> <p>This configuration of multiple IP addresses for the SM's Ethernet interface allows connections to multiple networks, often used as a mechanism for management access to the device from a convenient networking path.</p>
IP Address	Configure the IP address for the alias.
Subnet Mask	Configure the subnet mask for the alias.
Description	Provide a description to easily identify the IP alias and its purpose/connected network.
Ethernet Port	

Attribute	Meaning
Ethernet MTU	Maximum Transmission Unit; the size in bytes of the largest data unit that the device is configured to process. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Port	Disabled: The primary Ethernet port is disabled Enabled: The primary Ethernet port is enabled
Port Setting	Manual: The LAN Ethernet port speed and duplex mode can be manually configured. Auto-negotiate: The AP auto negotiates the LAN Ethernet port speed and duplex mode with the device connected to it.
Port Speed	With “Ethernet Port Configuration” set to Manual, the LAN Ethernet port speed can be forced to 1000 Mbps (only GPS Synchronized radio), 100 Mbps, or 10 Mbps.
Port Duplex Mode	With “Ethernet Port Configuration” set to Manual, the LAN Ethernet port duplex mode can be forced to Full or Half.
Auxiliary Port	Disabled: When disabled, the LAN Auxiliary port on the SM is shut down. Enabled: When enabled, the LAN Auxiliary port on the SM is up and able to bridge traffic with the primary Ethernet port. The default value is Enabled.
Auxiliary Port Configuration	Manual: The LAN Auxiliary port speed and duplex mode can be manually configured. Auto-negotiate: The AP auto negotiates the LAN Auxiliary port speed and duplex mode with the device connected to it.
Auxiliary Port Speed	With “Auxiliary Port Configuration” set to Manual, the LAN Auxiliary port speed can be forced to 1000 Mbps (only GPS Synchronized radio), 100 Mbps, or 10 Mbps.
Auxiliary Port Duplex Mode	With “Auxiliary Port Configuration” set to Manual, the LAN Auxiliary port duplex mode can be forced to Full or Half.
Auxiliary Port PoE	Disabled: When disabled, the LAN Auxiliary port on the SM will not provide proprietary PoE out. The default value is Disabled. Enabled: When enabled, the LAN Auxiliary port on the SM will provide proprietary PoE out to power external PoE devices such as another ePMP radio or a PoE camera.
Advanced	
Spanning Tree Protocol	Disabled: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the SM. Enabled: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the SM, allowing for the prevention of Ethernet bridge loops.
DHCP Servers Below SM	Disabled: This blocks the DHCP server connected to the SM’s LAN side from handing out IP addresses to DHCP clients above the SM (wireless side).

Attribute	Meaning
	Enabled: This allows DHCP servers connected to the SM's LAN side to assign IP addresses to DHCP clients above the SM (wireless side). This configuration is typical in PTP links.
NAT Helper For SIP	Disabled: When disabled, the SM does not perform any deep packet manipulation on the SIP request packet from a SIP Client. Enabled: When enabled, the SM in NAT mode replaces the Source IP within the SIP request to the Wireless IP of the SM. Please note that this translation is oftentimes handled by the SIP server so this option may not always be needed.
LLDP	The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol (as specified in IEEE 802.1AB) used by ePMP for advertising its identity, capabilities, and neighbors on the Ethernet/wired interface. Disabled: ePMP does not Receive or Transmit LLDP packets from/to its neighbors. Enabled: ePMP can Receive LLDP packets from its neighbors and Send LLDP packets to its neighbors, depending on the LLDP Mode configuration below.  Note LLDP packets are Received/Transmitted ONLY to the neighbors on the Ethernet Interface of the ePMP radio.
LLDP Mode	Receive and Transmit: ePMP sends and receives LLDP packets to/from its neighbors on the Ethernet/LAN interface. Receive Only: ePMP receives LLDP packets from its neighbors on the Ethernet/LAN interface and discovers them.
Point-to-Point Protocol over Ethernet (PPPoE)	
PPPoE	Point-to-Point Protocol over Ethernet: Used for Encapsulating PPP frames inside Ethernet frames.
Service Name	An optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the SM accepts the first service option that comes back from the Access Concentrator specified below, if any. This is limited to 32 characters.
Access Concentrator	An optional entry to set a specific Access Concentrator to connect to for the PPPoE session. If this is blank, the SM accepts the first Access Concentrator which matches the service name (if specified). This is limited to 32 characters.
Authentication	ALL: This means that CHAP authentication will be attempted first, then PAP authentication. The same password is used for both types. CHAP: This means that CHAP authentication will be attempted. PAP: This means that PAP authentication will be attempted.
Username	This is the CHAP/PAP username that is used. This is limited to 32 characters.
Password	This is the CHAP/PAP password that is used. This is limited to 32 characters.

Attribute	Meaning
MTU Size	Maximum Transmission Unit; the size in bytes of the largest data unit that the device is configured to process inside the PPPoE tunnel. This field allows the operator to specify the largest MTU value to use in the PPPoE session if PPPoE MSS Clamping is Enabled. The user will be able to enter an MTU value up to 1492. However, if the MTU determined in LCP negotiations is less than this user-specified value, the SM uses the smaller value as its MTU for the PPPoE link.
Keep Alive Time	Configure the Keep Alive Time to allow the radio to keep the PPPoE session up after establishment. As an example, if this field is set to 5, the PPPoE client will send a keep-alive message to the PPPoE server every 5 seconds. If there is no acknowledgment, it sends the 'Keep alive' message to the server 4 more times (for a total of 5 times) before tearing down the PPPoE session. Setting this to 12 will mean the keep-alive message will be sent every 12 seconds and when there is no acknowledgment, the client will try for a total of 12 times every 12 seconds before tearing down the PPPoE session.
MSS Clamping	<p>Disabled: The SM PPPoE session allows any MTU size determined by other devices in the PPPoE session during the LCP negotiations.</p> <p>Enabled: The SM PPPoE session enforces a max MTU size determined by the PPPoE MTU Size setting for all devices in the PPPoE session during the LCP negotiations unless one of the devices enforces an MTU setting that is smaller in value.</p>

SM Security page

The SM's **Security** page is used to configure system security features including SM authentication and Layer2/Layer3 Firewall rules.



Caution

If a device firewall rule is added with **Action** set to **Deny** and **Interface** set to **LAN** or **WAN** and no other rule attribute are configured, the device will drop all Ethernet or wireless traffic, respectively. Ensure that all firewall rules are specific to the type of traffic which must be denied and that no rules exist in the devices with the only **Action** set to **Deny** and **Interface** set to **LAN** or **WAN**. To regain access to the device, perform a factory default.

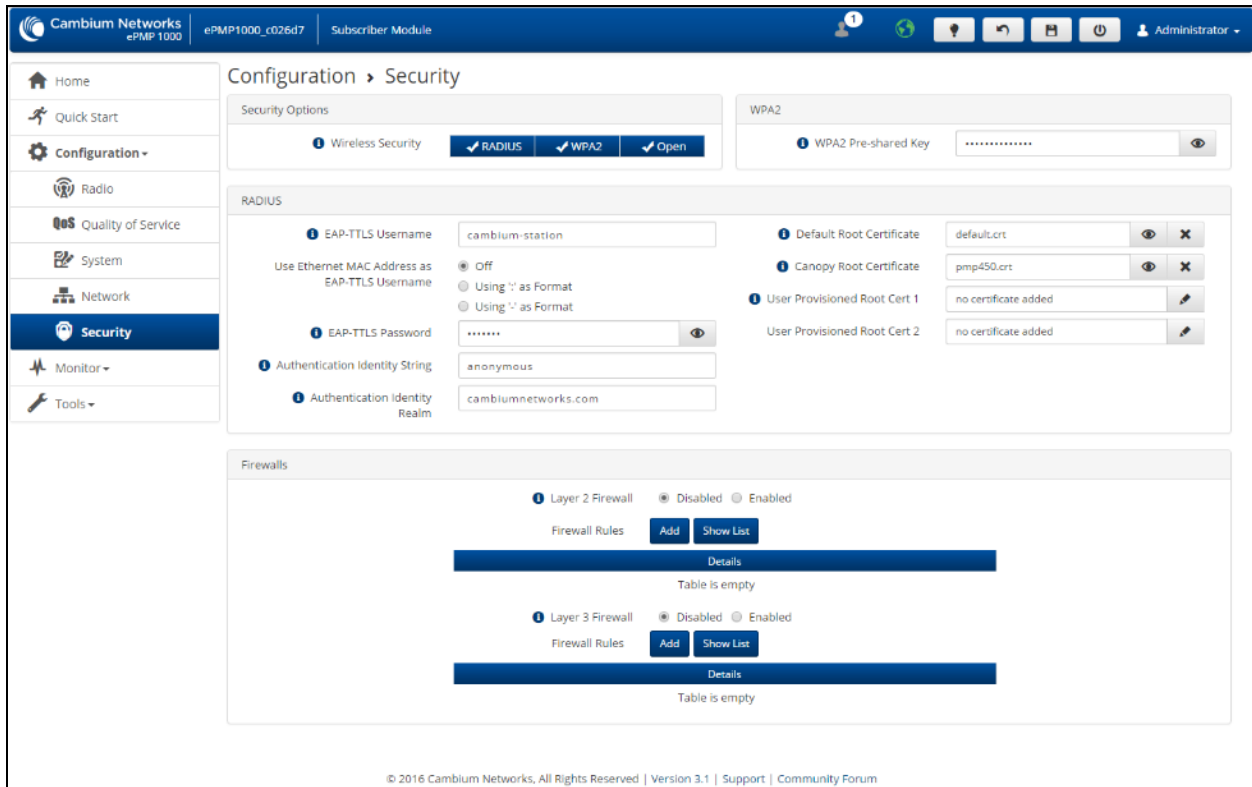



Figure 78: SM Security page

Table 133: SM Security attributes

Attribute	Meaning
Security Options	
Wireless Security	Select the type of authentication preferred, whether RADIUS, WPA2, Open, or a combination of the three.
WPA2	
WPA2 Pre-shared Key	Configure this key on the AP and then configure each of the network SMs with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.
RADIUS	
EAP-TTLS Username	Configure the EAP-TTLS Username to match the credentials on the RADIUS server being used for the network.
Use Ethernet MAC Address at EAP-TTLS Username	The device MAC Address can be used as the EAP-TTLS Username in either “:” or “-” delimited format.
EAP-TTLS Password	Configure the EAP-TTLS Password to match the credentials on the RADIUS server being used for the network.

Attribute	Meaning
Authentication Identity String	Configure this Identity string to match the credentials on the RADIUS server being used for the network. The default value for this parameter is “anonymous”.
Authentication Identity Realm	Configure this Identity string to match the credentials on the RADIUS server being used for the network. The default value for this parameter is “cambiumnetworks.com”.
Default Root Certificate	Default EAP-TTLS root certificate that must match the certificate on the RADIUS server.
Canopy Root Certificate	PMP 450 default EAP-TTLS root certificate to match the certificate on the RADIUS server used with current PMP 450 installations.
User Provisioned Root Cert 1	Import a user certificate if a certificate different from the default certificates is needed.
User Provisioned Root Cert 2	Import a second user certificate if a certificate different from the default or 1 st user provisioned certificate is needed.
Firewalls	
Layer 2 Firewall	<p>Enabled: Modifications to the Layer 2 Firewall Table are allowed and rules are enforced.</p> <p>Disabled: Modifications to the Layer 2 Firewall Table are not allowed and rules are not enforced.</p>
Firewall Rules	<p>The Layer 2 firewall table may be used to configure rules matching layer 2 (MAC layer) traffic which results in forwarding or dropping the traffic over the radio link or Ethernet interface.</p> <div style="display: flex; align-items: center;">  <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p>Note</p> <p>When the SM is in NAT mode, only the Src MAC filtering functionality is supported.</p> </div> </div>
Layer 3 Firewall	<p>Disabled: Modifications to the Layer 3 Firewall Table are not allowed and rules are not enforced.</p> <p>Enabled: Modifications to the Layer 3 Firewall Table are allowed and rules are enforced.</p>
Firewall Rules	The Layer 3 firewall table may be used to configure rules matching layer 3 (IP layer) traffic which results in forwarding or dropping the traffic over the radio link or Ethernet interface.

SM Monitor menu

Use the **Monitor** menu to access device and network statistics and status information. This section may be used to analyze and troubleshoot network performance and operation.

The **Monitor** menu contains the following pages:

- [SM Performance page](#)
- [SM System page](#)

- [SM Wireless page](#)
- [SM Throughput Chart page](#)
- [SM Network page](#)
- [SM System Log page](#)

SM Performance page

Use the Performance page to monitor system status and statistics to analyze and troubleshoot network performance and operation.

The screenshot shows the Performance page for a Cambium Networks ePMP1000_SM Subscriber Module. The page is divided into several sections:

- Monitor > Performance**: Includes a 'Reset Statistics' button and 'Time Since Last Reset' (0000:00:03:42).
- Ethernet Statistics - Transmitted**:

Total Traffic	0 Kbits
Total Packets	0
Packet Errors	0
Packet Drops	0
Multicast / Broadcast Traffic	0 Kbits
Broadcast Packets	0
Multicast Packets	0
- Ethernet Statistics - Received**:

Total Traffic	0 Kbits
Total Packets	0
Packet Errors	0
Packet Drops	0
Multicast / Broadcast Traffic	0 Kbits
Broadcast Packets	0
Multicast Packets	0
- Wireless Statistics - Downlink**:

Total Traffic	1179 Kbits
Total Packets	711
Error Drop Packets	0
Multicast / Broadcast Traffic	440 Kbit
Broadcast Packets	17
Multicast Packets	135
- Wireless Statistics - Uplink**:

Total Traffic	11652 Kbits
Total Packets	1208
Error Drop Packets	0
Capacity Drop Packets	0
Retransmission Packets	0
Multicast / Broadcast Traffic	15 Kbits
Broadcast Packets	15
Multicast Packets	10
Link Quality (Uplink)	100 %
Link Capacity (Uplink)	30 %
- QoS Statistics**:
 - TDD Voice Priority queue**:

Total count of transmitted packets	0
Total count of received packets	0
Total count of dropped packets	0
 - TDD Low Priority queue**:

Total count of transmitted packets	61
Total count of received packets	61
Total count of dropped packets	0
 - TDD High Priority queue**:

Total count of transmitted packets	0
Total count of received packets	0
Total count of dropped packets	0
 - TDD QoS queues**:

Total count of transmitted packets	68
Total count of received packets	68
Total count of dropped packets	0
- System Statistics**:

Session Drops	1
Device Reboots	123
Radar (DFS) Detections	0
- Downlink Packets Per MCS**:

MCS 15 - 64-QAM 5/6	0 (0%)
MCS 14 - 64-QAM 3/4	10 (1.2%)
MCS 13 - 64-QAM 2/3	64 (7.9%)
MCS 12 - 16-QAM 3/4	73 (9%)
MCS 11 - 16-QAM 1/2	114 (14.1%)
MCS 10 - QPSK 3/4	93 (11.5%)
MCS 9 - QPSK 1/2	72 (8.9%)
MCS 7 - 64-QAM 5/6	65 (8%)
MCS 6 - 64-QAM 3/4	57 (7%)
MCS 5 - 64-QAM 2/3	3 (0.4%)
MCS 4 - 16-QAM 3/4	3 (0.4%)
MCS 3 - 16-QAM 1/2	2 (0.2%)
MCS 2 - QPSK 3/4	25 (3.1%)
MCS 1 - QPSK 1/2	228 (28.2%)
- Uplink Packets Per MCS**:

MCS 15 - 64-QAM 5/6	0 (0%)
MCS 14 - 64-QAM 3/4	0 (0%)
MCS 13 - 64-QAM 2/3	0 (0%)
MCS 12 - 16-QAM 3/4	152 (11.6%)
MCS 11 - 16-QAM 1/2	295 (22.6%)
MCS 10 - QPSK 3/4	236 (18%)
MCS 9 - QPSK 1/2	167 (12.8%)
MCS 7 - 64-QAM 5/6	162 (12.4%)
MCS 6 - 64-QAM 3/4	173 (13.2%)
MCS 5 - 64-QAM 2/3	10 (0.8%)
MCS 4 - 16-QAM 3/4	9 (0.7%)
MCS 3 - 16-QAM 1/2	6 (0.5%)
MCS 2 - QPSK 3/4	65 (5%)
MCS 1 - QPSK 1/2	33 (2.5%)

Figure 79: SM Performance page

Table 134: SM Performance attributes

Attribute	Meaning
Time Since Last Reset	Time since the stats were last reset.
Reset Stats	Resets all statistics for both Ethernet and Wireless.
Ethernet Statistics - Transmitted	
Total Traffic	Total amount of traffic in Kbits transferred from the SM's Ethernet interface.
Total Packets	Total number of packets transferred from the SM's Ethernet interface.
Packet Errors	Total number of packets transmitted out of the SM's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	Total number of packets dropped before sending out of the SM's Ethernet interface due to Ethernet setup or filtering issues.
Multicast / Broadcast Traffic	Total amount of multicast and broadcast traffic in Kbits sent via the SM's Ethernet interface.
Broadcast Packets	Total number of broadcast packets sent via the SM's Ethernet interface.
Multicast Packets	Total number of multicast packets sent via the SM's Ethernet interface.
Ethernet Statistics - Received	
Total Traffic	Total amount of traffic in Kbits received by the SM's Ethernet interface.
Total Packets	Total number of packets received by the SM's Ethernet interface.
Packet Errors	Total number of packets received by the SM's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	Total number of packets dropped before sending out of the SM's wireless interface due to Ethernet setup or filtering issues.
Multicast / Broadcast Traffic	Total amount of multicast and broadcast traffic in Kbits received by the SM's Ethernet interface.
Broadcast Packets	Total number of broadcast packets received via the SM's Ethernet interface.
Multicast Packets	Total number of multicast packets received via the SM's Ethernet interface.
Wireless Statistics - Downlink	
Total Traffic	Total amount of traffic received via the SM's wireless interface in Kbits.
Total Packets	Total number of packets received via the SM's wireless interface.
Error Drop Packets	Total number of packets dropped before sending out of the SM's Ethernet interface due to RF errors (packet integrity error and other RF-related packet error).
Multicast / Broadcast Traffic	Total amount of multicast and broadcast traffic transmitted out of the SM's wireless interface in Kbits.

Attribute	Meaning
Broadcast Packets	Total number of broadcast packets transmitted out of the SM's wireless interface.
Multicast Packets	Total number of multicast packets transmitted out of the SM's wireless interface.
Wireless Statistics - Uplink	
Total Traffic	Total amount of traffic transmitted out of the SM's wireless interface in Kbits.
Total Packets	Total number of packets transmitted out of the SM's wireless interface.
Error Drop Packets	Total number of packets dropped after transmitting out of the SM's Wireless interface due to RF errors (No acknowledgment and other RF-related packet error).
Capacity Drop Packets	Total number of packets dropped after transmitting out of the SM's Wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).
Retransmission Packets	Total number of packets re-transmitted after transmitting out of the SM's Wireless interface due to the packets not being received by the AP.
Multicast / Broadcast Traffic	Total amount of multicast and broadcast traffic received on the SM's wireless interface in Kbits.
Broadcast Packets	Total number of broadcast packets transmitted on the SM's wireless interface.
Multicast Packets	Total number of multicast packets transmitted on the SM's wireless interface.
Link Quality (Uplink)	The Uplink quality is based on the current MCS and PER.
Link Capacity (Uplink)	The uplink capacity is based on the current MCS concerning the highest supported MCS (MCS15).
QoS Statistics	
TDD Voice Priority Queue	
Total count of transmitted packets	Total count of put packets to Voice queue
Total count of received packets	Total count of get packets from Voice queue
Total count of dropped packets	Total count of dropped packets from Voice queue
TDD High Priority Queue	
	Total count of put packets to High queue

Attribute	Meaning
Total count of transmitted packets	
Total count of received packets	Total count of get packets from High queue
Total count of dropped packets	Total count of dropped packets from High queue
TDD Low Priority Queue	
Total count of transmitted packets	Total count of put packets to Low queue
Total count of received packets	Total count of get packets from Low queue
Total count of dropped packets	Total count of dropped packets from Low queue
TDD QoS queues	
Total count of transmitted packets	Total count of put packets to all queues
Total count of received packets	Total count of get packets from all queues
Total count of dropped packets	Total count of dropped packets from all queues
System Statistics	
Session Drops	Total number of sessions dropped by the SM.
Device Reboots	Total number of reboots of the SM.
Radar (DFS) Detections	Total number of DFS events that were detected by the SM.
Downlink Packets Per MCS	Number of packets (and percentage of total packets) received on the SM's wireless interface for every modulation mode, based on radio conditions.
Uplink Packets Per MCS	Number of packets (and percentage of total packets) transmitted out of the SM's wireless interface for every modulation mode used by the SM's transmitter, based on radio conditions.

SM System page

Use the **System** page to reference key system information.

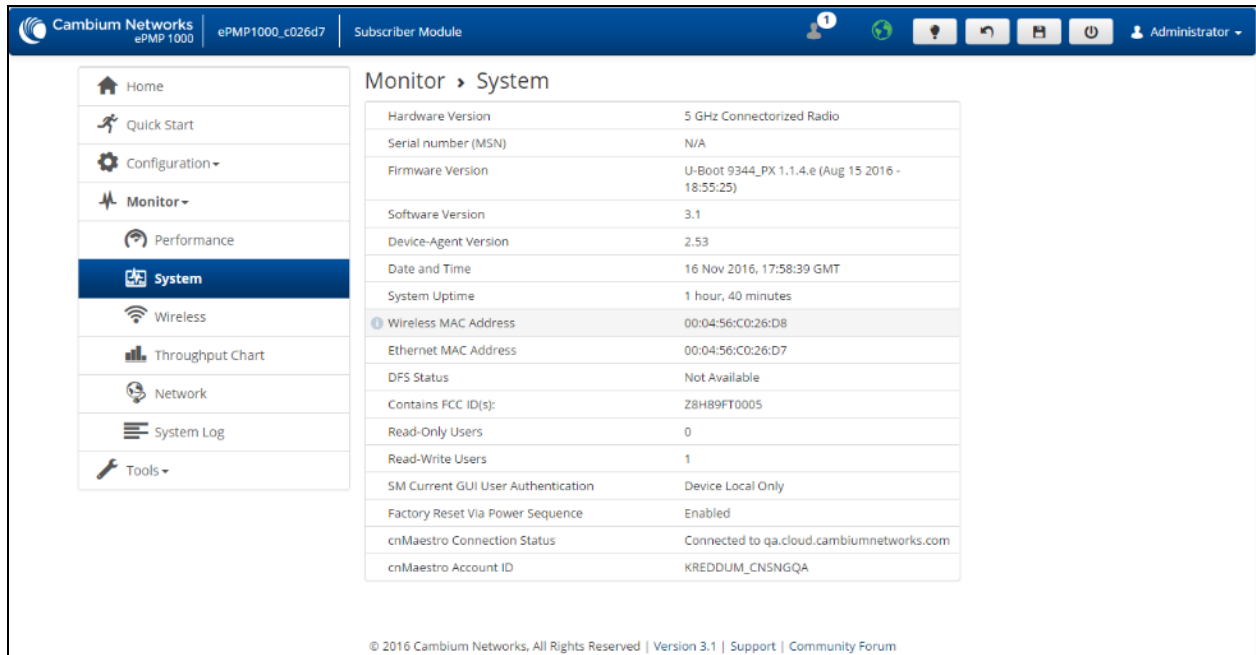


Figure 80: SM System page

Table 135: SM System page attributes

Attribute	Meaning
Hardware Version	Board hardware version information.
Serial Number (MSN)	Unit serial number (MSN).
Firmware Version	U-Boot version information.
Software Version	The current operating version of software on the device. This listing is also present on the GUI footer bar (which contains a hyperlink to download new system software).
Device-Agent Version	The operating version of the device agent, which is used for communication with cnMaestro.
Date and Time	Current date and time, subject to time zone offset introduced by the configuration of the device Time Zone parameter. This shows a factory-configured time until a valid NTP server is configured.
System Uptime	The total system uptime since the last device reset.
Wireless MAC Address	The hardware address of the device's wireless interface.
Ethernet MAC Address	The hardware address of the device Ethernet interface.
DFS Status	N/A: DFS operation is not required for the region configured in parameter Country Code

Attribute	Meaning
	<p>Channel Availability Check: Before transmitting, the device must check the configured Frequency Carrier for radar pulses for 60 seconds). If no radar pulses are detected, the device transitions to state In-Service Monitoring.</p> <p>In-Service Monitoring: Radio is transmitting and receiving normally while monitoring for radar pulses that require a channel move.</p> <p>Radar Signal Detected: The receiver has detected a valid radar pulse and is carrying out detect-and-avoid mechanisms (moving to an alternate channel).</p> <p>In-Service Monitoring at Alternative Channel: The radio has detected a radar pulse and has moved the operation to a frequency configured in DFS Alternative Frequency Carrier 1 or DFS Alternative Frequency Carrier 2.</p> <p>System Not In Service due to DFS: The radio has detected a radar pulse and has failed channel availability checks on all alternative frequencies. The non-occupancy time for the radio frequencies in which radar was detected is 30 minutes.</p>
Contains FCC ID (s)	Displays listing of FCC IDs applicable to the device.
Read-Only Users	Displays the number of active Read-Only users logged into the radio.
Read-Write Users	Displays the number of active Read-Write users logged into the radio.
SM Current GUI User Authentication	Displays the mechanism used for authentication of web management interface users.
Factory Reset Via Power Sequence	<p>Enabled: When Enabled under Tools > Backup/Restore > Reset Via Power Sequence, it is possible to reset the radio's configuration to factory defaults using the power cycle sequence explained under Resetting ePMP to factory defaults by power cycling.</p> <p>Disabled: When Disabled, it is not possible to factory default the radio's configuration using the power cycle sequence.</p>
cnMaestro Connection Status	The current management status of the device concerning the Cambium Cloud Server. When Enabled under Configuration > System , the device will be managed by the Cambium Remote Management System, which allows all Cambium devices to be managed from the Cambium Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Cloud Server.

SM Wireless page

Use the **Wireless** page to reference key information about the radio's wireless interface.

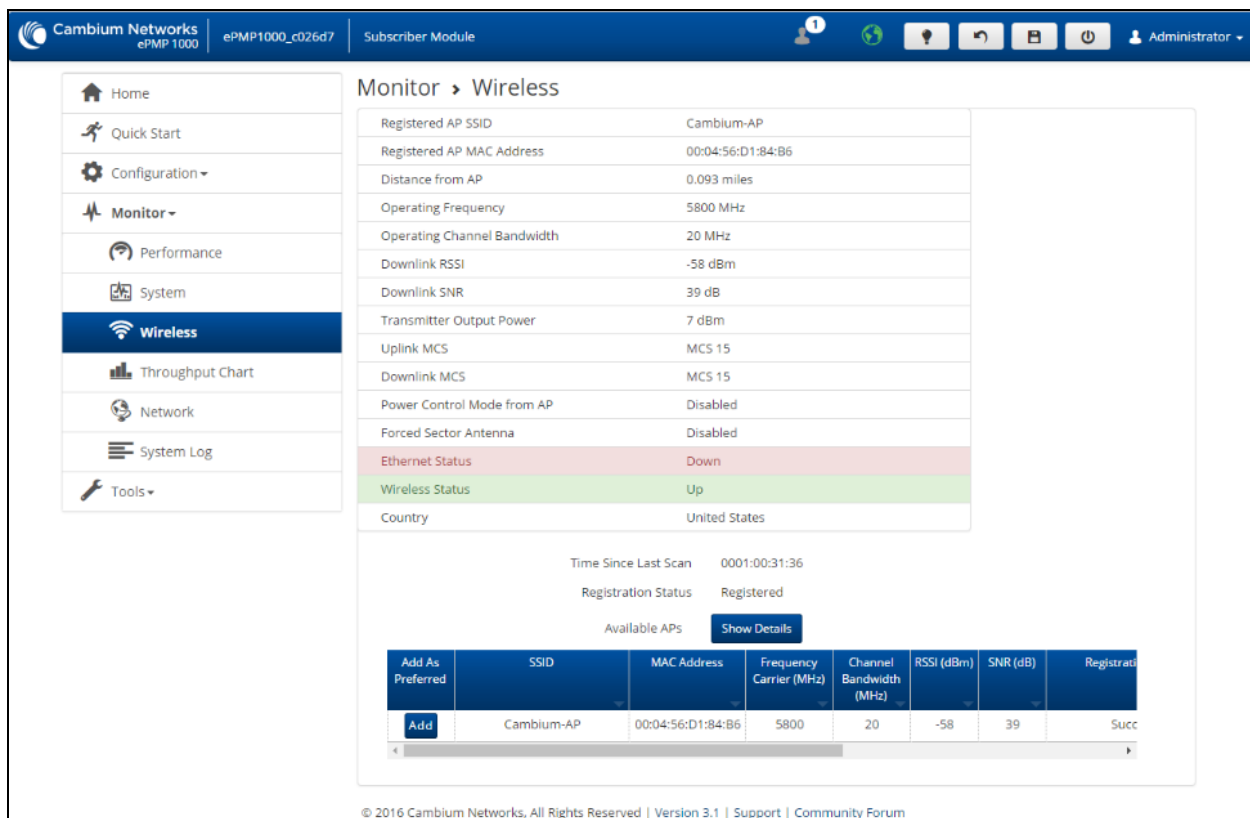



Figure 81: SM Wireless page

Table 136: SM Wireless page attributes

Attribute	Meaning
Registered AP SSID	SSID of the AP to which the SM is registered.
Registered AP MAC address	Wireless MAC address of the AP to which the SM is registered.
Distance from AP	The distance from the AP, determined by radio signal propagation delay.
Operating Frequency	The current frequency at which the SM is transmitting and receiving.
Operating Channel Bandwidth	The current channel size at which the SM is transmitting and receiving.
Downlink RSSI	The Received Signal Strength Indicator, which is a measurement of the power level being received by the SM's antenna.
Downlink SNR	The Signal to Noise Ratio, which is an expression of the carrier signal quality concerning signal noise.

Attribute	Meaning
Transmitter Output Power	The current power level at which the SM is transmitting.
Uplink MCS	Modulation and Coding Scheme - indicates the modulation mode used for the radio uplink, based on radio conditions (MCS 1-7, 9-15).
Downlink MCS	Modulation and Coding Scheme - indicates the modulation mode used for the radio downlink, based on radio conditions (MCS 1-7, 9-15).
Power Control Mode from AP	<p>Open Loop: In this mode, the SM will not receive any power change information in the Group Poll Frame. SM calculates the UL transmit power based on path loss calculations only.</p> <p>Closed Loop: In closed-loop UL power control, Subscriber Module will get the AP actual transmit power of beacon frame and SM Target Received Power Level in the beacon. Based on these two values, SM calculates the path loss. Based on path loss and TRL values it calculates its transmit power such that the signal from SM arrives at AP at the configured target level. Path loss calculation will be updated by SM every time there is a change in values of AP actual TX power or TRL in the Beacon.</p>
Forced Sector Antenna	When an ePMP 2000 AP is deployed with a Sector Antenna and a Smart Antenna, this parameter forces the AP to use only Sector Antenna for all Subscriber Modules.
Ethernet Interface	<p>Up: The radio (LAN) interface is functioning properly.</p> <p>Down: The radio (LAN) interface has encountered an error and is not servicing traffic.</p>
Wireless Interface	<p>Up: The radio (WAN) interface is functioning properly.</p> <p>Down: The radio (WAN) interface has encountered an error and is not servicing traffic.</p>
Country	The current code the SM is operating under.
Time since last scan	Amount of time elapsed since the last scan was completed by the SM for available APs.
Registration Status	The current registration status of the SM.
Available APs	The Available AP list may be referenced to view which APs are available for SM network entry, and also to view the status of the current AP to SM radio link.
Add as Preferred	Click the  button to add the AP to the Preferred AP List under Configuration->Radio.
SSID	The SSID of the visible AP.
MAC Address	The MAC address of the visible AP.
Frequency Carrier (MHz)	The current operating frequency of the visible AP.
Channel Bandwidth	The current operating channel bandwidth of the visible AP.

Attribute	Meaning
RSSI (dBm)	The current measured Received Signal Strength Indicator at the AP.
SNR (dB)	The current measured Signal-to-Noise Ratio of the SM to AP link.
Registration State	<p>The indication of the result of the SM's network entry attempt:</p> <p>Successful: SM registration is successful</p> <p>Failed: Out of Range: The SM is out of the AP's configured maximum range (Max Range parameter)</p> <p>Failed: Capacity limit reached at AP: The AP is no longer allowing SM network entry due to capacity reached</p> <p>Failed: No Allocation on AP: The SM to AP handshaking failed due to a misconfigured pre-shared key between the SM and AP</p> <p>Failed: SW Version Incompatibility: The version of software resident on the AP is older than the software version on the SM</p> <p>Failed: PTP Mode: ACL Policy: The AP is configured with PTP Access set to MAC Limited and the SM's MAC address is not configured in the AP's PTP MAC Address field</p> <p>Failed: Other: The AP does not have the required available memory to allow network entry</p>
Session Time (hh:mm:ss)	This timer indicates the time elapsed since the SM registered to the AP.
Wireless Security	This field indicates the security state of the AP to SM link.
Meets Reg Criteria	<p>Yes: The scanned AP meets the Network Entry criteria defined by the internal Network Algorithm.</p> <p>No: The scanned AP does not meet the Network Entry criteria defined by the internal Network Algorithm.</p>

SM Throughput Chart page

Use the Throughput page to reference a line chart visual representation of system throughput over time. The blue line indicates downlink throughput and the orange line indicates uplink throughput. The X-axis may be configured to display data over seconds, minutes, or hours, and the Y-axis is adjusted automatically based on average throughput. Hover over data points to display details.

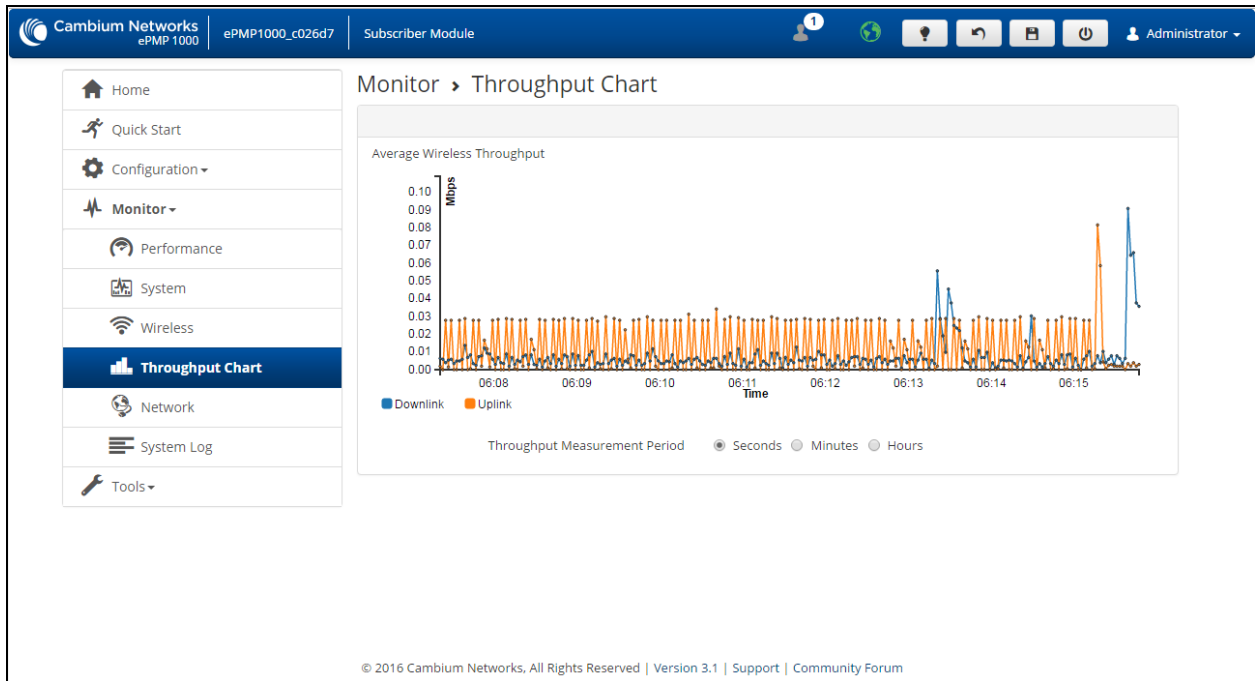


Figure 82: SM Throughput Chart page

Table 137: SM Throughput Chart page attributes

Attribute	Meaning
Throughput Measurement Period	Adjust the X-axis to display throughput intervals in seconds, minutes, or hours.

SM Network page

Use the **SM Network** page to reference key information about the device network status.

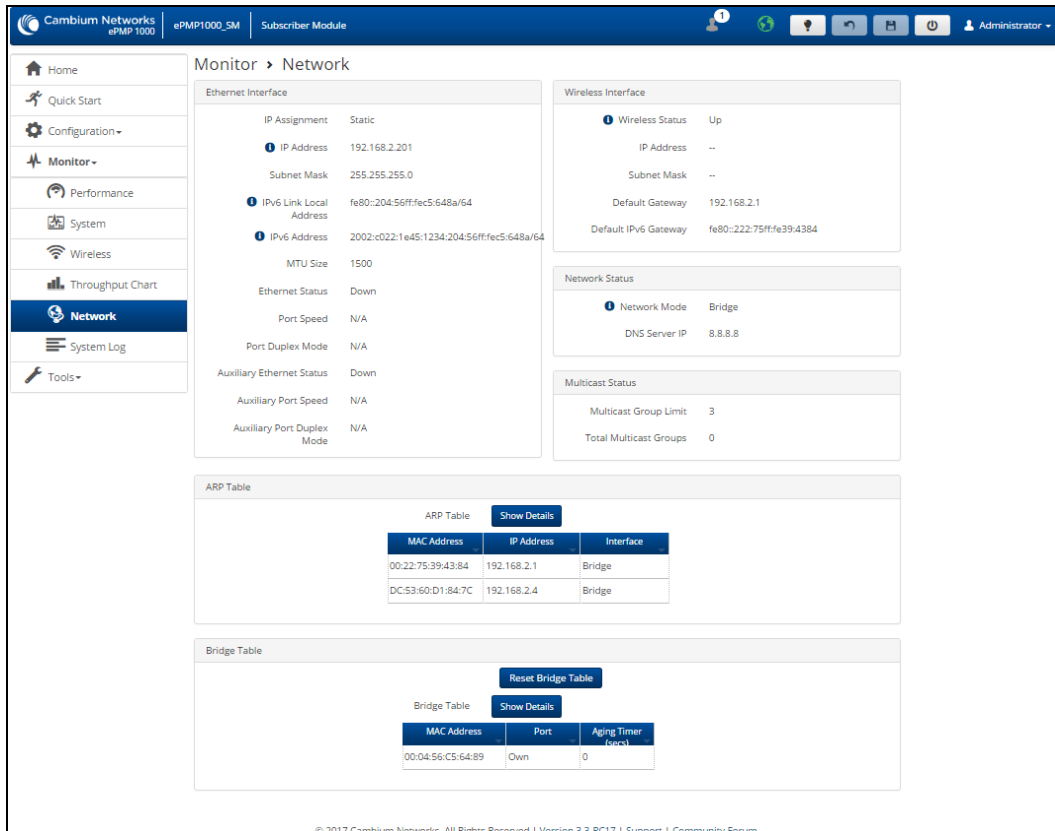


Figure 83: SM Network page, Bridge Mode

Table 138: SM Network page attributes, Bridge Mode

Attribute	Meaning
Ethernet Interface	
IP Address	The IP address for the device when the device is used in Bridge mode.
Subnet Mask	The currently configured device IP subnet mask.
IPv6 Link Local Address	A link-local address is required for the IPv6-enabled interface (applications may rely on the link-local address even when there is no IPv6 routing). The IPv6 link-local address is comparable to the auto-configured IPv4 address 169.254.0.0/16.
IPv6 Address	The IPv6 address for device management.
MTU Size	The currently configured Maximum Transmission Unit for the AP's Ethernet (LAN) interface. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Status	Up: The device Ethernet interface is functioning and passing data Down: The device Ethernet interface has encountered an error disallowing full operation. Reset the device to reinitiate the Ethernet interface.
Port Speed	The current speed of the SM's LAN port.

Attribute	Meaning
Port Duplex Mode	The current duplex mode of the SM's LAN port.
Auxiliary Ethernet Status	The current status of the SM's Auxiliary Ethernet Port.
Auxiliary Port Speed	The current operating speed of the SM's Auxiliary Ethernet Port.
Auxiliary Port Duplex Mode	The current operating duplex mode of the SM's Auxiliary Ethernet Port.
Wireless Status	
Wireless Interface	Up: The device wireless interface is functioning and passing data Down: The device's wireless interface has encountered an error disallowing full operation. Reset the device to reinitiate the wireless interface.
IP address	The IP address for the wireless interface is displayed only when the SM is in NAT Mode.
Subnet Mask	The subnet for the wireless interface is displayed only when the SM is in NAT Mode.
Default Gateway	The current configured gateway for the bridge network of the SM.
Network Status	
Network Mode	Bridge: The SM acts as a switch, and packets are forwarded or filtered based on their MAC destination address. NAT: The SM acts as a router, and packets are forwarded or filtered based on their IP header (source or destination) which can be grouped into subnets for finer granularity. Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.
DNS Server IP	Represents the IP address of the DNS Server.
Multicast Status	
Multicast Group Limit	The maximum number of simultaneous multicast groups will be allowed through the SM.
Total Multicast Groups	The current number of Multicast groups that have subscribed under this SM.
ARP Table	
MAC Address	MAC Address of the devices on the bridge.

Attribute	Meaning
IP Address	IP Address of the devices on the bridge.
Interface	The interface on which the SM identified the devices on.
Bridge Table	
MAC Address	MAC Address of the SM connected to the AP.
Port	The port to which the device is connected.
Aging Timer (secs)	Time set for the MAC addresses in the Bridge table.

The screenshot shows the 'Monitor > Network' page in the Cambium Networks ePMP 1000 Subscriber Module. The page is divided into several sections:

- Ethernet Interface:** IP Address: 10.120.210.135, Subnet Mask: 255.255.255.0, MTU Size: 1500, Ethernet Status: Down, Port Speed: N/A, Port Duplex Mode: N/A, Auxiliary Ethernet Status: Down, Auxiliary Port Speed: N/A, Auxiliary Port Duplex Mode: N/A.
- Separate Wireless Management IP Status:** Separate Management IP: Disabled.
- Wireless Interface:** Wireless IP Assignment: DHCP, Wireless Status: Up, IP Address: --, Subnet Mask: --, Default Gateway: 10.120.210.254.
- Network Status:** Network Mode: Bridge, DNS Server IP: 10.120.12.30, 10.120.12.31, PPPoE Mode: Disabled.
- ARP Table:** A table with columns for MAC Address, IP Address, and Interface. One entry is shown: MAC Address: 00:22:BE:6E:40:00, IP Address: 10.120.210.254, Interface: Bridge.
- Local DHCP Server:** DHCP Server Status: Disabled.

Figure 84: SM Network page, NAT Mode

Table 139: SM Network page attributes, NAT mode

Attribute	Meaning
Ethernet Interface	

Attribute	Meaning
IP Address	The IP address for the subnet that is associated with the Ethernet interface when the device is used in NAT and Router modes.
Subnet Mask	The currently configured device IP subnet mask.
MTU Size	The currently configured Maximum Transmission Unit for the AP's Ethernet (LAN) interface. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Status	Up: The device Ethernet interface is functioning and passing data Down: The device Ethernet interface has encountered an error disallowing full operation. Reset the device to reinitiate the Ethernet interface.
Port Speed	The current speed of the SM's LAN port.
Port Duplex Mode	The current duplex mode of the SM's LAN port.
Auxiliary Ethernet Status	The current status of the SM's Auxiliary Ethernet Port.
Auxiliary Port Speed	The current operating speed of the SM's Auxiliary Ethernet Port.
Auxiliary Port Duplex Mode	The current operating duplex mode of the SM's Auxiliary Ethernet Port.
Separate Wireless Management IP	
Separate Management IP	Disabled: A separate wireless management interface is not available. Enabled: A Separate Wireless Management IP has been configured and a management interface is available.
IP Assignment	Static: Device management IP addressing is configured manually in fields IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server. DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are unused.
IP Address	The IP address for the separate wireless management interface is displayed only when the Separate Wireless Management IP is enabled.
Subnet Mask	The subnet for the separate wireless management interface.
Gateway	The default gateway for the separate wireless management interface.
Wireless Status	
Wireless IP Assignment	Static: Device management IP addressing is configured manually in fields IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server.

Attribute	Meaning
	DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are unused.
Wireless Status	Up: The device wireless interface is functioning and passing data Down: The device's wireless interface has encountered an error disallowing full operation. Reset the device to reinitiate the wireless interface.
IP Address	The IP address for the wireless interface of the SM.
Subnet Mask	The subnet for the wireless interface of the SM.
Default Gateway	The default gateway for the wireless interface of the SM.
Network Status	
Network Mode	Bridge: The SM acts as a switch, and packets are forwarded or filtered based on their MAC destination address. NAT: The SM acts as a router, and packets are forwarded or filtered based on their IP header (source or destination) which can be grouped into subnets for finer granularity. Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.
DNS Server IP	Represents the IP address of the DNS Server.
PPPoE Mode	Disabled: If this is left blank the STA will accept the first service option that comes back from the Access Concentrator specified below if any. PPPoE is 'Disabled' by default. Enabled: An optional entry is 'Enabled' to set a specific service name to connect to the PPPoE session. This is limited to 32 characters.
DHCP Lease Time	Currently configured time for which a DHCP IP address is leased. When the lease time expires, the DHCP client must renew IP addresses via DHCP request.
ARP Table	
MAC Address	MAC Address of the devices in the SM's routing table.
IP Address	IP Address of the devices in the SMs routing table.
Interface	The interface on which the SM identified the devices on.
Local DHCP Server	
DHCP Server Status	Indicates if the local DHCP server on the SM in NAT mode is Enabled/Disabled.
DHCP Server IP Start Address	The first IP address in the DHCP pool issued to a DHCP client. Upon additional DHCP requests, the DHCP Start IP is incremented until the Local DHCP End IP is reached.

Attribute	Meaning
DHCP Server IP End Address	The last/highest address IP address in the DHCP pool of addresses is issued to a DHCP client.
DHCP Gateway IP Address	The gateway of the local DHCP server
DHCP DNS IP Address	DNS Server IP address which will be used to configure DHCP clients (if Local DHCP Server is set to Enabled under Configuration > Network).
DHCP Static MAC to IP Configuration Table	
MAC Address	MAC address of clients that were statically assigned an IP address in the DHCP Static MAC to IP Configuration Table under Configuration > Network
IP Address	The IP address of clients that were statically assigned an IP address in the DHCP Static MAC to IP Configuration Table under Configuration > Network .
DHCP Assigned IP Address Table	
MAC Address	MAC address of clients that were assigned an IP address through DHCP from the Local DHCP Server
IP Address	The IP address of clients that were assigned an IP address through DHCP from the Local DHCP Server
Device Name	Device Name of clients that were assigned an IP address through DHCP from the Local DHCP Server

Cambium Networks ePMP 1000 ePMP1000_c026d7 Subscriber Module Administrator

Monitor > Network

- Home
- Quick Start
- Configuration
- Monitor**
- Performance
- System
- Wireless
- Throughput Chart
- Network**
- System Log
- Tools

Ethernet Interface

- IP Address: 10.120.210.135
- Subnet Mask: 255.255.255.0
- MTU Size: 1500
- Ethernet Status: Down
- Port Speed: N/A
- Port Duplex Mode: N/A
- Auxiliary Ethernet Status: Down
- Auxiliary Port Speed: N/A
- Auxiliary Port Duplex Mode: N/A

Wireless Interface

- Wireless IP Assignment: DHCP
- Wireless Status: Up
- IP Address: --
- Subnet Mask: --
- Default Gateway: 10.120.210.254

Network Status

- Network Mode: Bridge
- DNS Server IP: 10.120.12.30, 10.120.12.31
- PPPoE Mode: Disabled

ARP Table

ARP Table [Show Details](#)

MAC Address	IP Address	Interface
00:22:BE:6E:40:00	10.120.210.254	Bridge

Local DHCP Server

DHCP Server Status: Disabled

Static Routes

Static Routes [Show Details](#)

Target Network IP	Subnet Mask	Gateway	Interface
	255.255.255.255	10.120.210.254	Bridge

IP Aliases

IP Aliases [Show Details](#)

IP Address	Netmask
Table is empty	

© 2016 Cambium Networks. All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 85: SM Network page, Router Mode

Table 140: SM Network page attributes, Router mode

Attribute	Meaning
Ethernet Interface	
IP Address	The IP address for the subnet is associated with the Ethernet interface when the device is used in NAT and Router modes.
Subnet Mask	The currently configured device IP subnet mask.
MTU Size	The currently configured Maximum Transmission Unit for the AP's Ethernet (LAN) interface. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Status	Up: The device Ethernet interface is functioning and passing data Down: The device Ethernet interface has encountered an error disallowing full operation. Reset the device to reinitiate the Ethernet interface.
Port Speed	The current speed of the SM's LAN port.
Port Duplex Mode	The current duplex mode of the SM's LAN port.
Auxiliary Ethernet Status	The current status of the SM's Auxiliary Ethernet Port.
Auxiliary Port Speed	The current operating speed of the SM's Auxiliary Ethernet Port.
Auxiliary Port Duplex Mode	The current operating duplex mode of the SM's Auxiliary Ethernet Port.
Wireless Interface	
Wireless IP Assignment	Static: Device management IP addressing is configured manually in fields IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server. DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are unused.
Wireless IP Assignment	Static: Device management IP addressing is configured manually in fields IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server. DHCP: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server, and parameters IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are unused.
IP Address	The IP address for the separate wireless management interface is displayed only when the Separate Wireless Management IP is enabled.
Subnet Mask	The subnet for the separate wireless management interface of the

Attribute	Meaning
	SM.
Default Gateway	The default gateway for the separate wireless management interface of the SM.
Network Status	
Network Mode	<p>Bridge: The SM acts as a switch, and packets are forwarded or filtered based on their MAC destination address.</p> <p>NAT: The SM acts as a router, and packets are forwarded or filtered based on their IP header (source or destination) which can be grouped into subnets for finer granularity.</p> <p>Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.</p>
DNS Server IP	Represents the IP address of the DNS Server.
PPPoE Mode	<p>Disabled: If this is left blank the STA will accept the first service option that comes back from the Access Concentrator specified below if any. PPPoE is 'Disabled' by default.</p> <p>Enabled: An optional entry is 'Enabled' to set a specific service name to connect to the PPPoE session. This is limited to 32 characters.</p>
DHCP Lease Time	Currently configured time for which a DHCP IP address is leased. When the lease time expires, the DHCP client must renew IP addresses via DHCP request.
ARP Table	
MAC Address	MAC Address of the devices in the SM's routing table.
IP Address	IP Address of the devices in the SMs routing table.
Interface	The interface on which the SM identified the devices on.
Local DHCP Server	
DHCP Server Status	Indicates if the local DHCP server on the SM in NAT mode is Enabled/Disabled.
DHCP Server IP Start Address	The first IP address in the DHCP pool is issued to a DHCP client. Upon additional DHCP requests, the DHCP Start IP is incremented until the Local DHCP End IP is reached.
DHCP Server IP End Address	The last/highest address IP address in the DHCP pool of addresses is issued to a DHCP client.
DHCP Gateway IP Address	The gateway of the local DHCP server
DHCP DNS IP Address	DNS Server IP address which will be used to configure DHCP clients (if Local DHCP Server is set to Enabled under Configuration > Network).

Attribute	Meaning
Static Routes	
Target Network IP	Target subnet/network's IP address to which the SM should route the packets.
Subnet Mask	Subnet mask for the Target Network IP address.
Gateway	Gateway to which packets that match the Target Network IP Address and Subnet Mask are sent.
Interface	Interface to which the static route is active.
IP Aliases	
IP Address	The IP address for the configured IP alias.
Subnet Mask	Subnet mask for the configured IP alias.

SM System Log page

Use the **SM System Log** page to view the device system log and to download the log file to the accessing PC or device.

The screenshot shows the Cambium Networks ePMP 1000 management interface. The top navigation bar includes the Cambium Networks logo, device ID (ePMP1000_c026d7), and user role (Administrator). The left sidebar contains navigation options: Home, Quick Start, Configuration, Monitor (selected), Performance, System, Wireless, Throughput Chart, Network, System Log (highlighted), and Tools. The main content area is titled 'Monitor > System Log' and features a 'Syslog Display' toggle set to 'Enabled'. Below this is a 'Syslog File' section with a scrollable log of system messages. The log entries include timestamps and details about DNS resolution failures, connection attempts to cnMaestro, and network configuration changes such as adding and removing interfaces from zones. A 'Download' button is located at the bottom of the log area.

Figure 86: SM System Log page

Table 141: SM System Log attributes

Attribute	Meaning
Syslog Display	Enabled: The system log file is displayed on the management GUI.

Attribute	Meaning
	Disabled: The system log file is hidden on the management GUI.
Syslog file	Use this button to download the full system log file to a connected PC or device.

SM Tools menu

The **SM Tools** menu provides several options for upgrading device software, configuration backup/restore, analyzing RF spectrum, testing device throughput, running ping, and traceroute tests.

- [SM Software Upgrade page](#)
- [SM Backup / Restore page](#)
- [SM eDetect page](#)
- [SM Spectrum Analyzer page](#)
- [SM eAlign page](#)
- [SM Wireless Link Test page](#)
- [SM Ping page](#)
- [SM Traceroute page](#)

SM Software Upgrade page

Use the **SM Software Upgrade** page to update the device radio software to take advantage of new software features and improvements.



Caution

Please read the Release Notes associated with each software release for special notices, feature updates, resolved software issues, and known software issues. The Release Notes may be accessed at the [Cambium Support Center](#).

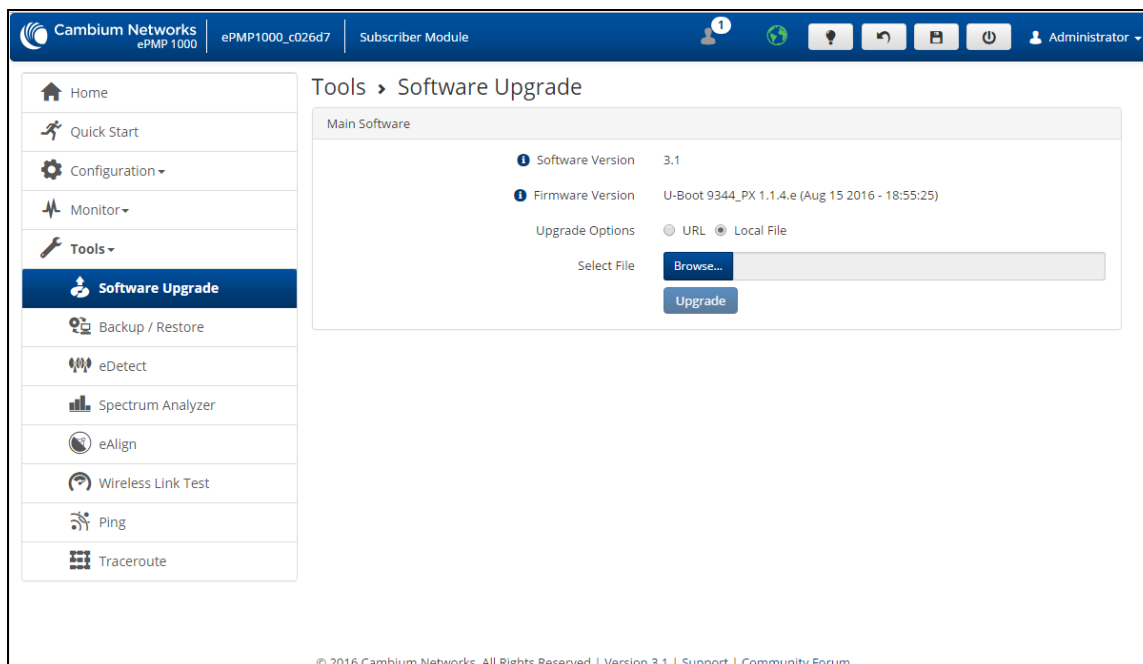


Figure 87: SM Software Upgrade page

Table 142: SM Software Upgrade attributes

Attribute	Meaning
Software Version	The current operating software version. ePMP boards that do not have an onboard GPS have one bank of flash memory which contains a version of the software. The version of the software last upgraded onto the Flash memory is present on this bank of flash memory. This software will be used by the SM when the SM is rebooted.
Firmware Version	Specifies the code used to boot the board.
Upgrade Options	<p>From URL: A web server may be used to retrieve software upgrade packages (downloaded to the device via the webserver). For example, if a web server is running at IP address 192.168.2.1 and the software upgrade packages are located in the home directory, an operator may select an option From URL and configure the Software Upgrade Source Info field to http://192.168.2.1/<software_upgrade_package></p> <p>From Local File: Click Browse to select the local file containing the software upgrade package</p>
Select File	Click Browse to select a local file (located on the device accessing the web management interface) for upgrading the device software.

To upgrade the device software, follow this procedure:

Procedure:

1. Download the software upgrade packages from <https://support.cambiumnetworks.com/files/epmp>
2. Clear the cache of the accessing browser.

3. On the device GUI, navigate to **Tools > Software Upgrade**.
4. Select the **SW Upgrade Option** which represents the location of your software upgrade packages.
5. Based on the configuration of **SW Upgrade Option**, enter either the **Software Upgrade Source Info** or click the **Browse** button and locate the software package.
6. Click **Upgrade**.
7. When the upgrade is completed successfully, click the **Reset** icon.

SM Backup / Restore page

Use the **SM Backup / Restore** page to perform the following functions:

- Back up the configuration in either text (.json) format or binary (.bin) format.
- Restore the configuration of using a configuration file that was previously backed up.
- Reset the device to its factory default configuration. For more factory defaulting methods, see:
 - [Using the device external reset button](#)
 - [Resetting ePMP to factory defaults by power cycling](#)

The screenshot displays the Cambium Networks ePMP 1000 GUI. The top navigation bar shows the device name 'ePMP1000_c026d7' and the role 'Subscriber Module'. The left sidebar contains a menu with 'Tools > Backup / Restore' highlighted. The main content area is titled 'Tools > Backup / Restore' and is divided into three sections:

- Backup Configuration:** Features a 'Configuration File Format' section with radio buttons for 'Text (Editable)' (selected) and 'Binary (Secured)'. A 'Download' button is located below these options.
- Restore Configuration:** Includes a 'Select File' label, a 'Browse...' button, and an 'Upload' button.
- Factory Default Configuration:** Contains four settings:
 - 'Reset Via Power Sequence' with radio buttons for 'Disabled' and 'Enabled' (selected).
 - 'Retain Passwords' with radio buttons for 'Disabled' (selected) and 'Enabled'.
 - 'Keep Passwords' with an unchecked checkbox.
 - 'Reset to Factory Defaults' with an unchecked checkbox and a 'Reset' button.

The footer of the page states: © 2016 Cambium Networks. All Rights Reserved | Version 3.1 | Support | Community Forum

Figure 88: SM Backup / Restore page

Table 143: SM Backup / Restore attributes

Attribute	Meaning
Backup Configuration	
Configuration File Format	<p>Text (Editable): Choosing this option will download the configuration file in the .json format and can be viewed and/or edited using a standard text editor.</p> <p>Binary (Secured): Choosing this option will download the configuration file in the .bin format, and cannot be viewed and/or edited using an editor. Use this format for a secure backup.</p>
Restore Configuration	
Select File	Click Browse to select a local file (located on the device accessing the web management interface) for restoring the device configuration.
Factory Default Configuration	
Reset Via Power Sequence	<p>Enabled: When Enabled, it is possible to reset the radio's configuration to factory defaults using the power cycle sequence explained under Resetting ePMP to factory defaults by power cycling on page 1.</p> <p>Disabled: When Disabled, it is not possible to factory default the radio's configuration using the power cycle sequence.</p>
Retain Passwords	<p>When set to Enabled, then after a factory default of the radio for any reason, the passwords used for GUI and CLI access will not be defaulted and will remain unchanged. The default value of this field is Disabled.</p> <div style="border: 1px solid black; background-color: #f4a460; padding: 5px;"> <p>Caution</p> <p>If the passwords cannot be retrieved after the factory default, access to the radio will be lost/unrecoverable. This feature prevents unauthorized users from gaining access to the radio for any reason, including theft.</p> </div>
Keep Passwords	When the Keep Passwords checkbox is selected, the passwords used for GUI and CLI access will not be defaulted and will remain unchanged. This is a one-time option, and it does not apply to factory default procedures completed by power cycling (Reset Via Power Sequence).
Reset to Factory Defaults	<p>Use this button to reset the device to its factory default configuration.</p> <div style="border: 1px solid black; background-color: #f4a460; padding: 5px;"> <p>Caution</p> <p>A reset to factory default configuration resets all device parameters. With the SMs in the default configuration, it may not be able to register to an AP configured for your network.</p> </div>

SM eDetect page

The **eDetect** tool (not available in ePTP Slave mode) is used to measure the 802.11 interference at the ePMP radio or system when run from the AP, on the current operating channel. When the tool is run, the

ePMP device processes all frames received from devices not connected to the ePMP system and collects the interfering frame's information such as MAC Address, RSSI, and MCS. Use the SM **eDetect** page to collect information about interferers locally at the SM to display on the SM's GUI.

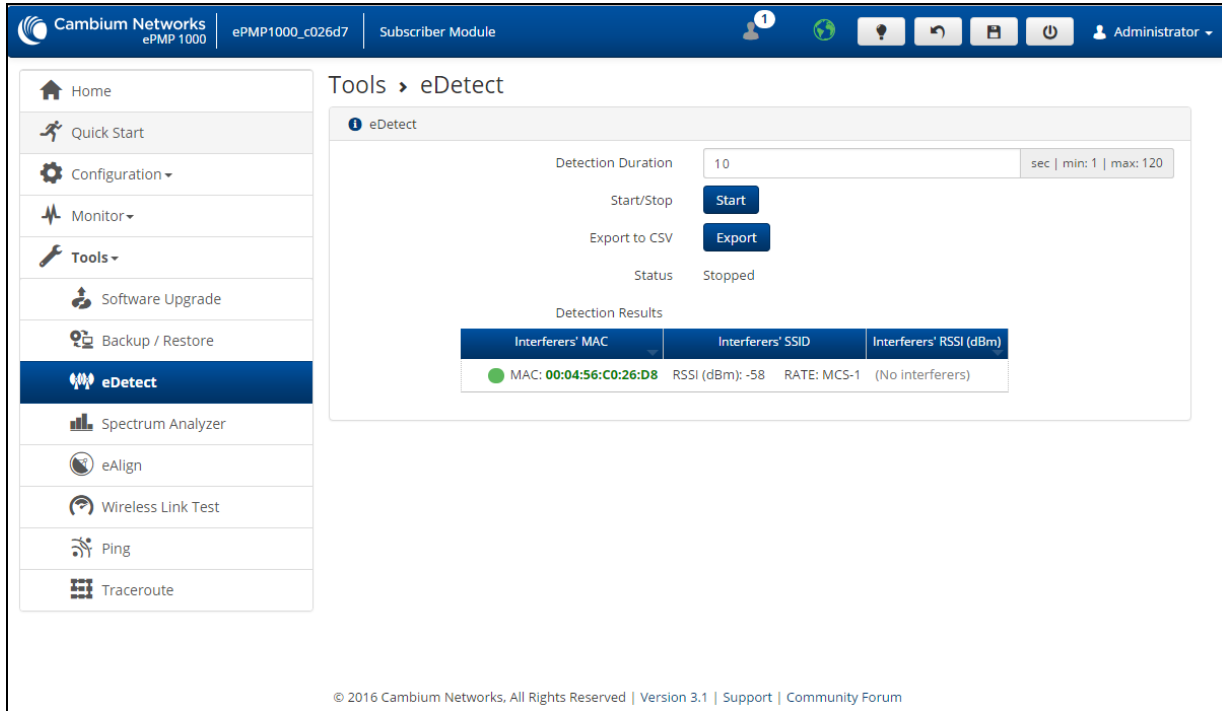



Figure 89: SM eDetect page

Table 144: SM eDetect attributes

Attribute	Meaning
eDetect	
Detection Duration	Configure the duration for which the SM scans for interferers.  <div style="border: 1px solid black; background-color: #f4a460; padding: 5px; margin-top: 5px;"> <p>Caution</p> <p>During the scanning period, the SM must be connected to the AP and passing user traffic, and there cannot be any outage (unlike running a Spectrum Analyzer). There may be a negligible degradation in the SM's throughput.</p> </div>
Start/Stop	Use to start or stop the interference detection.
Export to CSV	Choose this option to export the detection results to .csv format.
Status	Current status of the Interference Detection tool.
Detection Results	Use the Detection Results table to monitor interferers at the SM and their key RF parameters.
Device Instant Health	This is an indicator of the device's health in terms of channel conditions in the presence of interferer(s). <p>Green: Indicates that the channel is relatively clean and has good C/I levels (>25dB). The interference level is low.</p> <p>Yellow: Indicates that the channel has moderate or intermittent interference (C/I between 10dB and 25dB).</p> <p>Red: Indicates that the channel has high interference and poor C/I levels (<10dB).</p>
Device MAC	The MAC address of the SM's wireless interface.
Device RSSI (dBm)	The Received Signal Strength Indicator, which is a measurement of the power level being received by the device's antenna.
Device MCS	Modulation and Coding Scheme - indicates the modulation mode used for a radio's receiver side, based on radio conditions (MCS 1-7, 9-15).
Interferers' MAC	The MAC address of the interferer's wireless interface.
Interferers' RSSI (dBm)	The Received Signal Strength Indicator, which is a measurement of the interferer's power level being received by the device's antenna.
Interferers' MCS	Modulation and Coding Scheme - indicates the modulation mode used by the interferer, based on radio conditions (ex: MCS 1--15).

SM Spectrum Analyzer page

Use the **SM Spectrum Analyzer** page to configure SM spectrum analyzer parameters and to download the spectrum analyzer tool.

To download the spectrum analyzer tool, the AP **Device Mode** must be set to **Spectrum Analyzer**.

Java Runtime Environment is required to run the AP spectrum analyzer.



Caution

Conducting spectrum analysis causes the SM to enter scan mode and the SM drops all RF connections.

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

To conduct a spectrum analysis, follow these steps:

Required Software:

- Java Run-time Environment (JRE)

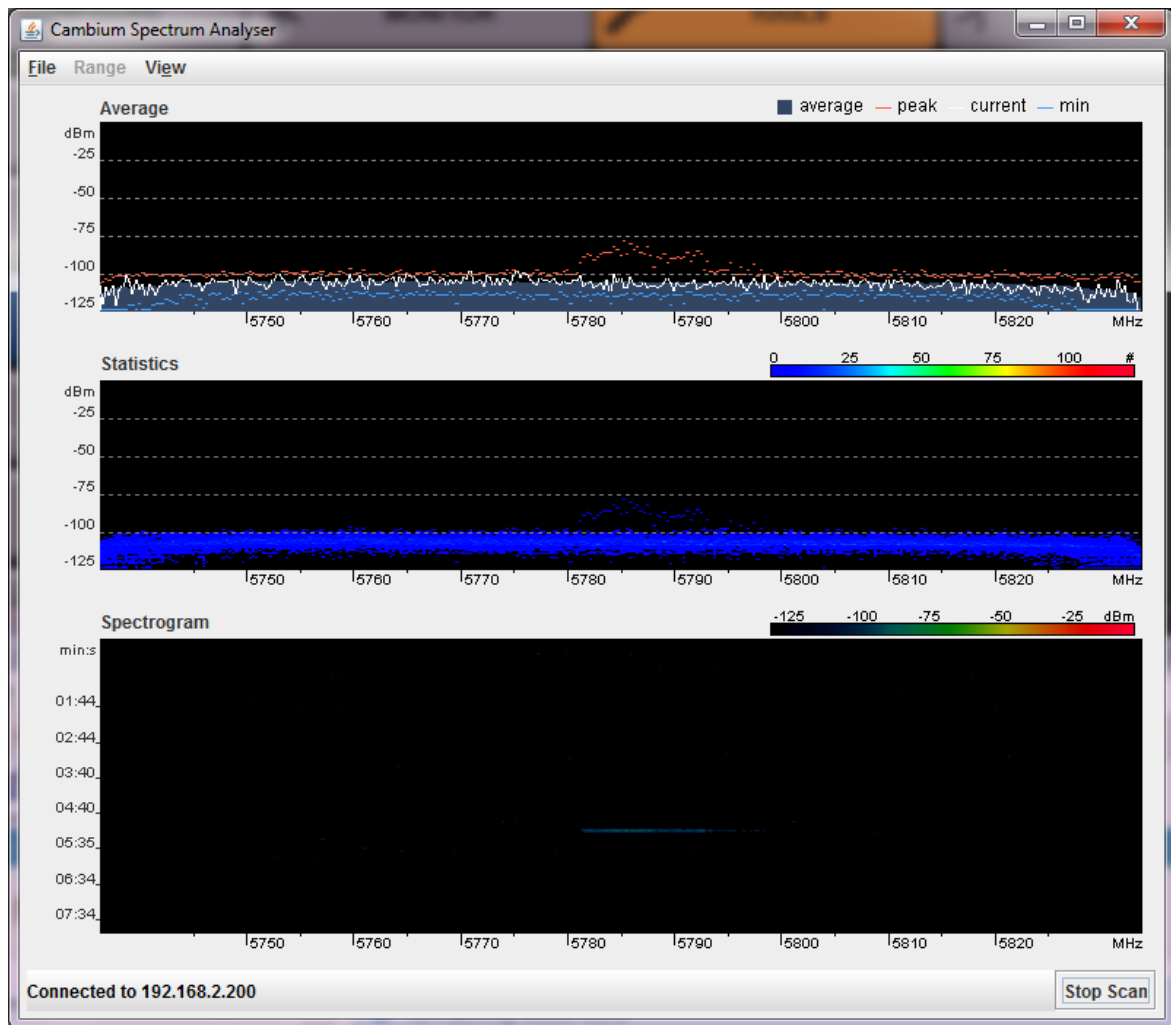
Procedure:

1. On the SM GUI, navigate to **Configure > System**.
2. Configure Device mode to Spectrum Analyzer.
3. Click the **Save** button.
4. Click the **Reset** button.
5. Login to the SM and navigate to **Tools > Spectrum Analyzer**.
6. Click Download Spectrum Analyzer Tool.
7. Locate the folder to which the spectrum analyzer tool was saved, and double-click on file csa.jnlp to launch the tool.
8. If a security warning window is presented, tick the checkbox next to “I accept the risk and want to run this application”.
9. In the security warning window, click **Run**.
The spectrum analyzer interface is displayed.
10. Click **Range** to configure the range of frequencies to scan.

Display of the average, peak, current, and minimum power levels for the configured range
Click **Start Scan** to begin scanning.

Spectrogram display of the energy levels detected throughout the configured range, over time

Statistical display of the number of times each frequency in the range was scanned



When scanning is complete, follow these steps to return the device to SM operation:

Procedure:

1. In the spectrum analyzer application, click **Stop Scan**.
2. Close the spectrum analyzer application by clicking **File > Exit**.
3. On the SM GUI, navigate to **Configure > System**.
4. Configure Device Mode to SM.
5. Click the **Save** button.
6. Click the **Reset** button.

SM eAlign page

Use the eAlign page to aid with link alignment. A valid link to an AP is required for eAlign to provide meaningful measurements.



Figure 90: SM eAlign page

Table 145: SM eAlign attributes

Attribute	Meaning
Operating Frequency	The current frequency at which the SM is operating.
Registered AP SSID	The SSID of the AP to which the SM is registered.
Current RSSI	Current RSSI value measured on the uplink by the SM's receiver.
Peak RSSI	Peak RSSI value measured by the SM's receiver from the time the user navigated to the eAlign page.
Reset Measurements	Click this button to reset all current measurements.

SM Wireless Link Test page

Use the **SM Wireless Link Test** page to conduct a simple test of SM wireless throughput to the AP to which it is registered. This allows you to determine the throughput that can be expected on a particular link without having to use external tools.

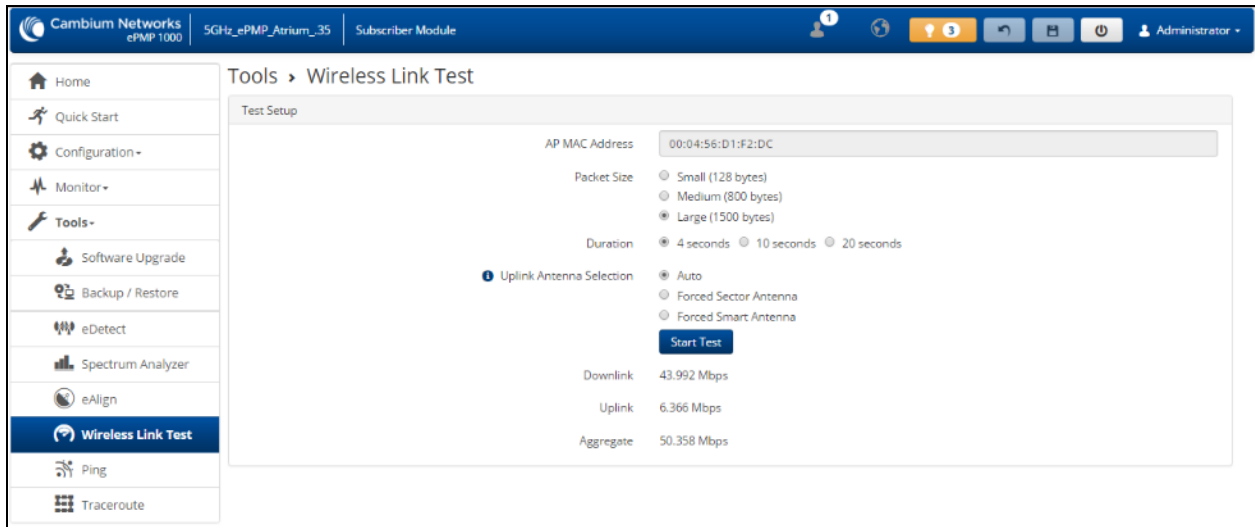


Figure 91: SM Wireless Link Test page

Table 146: SM Wireless Link Test attributes

Attribute	Meaning
Test Setup	
AP MAC Address	This is not an editable field. It is automatically populated with the wireless MAC address of the AP to which the SM is registered.
Packet Size	Choose the Packet Size to use for the throughput test.
Duration	Choose the time duration in seconds to use for the throughput test.
Uplink Antenna Selection	Uplink Antenna Selection specifies the antenna to be used in the uplink for the wireless link test. The antenna cannot be forced if it is already configured to Forced Sector Antenna or Forced Smart Antenna in the AP.
Downlink	This field indicates the result of the throughput test on the downlink, in Mbps.
Uplink	This field indicates the result of the throughput test on the uplink, in Mbps.
Aggregate	This field indicates the result of the aggregate throughput on the link, in Mbps. Displayed only when Downlink/Uplink Ratio is set to 75/25, 50/50, or 30/70.

SM Ping page

Use the SM **Ping** page to conduct a simple test of SM IP connectivity to other devices which are reachable from the network. If no ping response is received or if “Destination Host Unreachable” is reported, the target may be down, there may be no route back to the SM, or there may be a failure in the network hardware (i.e. DNS server failure).

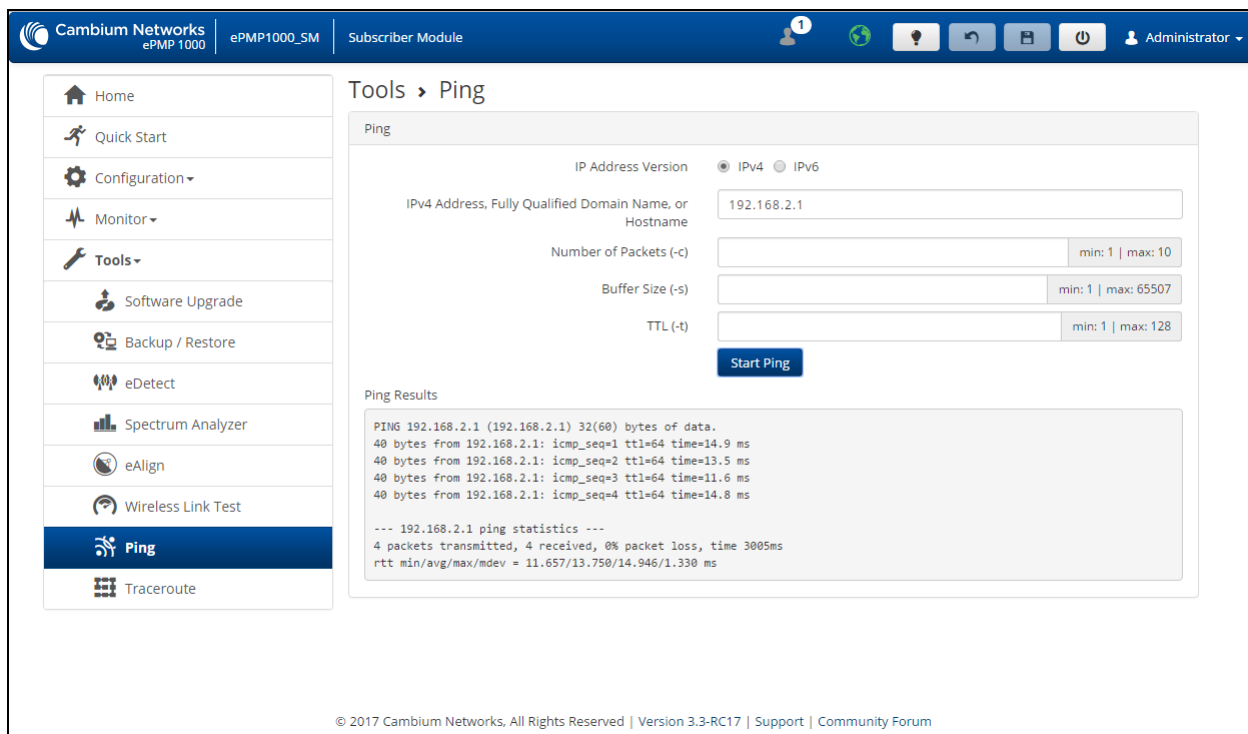


Figure 92: SM Ping page

Table 147: SM Ping attributes

Attribute	Meaning
Ping	
IP Address Version	IPv4: The ping test is conducted via IPv4 protocol. IPv6: The ping test is conducted via IPv6 protocol.
IP Address	Enter the IP address of the ping target.
Number of packets (-c)	Enter the total number of ping requests to send to the target.
Buffer size (-s)	Enter the number of data bytes to be sent.
TTL (-t)	Set the IP Time-To-Live (TTL) for multicast packets. This flag applies if the ping target is a multicast address.
Ping Results	Displays the ping test results.

SM Traceroute page

Use the **SM Traceroute** page to display the route (path) and associated diagnostics for IP connectivity between the SM and the destination specified.

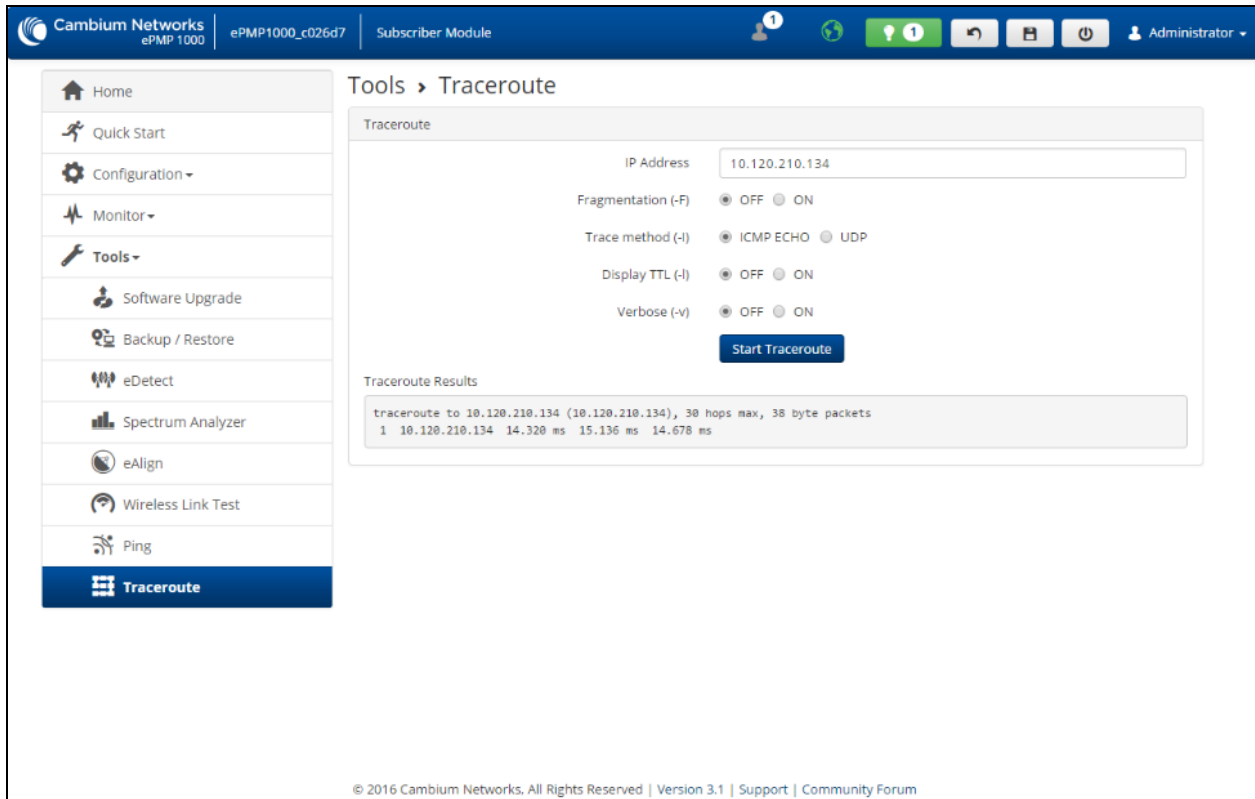


Figure 93: SM Traceroute page

Table 148: SM Traceroute attributes

Attribute	Meaning
Traceroute	
IP Address	Enter the IP address of the target of the traceroute diagnostic.
Fragmentation (-F)	ON: Allow source and target to fragment probe packets. OFF: Do not fragment probe packets (on the source or target).
Trace method (-I)	ICMP ECHO: Use ICMP ECHO for traceroute probes. UDP: Use UDP for traceroute probes.
Display TTL (-I)	ON: Display TTL values for each hop on the route. OFF: Suppress display of TTL values for each hop on the route.
Verbose (-v)	ON: ICMP packets other than TIME_EXCEEDED and UNREACHABLE are displayed in the output. OFF: Suppress display of extraneous ICMP messaging.
Traceroute Results	Displays the results of the traceroute diagnostics.

Radius Server

Installing Free-radius on Ubuntu 12.04 LTS

To install the Radius server on Ubuntu 12.04 LTS, follow these instructions:

1. On the free-radius web page <http://freeradius.org>, download the latest package (currently 3.1), either from the main page or the download page.
2. Extract the archive file by using the command line as shown below:
 - To extract a tar.bz2 file, use the command (note the j option)
`tar -jxvf freeradius-server-x.x.x.tar.bz2`
 - To extract a tar.gz file, use the command (note the z option)
`tar -zxvf freeradius-server-x.x.x.tar.gz`
3. Once the files are extracted to a folder (`cd freeradius-server-x.x.x`), execute these commands:
`sudo apt-get install libssl-dev`
`sudo apt-get install libtalloc-dev`
`./configure`
`make`
`make install`

Configuring Free-radius server

To configure the Free-Radius server, follow these steps:



Note

IP address or subnet of the client must be configured in the `clients.conf` file.

Ex. - For the examples listed in the document, the subnet of the external machine is 172.22.121.0 or 192.168.0.0.

1. For testing from external machines, edit `/usr/local/etc/raddb/clients.conf` and add an entry.

For example:

```
client 172.22.121.0/24 {
    ipaddr = 172.22.121.0
    netmask = 24
    secret = cambium
    proto = *
    shortname = epmp1
}
client 127.0.0.0/24 {
    ipaddr = 172.22.121.0
```

```
netmask = 24
secret = cambium
proto = *
shortname = epmp1
}
```

```
client 192.168.0.0/16 {
    ipaddr = 192.168.0.0
    netmask = 16
    secret = cambium
    proto = *
}
```

2. To add EAP-TTLS Username and EAP-TTLS Password, edit `usr/local/etc/raddb/user`.

For example put this string at the end of file:

```
cambium-SubscriberModule Cleartext-Password := "cambium",
```

where `cambium-SubscriberModule - EAP-TTLS Username` and `"cambium" - EAP-TTLS Password`.

3. To configure free-radius key and certificate, edit `/usr/local/etc/raddb/mods-available/eap` and add your certificates to folder `/usr/local/etc/raddb/certs`.

Locate a string such as `default_eap_type`, `private_key_file`, `certificate_file` in `eap` file and change the value to:

```
default_eap_type = ttls
private_key_password = *** - according to your certificate
private_key_file = ${certdir}/**/*.key
certificate_file = ${certdir}/**/*.crt
```

Under the `ttls` section, change the following:

```
copy_request_to_tunnel=yes
```

```
use_tunnel_reply=yes
```

**Note**

Once these steps are performed, free-radius in debug mode can be initiated: `$ radiusd -X`.

Configuring radius parameters on AP

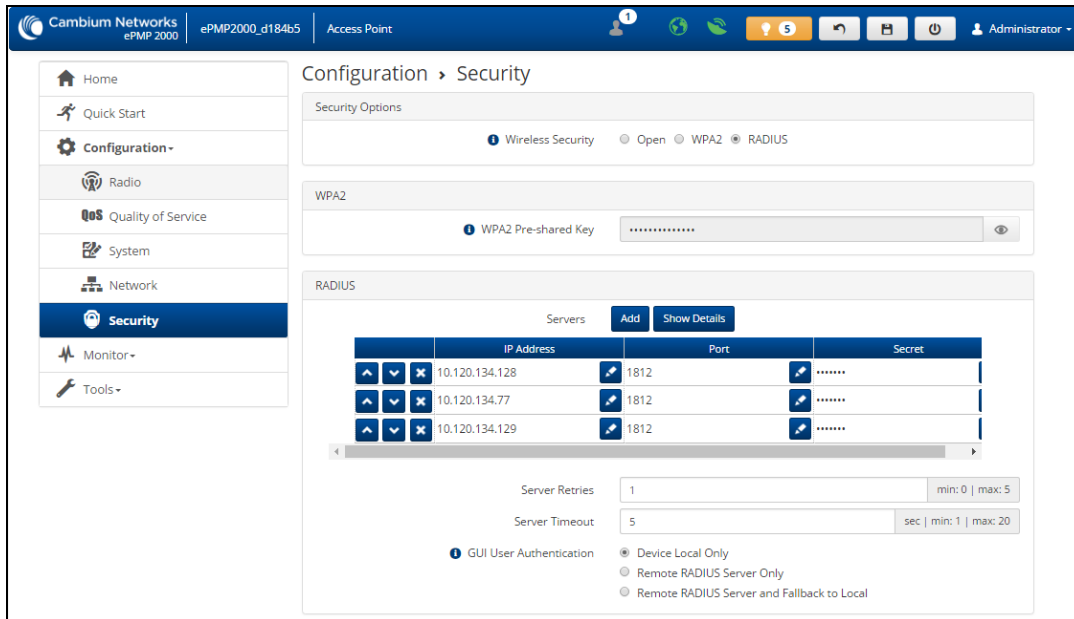


Figure 94: AP Radius configuration

To configure Radius parameters on the AP, follow these steps:

1. Open the GUI and login as **admin**.
2. Navigate to **Configure > Security > Wireless Security**.
3. **Change** the value to **RADIUS**.
4. Add the IP Address of your RADIUS Server in the **Radius Servers** table.
5. Also, configure **Port** (you may use default 1812) and **Secret** which has to be the same as in clients.conf file.
6. Click **Save**, to keep the changes.

Configuring radius parameters on SM

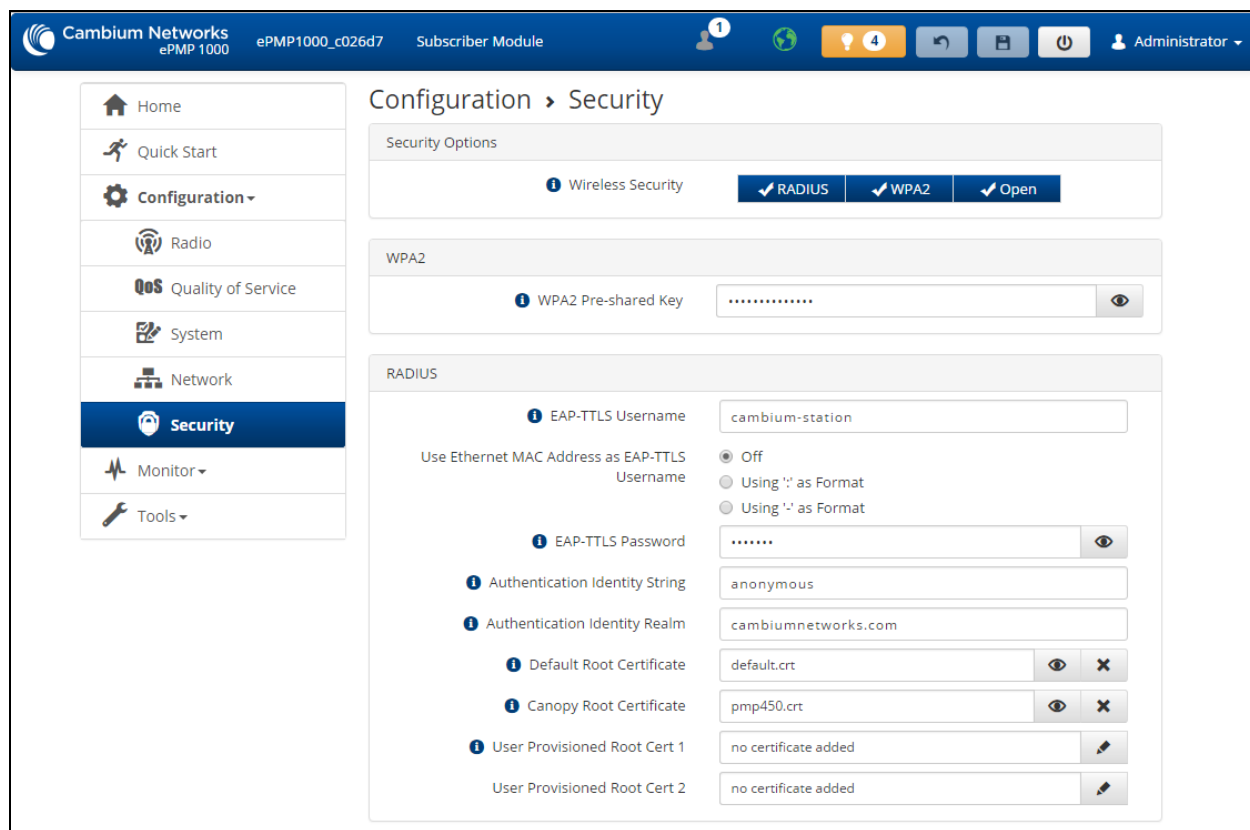


Figure 95: SM Radius configuration

To configure Radius parameters on SM, follow these steps:

1. Select **Wireless Security** as RADIUS.
2. Configure EAP-TTLS Username and EAP-TTLS Password, as configured in file users.
3. Choose the **Default Root Certificate**.
4. Click **Save**, to keep the changes.

Configuring MIR profiles

To configure the MIR profiles, follow these steps:

1. Create a dictionary file with the MIR Profiles:
touch dictionary.cambium
2. Edit dictionary.cambium according to the instructions that you can find under /usr/local/etc/raddb directory in file dictionary.

For example:

```
ATTRIBUTE Cambium-ePMP-ULMIR 110 integer #Max Burst Uplink Rate
```

```

ATTRIBUTE Cambium-ePMP-DLMIR 110 integer #Max Burst Downlink Rate
VENDOR Cambium 17713
#
# Cambium vendor-specific attributes.
#
BEGIN-VENDOR Cambium
ATTRIBUTE Cambium-ePMP-ULMIR 26 integer #Max Burst Uplink Rate
ATTRIBUTE Cambium-ePMP-DLMIR 27 integer #Max Burst Downlink Rate

```

3. Create link on your dictionary:

```
#ln -s dictionary.cambium dictionary.local
```

4. To configure MIR profiles, edit `usr/local/etc/raddb/users` and add profiles for each client below users configuration :

```
SubscriberModule33 Cleartext-Password := "cambium33"
Cambium-ePMP-ULMIR = 100,
Cambium-ePMP-DLMIR = 100
```

```
SubscriberModule34 Cleartext-Password := "cambium34"
Cambium-ePMP-ULMIR = 110,
Cambium-ePMP-DLMIR = 110
```

```
SubscriberModule35 Cleartext-Password := "cambium35"
Cambium-ePMP-ULMIR = 120,
Cambium-ePMP-DLMIR = 120
```

Example scenarios of MIR and RADIUS configurations are described in [Table 149](#).

Table 149: Example scenarios of MIR and RADIUS configurations

Scenario	Description
No MIR control via Radius	In a scenario where Radius is not in use for MIR profiles, the GUI will be the only place to configure MIR profiles and apply them to the corresponding SMs. Configure the MIR profiles in the Configure > Quality of Service menu option on the AP GUI and apply the corresponding profile # in the SM under the same menu option on SM.

Scenario	Description
MIR control using only Radius	In the case where only the Radius server is being used for MIR profiles, all settings in the GUI will be overridden for any SM being managed by the Radius Server. In this case, create the MIR profile with Subscriber Module usernames and passwords on the Radius server. At the time of registration, the AP uses the radius information and applies the corresponding profile to the SM. In the wireless statistics page (> Wireless Status), the MIR profile # from the Radius server along with UL and DL rate information will show up. In this scenario the QoS profiles in the AP GUI are irrelevant. Multiple SMs across multiple APs can then be managed via Radius.
Hybrid control using both Radius and MIR profile on the AP GUI	The system also supports a hybrid mode where Radius and the GUI QoS profiles can be used simultaneously as long as the same SM does not have a profile # associated with the AP & Radius. In a case where it is redundant, the Radius server setting will override the MIR profile settings from the GUI.

Creating certificate for Radius server and SM device

Create your own certification center

Creating a CA private key

1. Create a root (self-signed) certificate from our private certificate. Go to the directory where the database is stored for our certificates and start generating.
2. Create a private key CA (my own Certificate Authority). RSA key length of 2048 bits encryption algorithm 3DES. Filename with a key - cambium-ca.key

```
openssl genrsa -des3 -out cambium-ca.key 2048
```

Generating RSA private key, 2048 bit long modulus

```
..... + + +
```

```
..... + + +
```

e is 65537 (0x10001)

Enter pass phrase for cambium.key:

Verifying - Enter pass phrase for cambium-ca.key:

3. While creating the private key, you must enter a passphrase, which will be closed by key (and confirm it). The content key can be viewed from the following command:

```
openssl rsa -noout -text -in cambium-ca.key
```

In this case, you must enter the private key again.

Creating a CA certificate

1. Generate a self-signed certificate CA:

```
openssl req -new -x509 -days 3650 -key cambium-ca.key -out cambium-ca.crt
```

2. Enter pass phrase for cambium.key:

You are asked to enter information that will be incorporated into your certificate request.

What you enter is called a Distinguished Name or a DN. There are quite a few fields of which you can leave some blank. For some fields, there is a default value,

If you enter '.', the field is left blank.

Country Name (2 letter country code)

State or Province Name (full name)

Locality Name (Ex. City)

Organization Name (Ex, Cambium Networks)

Organizational Unit Name (Ex. Cambium)

Common Name (Ex. cambium root CA)

Email Address (Ex. admin@cambium.com)

3. Generating the certificate, you must enter a passphrase, with a closed key CA, and then - to fill in the required fields (company name, email, etc.); the most important of these is the Common Name - the unique name of the certification center.

In this case, as the Common name was chosen "cambium root CA", view the resulting certificate command as shown below:

```
openssl x509 -noout -text -in cambium-ca.crt
```

As a result, we see:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

ea: 30:7 b: 69 : a2: 13:0 c: 70

Signature Algorithm: md5WithRSAEncryption

Issuer: C = UA, ST = Euro, L = Kiev, O = Cambium Networks, OU = Cambium,

CN = cambium root CA / email address = admin@cambium.com

Issued to (by us, that is self-signed)

Validity

Not Before: Dec 9, 2005 11:34:29 GMT

Not After: Dec 7, 2015 11:34:29 GMT

Validity of the certificate

Subject: C = UA, ST = Euro, L = Kiev, O = Cambium Networks, OU = Cambium,

CN = cambium root CA / email address = admin@cambium.com

Filter (field) certificate

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00: c0: ff: 50 : fd: a8: eb: 07:9 b: 17 : d1: a9: e2: a5: dc:
59: a7: 97:28:9 f: bc: a4: 01:16:45:37: f5: 8d: ca: 1e:
12: ca: 25:02:8 a: cf: ee: ae: 35:59: ed: 57:89: c7: 2b:
17:9 f: 8b: de: 60 : db: e5: eb: b3: de: 09:30:3 b: a9: 68:
40: f7: f8: 84 : f4: 6c: b2: 24:3 d: ed: 45 : a3: 8a: 66:99:
40: a9: 53:0 c: 75 : e3: df: f3: ef: 20:0 c: a6: 3f: f2: dd:
e9: 1c: f5: d1: c1: 32:4 c: 44 : fd: c1: a2: d9: e6: e0: dc:
04:0 c: f8: dd: 9e: 31 : aa: 9d: 60 : b0: 84 : d2: e0: b7: a5:
eb: 82:31:4 f: 71 : c4: ee: ab: 5c: 8e: ef: 8c: a1: 1a: 2a:
62: e9: e9: 36 : ff: 12 : b9: c9: ac: 0e: 4d: ac: 08:97:87:
d2: 30:2 f: 41 : a1: 9e: ef: 8b: bf: c6: cf: 66:70:02: ab:
2d: b0: 9c: 56 : b8: 13 : e8: 92:59: f5: d9: 33 : d7: 33:6 a:
7c: cb: 9b: 92 : ee: 4b: 22:32:73:59:70:3 f: b1: f6: 1b:
67:1 d: 28 : eb: bb: 4b: 5e: 61:95:43:78: d5: 3b: db: e1:
37 : f1: ec: 0d: db: 50:65:22: cb: f4: f9: b8: 2a: c6: 1f:
2b: e9: f8: 64:03:4 f: 36 : dc: 72:8 e: be: 3d: 12:8 a: ca:
8b: 95

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

4C: 80 : F5: 82:4 C: A4: 52 : DF: 9E: 0C: OD: 64:74:68:1 E: 45 : F6: C1: C7: 68

X509v3 Authority Key Identifier:

keyid: 4C: 80 : F5: 82:4 C: A4: 52 : DF: 9E: 0C: OD: 64:74:68:1 E: 45 : F6: C1: C7: 68

DirName :/ C = UA / ST = Euro / L = Kiev / O = Cambium Networks / OU = Cambium /

CN = cambium root CA / emailAddress = admin@cambium.com

serial: EA: 30:7 B: 69 : A2: 13:0 C: 70

X509v3 Basic Constraints:

CA: TUAE

Signature Algorithm: md5WithRSAEncryption

```
57 : db: 0d: 2b: 27 : eb: 0a: 97:7 f: b1: 37 : b3: d1: d7: 14 : a6: 80:66:
    3d: 7c: 00:4 a: 45:1 f: 7c: 2b: 5e: 30 : b2: 72:74:9 f: 6d: 33:82: f7:
    f7: de: 54 : a9: 2b: e7: ea: 1b: 93 : bd: cc: 74:4 f: 11 : ed: 94:0 b: b9:
    b2: 1f: b1: 86:6 e: c6: 48:71:48:9 b: 2b: 0a: 36 : f3: ab: d6: f9: 75 :
    c9: 0d: 1b: e9: 2c: 85:04: fc: 17:9 a: 94 : b9: 14:0 d: 15 : d1: 1e: 8b:
    bb: 9e: 91 : ca: 40:8 c: d8: ef: dd: 4a: 75 : d0: b9: 62 : d4: ee: 1b: e5:
    b5: 7e: fa: f1: 5d: 62 : d1: 78 : b0: 34:04: bb: 60:37:8 a: a8: 74:88:
    f6: 94:3 b: c8: fb: c0: 98 : f4: 94 : e9: d5: 53:8 e: 31 : e6: 25:56: c3:
    84:7 c: 46 : b9: 09:5 f: e3: 43 : a8: 57 : c9: 3a: d9: 3d: a7: b0: 41 : db:
    ea: ca: 60:28:0 b: a3: f0: 0b: e6: d6: c0: 5b: 15:0 c: f8: 19:36:26:
    d3: 2a: 8d: c9: 67 : fe: 04:6 f: e9: bf: f9: 55 : de: 2c: 92:04:81:6 f:
    43 : d5: 94:25: af: 83 : b8: 01:22: c8: 1a: 7e: 2e: a9: 10 : b0: e5: 35 :
    a7: 17 : bf: 65 : a1: 31:55:85: ba: 10:24:71:03:3 b: d6: 71 : a4: ad:
    48:28:46:8 f: 7e: e6: b3: 8c: 37:97:4 f: 36:05:8 c: f6: d1: 40 : a8:
    c4: 58:9 b: 28
```

4. Now copy the certificate and key of the CA in a public place, for example, in /etc/ssl/cambium:

```
mkdir /etc /ssl /cambium
cp cambium-ca. * /etc/ssl/cambium/
```

Issuance of certificates

Script certificate generation

- Download (from the Cambium support web-site) the script sign_cert.sh. It allows you to create server/user.
- Edit the following lines:

```
ROOTCA = "cambium"
root CA name - Filename of the root certificate (without the suffix '-ca')
O = "Cambium Networks" - Name of the organization
C = "UA" - country
ST = "Euro" - staff
L = "Kiev" - city
OU = "Cambium" - unit
EMAIL = email@cambium.com - email
BITS = 2048 - Size of the generated key in bits
```

CLIENT_DAYS = 730 - Client certificate validity period in days

SERVER_DAYS = 1461 - Server certificate validity period in days

Lines related to the country, city, department, email, etc must be fixed (though not necessarily, this is default values that can be changed in the process of creating the certificate). Variables related to the terms of validity of the certificate can be left without changes.

Creating a server certificate (for RADIUS)

1. Create a server certificate (option server_cert), filename (and certificate) radius.cambium.com.

```
./ sign_cert.sh server_cert radius.cambium.com
```

```
create certificate key: radius.cambium.com.key
```

Generating RSA private key, 2048 bit long modulus

```
..... + + +
```

```
..... + + +
```

```
e is 65537 (0x10001)
```

```
# First generates key, it is necessary enter the password which will close the key
```

```
Enter pass phrase for radius.cambium.com.key:
```

```
Verifying - Enter pass phrase for radius.cambium.com.key:
```

```
decrypt certificate key: radius.cambium.com.crt
```

```
Enter pass phrase for radius.cambium.com.key:
```

```
writing RSA key
```

```
# Create a certificate request
```

```
Create certificate request: radius.cambium.com.csr
```

```
./ sign_cert.sh radius.cambium.com server_cert
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

2. Then you must specify the fields you want, like for the root certificate. Default values have already populated in square brackets. To use them simply click ENTER.

- Your Country Name (2 letter country code):
- State or Province Name (full name):
- Locality Name (Ex.- city)
- Organization Name (Ex.- Cambium Networks):
- Organizational Unit Name (Ex.- Cambium):
- Common Name (Ex.- radius.cambium.com):
- Email Address (Ex.- email@cambium.com):

Sign the certificate request

sign certificate by CA: radius.cambium.com.crt

sign ca is: cambium-ca

CA signing: radius.cambium.com.csr -> radius.cambium.com.crt:

Using configuration from ca.config

3. Since we sign new created certificate with root certificate, we must enter the password which we used to close root certificate of our center CA

Enter pass phrase for. /.. / cambium-ca.key:

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName: PRINTABLE: 'UA'

stateOrProvinceName: PRINTABLE: 'Euro'

localityName: PRINTABLE: 'Kiev'

organizationName: PRINTABLE: 'Cambium Networks'

organizationalUnitName: PRINTABLE: 'Cambium'

commonName: T61STRING: 'radius.cambium.com'

emailAddress: IA5STRING: 'email@cambium.com'

Certificate is to be certified until Dec 25 12:05:18 2013 GMT (730 days)

Everything is OK, completing work

Server certificate is created.

Vendor-Specific Attribute (VSA) Reference

The ePMP RADIUS Dictionary file defines all of the ePMP Vendor-specific Attributes that can be utilized in the radio network. This file must be stored on the RADIUS server to be able to provision RADIUS users and clients with VSA configurations or to control administrator login credentials and privileges.

Table 150: ePMP VSA additional details

Attribute Name	Number OFOF0F ¹	Bridge Mode	NAT / Router Mode	GUI Analogue	Valid Values Usage Examples
Cambium-ePMP-VLIGVID	26.17713.21	Applicable	Not Applicable	Data VLAN ID	1-4094
Cambium-ePMP-VLMGVID	26.17713.22	Applicable	Applicable	AP or SM in Bridge Mode: Management VLAN ID	1-4094
				SM in NAT or Router Mode with Separate Management IP Enabled: VLAN (Data) > VLAN ID SM in NAT or Router Mode with Separate Management IP Disabled: VLAN (Management + Data) > VLAN ID	
Cambium-ePMP-ULMIR	26.17713.26	Applicable	Applicable	Uplink Maximum Information Rate (MIR)	100-1000000 (kbps)
Cambium-ePMP-DLMIR	26.17713.27	Applicable	Applicable	Downlink Maximum Information Rate (MIR)	100-1000000 (kbps)
Cambium-ePMP-UserLevel	26.17713.50	Applicable	Applicable	Section Account Management	2-5 2 - Installer (permission to read and write parameters applicable to unit installation and monitoring)

¹26 connotes Vendor-specific Attribute, per RFC 2865

Attribute Name	Number OFOF1	Bridge Mode	NAT / Router Mode	GUI Analogue	Valid Values Usage Examples
					3 - Administrator (full read and write permission) 4 - User (permission only to access pertinent information for support purposes) 5 - Readonly (permission to only view the Monitor page)
Cambium-ePMP-STAPRI	26.17713.51	Applicable	Applicable	Subscriber Module Priority	0-2 0 - Normal 1 - High 2 - Low
Cambium-ePMP-VLANMEMSET	26.17713.52	Applicable	Not Applicable	Membership VLANs table	1-4094 (for each VLAN ID in the range) Example: To set a VLAN Membership range from VLAN ID 256 (Begin) to VLAN ID 300 (End), in the RADIUS users file set: Cambium-ePMP-VLANMEMSET = "16777516"

¹26 connotes Vendor-specific Attribute, per RFC 2865

Attribute Name	Number OFOF1	Bridge Mode	NAT / Router Mode	GUI Analogue	Valid Values Usage Examples
					This decimal value in hex is 0x0100012C. In this case, the first two bytes represent the beginning of the range, 0x0100 (256 in decimal), and the last two bytes represent the end of the range, 0x012C (300 in decimal).
Cambium-ePMP-VLManagPVID	26.17713.53	Applicable	Applicable	AP or SM in Bridge Mode: Management VLAN Priority	0-7
				SM in NAT or Router Mode with Separate Management IP Enabled: VLAN (Data) > VLAN Priority SM in NAT or Router Mode with Separate Management IP Disabled: VLAN (Management + Data) > VLAN Priority	
Cambium-ePMP-VLDataPVID	26.17713.54	Applicable	Not Applicable	Data VLAN Priority	0-7
Cambium-ePMP-VLMG2VID	26.17713.55	Not Applicable	Applicable	Separate Management VLAN > VLAN ID	1-4094

¹26 connotes Vendor-specific Attribute, per RFC 2865

Attribute Name	Number OFOF1	Bridge Mode	NAT / Router Mode	GUI Analogue	Valid Values Usage Examples
Cambium-ePMP-VLMG2PVID	26.17713.56	Not Applicable	Applicable	Separate Management VLAN > VLAN Priority	0-7
Cambium-ePMP-VLMultiCastVID	26.17713.57	Applicable	Not Applicable	Multicast VLAN ID	1-4094
Cambium-ePMP-VLMAPPING	26.17713.58	Applicable	Not Applicable	VLAN Mapping table	<p>1-4094 (for each VLAN ID in the range)</p> <p>Example:</p> <p>To map C-VLAN 23 to S-VLAN 400, in the RADIUS users file set:</p> <p>Cambium-ePMP-VLMAPPING = "1507728"</p> <p>This decimal value in hex is 0x00170190. In this case, the first two bytes represent the C-VLAN value 0x0017 (23 in decimal) and the last two bytes represent the S-VLAN value 0x0190 (400 in decimal).</p>

¹26 connotes Vendor-specific Attribute, per RFC 2865

Chapter 7: Operation and Troubleshooting

This chapter provides instructions for operators of ePMP networks. The following topics are described:

- [General Planning for Troubleshooting](#)
- [Upgrading device software](#)
- [Testing hardware](#)
- [Troubleshooting the radio link](#)
- [Using the device external reset button](#)
- [Resetting ePMP to factory defaults by power cycling](#)

General Planning for Troubleshooting

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

Procedure:

1. Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
2. Identify commands and other sources that can capture baseline data for the site. These may include:
 - Ping
 - tracert or traceroute
 - Throughput Test results
 - Throughput data
 - Configure GUI page captures
 - Monitor GUI page captures
 - Session logs
3. Start a log for the site, including:
 - Operating procedures
 - Site-specific configuration records
 - Network topology
 - Software releases
 - Types of hardware deployed

- Site-specific troubleshooting process
- Escalation procedures
- GPS latitude/longitude of each network element

General fault isolation process

Effective troubleshooting also requires an effective fault isolation methodology that includes

- Attempting to isolate the problem to the level of a system, subsystem, or link, such as
 - AP to SM
 - AP to CMM
 - AP to GPS
 - CMM to GPS
 - power
- Researching System Logs of the involved equipment.
- Answering the questions listed in the following section.
- Reversing the last previous corrective attempt before proceeding to the next.
- Performing only one corrective attempt at a time.

Questions to help isolate the problem

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

1	<p>What is the history of the problem?</p> <ul style="list-style-type: none"> • Have we changed something recently? • Have we seen other symptoms before this?
2	<p>How wide-spread is the symptom?</p> <ul style="list-style-type: none"> • Is the problem on only a single SM? (If so, focus on that SM.) • Is the problem on multiple SMs? If so: <ul style="list-style-type: none"> • is the problem with one AP in the cluster? (If so, focus on that AP) • is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs) • is the problem with all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
3	<p>Based on data in the System Log</p> <ul style="list-style-type: none"> • Is intermittent connectivity indicated? (If so, verify your configuration, power level, CINR, cables and connections, and the speed duplex of both ends of the link).

	<ul style="list-style-type: none"> Does the problem correlate to loss-of-sync events?
4	Are connections made via shielded cables?
5	Does the GPS antenna have an unobstructed view of the entire horizon?

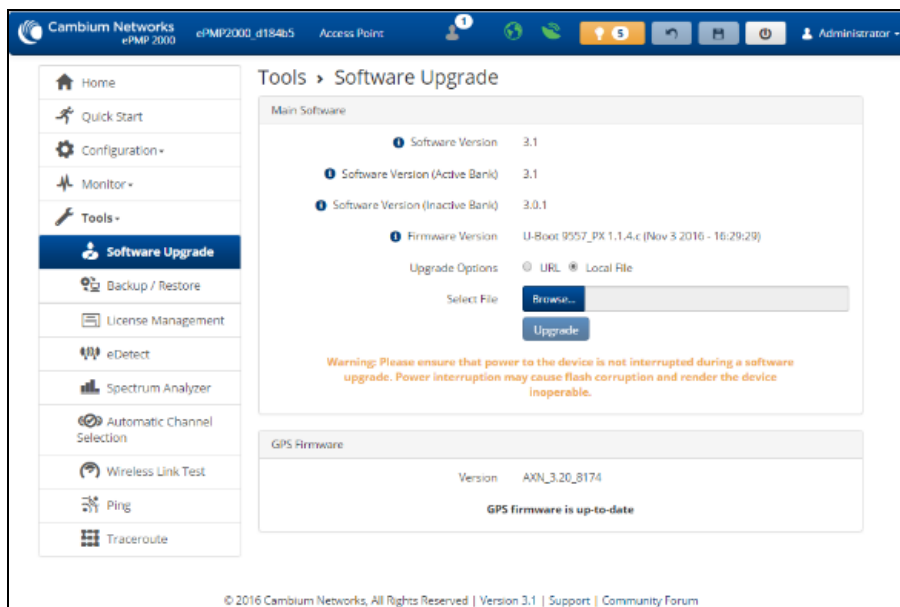
Upgrading device software

To take advantage of new features and software improvements for the ePMP system, monitor the Cambium Networks PMP Software website: <https://support.cambiumnetworks.com/files/epmp>

To upgrade the device software (AP or SM), follow this:

Procedure:

1. When upgrading multiple v1.0.3 integrated devices, ensure that the browser cache is cleared at the beginning of the upgrade process.
2. Log in to the device GUI via the management IP.
3. Navigate to page Tools, **Software Upgrade**.



4. Under the **Main Software** section, set the **Upgrade Option** to **URL** to pull the software file from a network software server or select **Local File** to upload a file from the accessing device. If **URL** is selected, enter the server IP address, Server Port, and File path.
5. If **Local File** is selected, click **Browse** to launch the file selection dialogue.

6. Click **Upgrade**.



Caution

Do not power off the unit in the middle of an upgrade process.

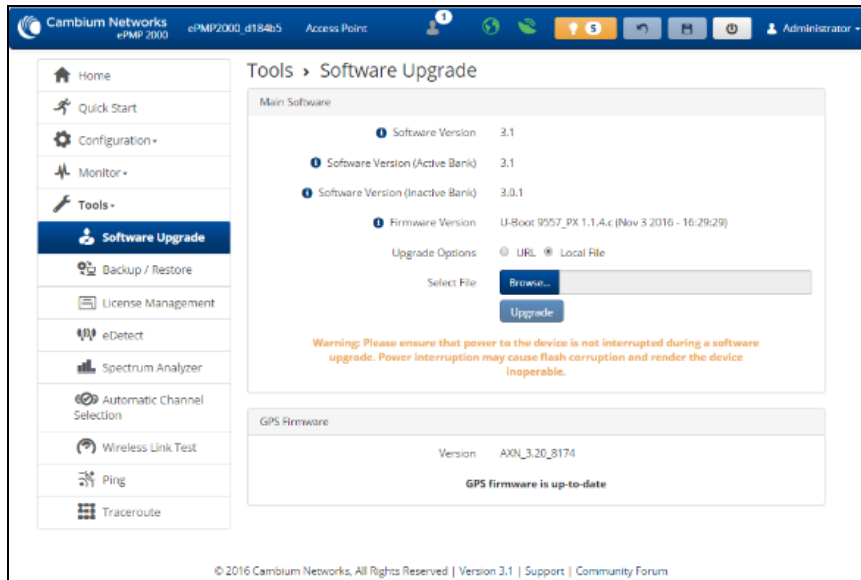
7. Once the software upgrade is complete, click the **Reset** icon.

Upgrading on-board GPS chip firmware

To upgrade the GPS Synchronized ePMP radio's onboard GPS chip, follow this:

Procedure:

1. When upgrading multiple v1.0.3 (or later) integrated devices, ensure that the browser cache is cleared at the beginning of the upgrade process.
2. Log in to the device GUI via the management IP.
3. Navigate to page Tools, **Software Upgrade**.



4. Under the section **GPS Firmware**, set the **Upgrade Options** to **URL** to pull the software file from a network software server or select **Local File** to upload a file from the accessing device.



Note

Use the same package that is used to upgrade the device's software. The new GPS firmware is part of the software upgrade packages.

5. If **Local File** is selected, click **Browse** to launch the file selection dialogue and click **Upgrade**.



Caution

Do not power off the unit in the middle of an upgrade process.

6. Once the software upgrade is complete, click the **Reset** icon.



Caution

In the case of a locked GPS device the upgrade typically has a "GPS Firmware Version" as "Not Available"(although not always). The user must attempt the upgrade anyway. It is however likely to fail with a "GPS general communication error" displayed in the notification icon. If this occurs the user must power-cycle (not just reboot) the radio and attempt the upgrade again.

GPS Chip and Software Reference

	ePMP 1000 (1st Generation)	ePMP 1000 (2nd Generation)	ePMP 2000
GPS Chip Type	GPS only	GPS + GLONASS	GPS + GLONASS
Default GPS Firmware	AXN_1.51_2801	AXN_3.20_8174	AXN_3.20_ 8174
Potential Issues (With Default Firmware Installed)	GPS chip locked, resulting in loss of sync and no display of firmware version or visible/tracked satellites	Occasional sync loss following a low number of tracked satellites for customers in APAC and Russian regions	Occasional sync loss following a low number of tracked satellites for customers in APAC and Russian regions
Current GPS Firmware	AXN_1.51_2838	AXN_5.1._8174	AXN_5.1._8174
Corresponding ePMP Software Release	2.1	3.5.1	3.5.1
Known issues (With Current GPS Firmware)	None	None	None

Testing hardware

This section describes how to test the hardware when it fails on startup or during operation.

Before testing hardware, confirm that all outdoor cables, that is those that connect the AP or SM to equipment inside the building, are of the supported type, as defined in [Ethernet cabling](#).

Checking the power supply LED

When the power supply is connected to the main power supply, the expected LED behavior is:

- The Power (green) LED illuminates steadily.

If the expected LED operation does not occur, or if a fault is suspected in the hardware, check the LED states and choose the correct test procedure:

- [Power LED is off](#)
- [Ethernet LED is off](#)

Power LED is off

Meaning: Either the power supply is not receiving power from the AC/DC outlet, or there is a wiring fault in the unit.

Action: Remove the AP/SM cable from the PSU and observe the effect on the Power LED. If the Power LED does not illuminate, confirm that the mains power supply is working, for example, check the plug. If the power supply is working, report a suspected power supply fault to Cambium Networks.

Ethernet LED is off

Meaning: There is no Ethernet traffic between the AP/SM and power supply.

Action: The fault may be in the LAN or AP/SM cable:

- Remove the LAN cable from the power supply, examine it and confirm it is not faulty.
- If the PC connection is working, remove the AP/SM cable from the power supply, examine it, and check that the wiring to pins 1&2 and 3&6 is correct and not crossed.

Test Ethernet packet errors reported by AP/SM

Log in to the AP or SM and click **Monitor, Performance**. Click **Reset System Counters** at the bottom of the page and wait until **LAN RX – Total Packet Counter** has reached 1 million. If the counter does not increment or increments too slowly, because for example the ePMP system is newly installed and there is no offered Ethernet traffic, then abandon this procedure and consider using the procedure [Test ping packet loss](#).

Check the **LAN RX – Error Packet Counter** statistic. The test has passed if this is less than 10.

Test Ethernet packet errors reported by managed switch or router

If the AP/SM is connected to a managed Ethernet switch or router, it may be possible to monitor the error rate of Ethernet packets. Please refer to the user guide of the managed network equipment. The test has passed if the rate of packet errors reported by the managed Ethernet switch or router is less than 10 in 1 million packets.

Test ping packet loss

Using a computer, it is possible to generate and monitor packets lost between the power supply and the AP/SM. This can be achieved by executing the Command Prompt application which is supplied as standard with Windows and Mac operating systems.



Caution

This procedure disrupts network traffic carried by the AP or SM under test.

Procedure:

1. Ensure that the IP address of the computer is configured appropriately for connection to the AP or SM under test, and does not conflict with other devices connected to the network.
2. If the power supply is connected to an Ethernet switch or router then connect the computer to a spare port, if available.
3. If it is not possible to connect the computer to a spare port of an Ethernet switch or router, then the power supply must be disconnected from the network to execute this test:
 - Disconnect the power supply from the network.
 - Connect the computer directly to the LAN port of the power supply.
4. On the computer, open the Command Prompt application.
5. Send 1000 ping packets of length 1500 bytes. The process will take 1000 seconds, which is approximately 17 minutes.

If the computer is running a Windows operating system, this is achieved by typing (for an IPv6 address, use the ping6 command):

```
ping -n 1000 -l 1500 <ipaddress>
```

where <ipaddress> is the IP address of the AP or SM under test.

If the computer is running a MAC operating system, this is achieved by typing:

```
ping -c 1000 -s 1492 <ipaddress>
```

where <ipaddress> is the IP address of the AP/SM under test.

6. Record how many Ping packets are lost. This is reported by Command Prompt on completion of the test.

The test has passed if the number of lost packets is less than 2.

Troubleshooting the radio link

This section describes how to test the link when there is no radio communication, when it is unreliable, or when the data throughput rate is too low. It may be necessary to test both the AP and the SM.

Module has lost or does not establish radio connectivity

If there is no wireless activity, follow this:

Procedure:

1. Check that the AP and SMs are configured with the same **Frequency Carrier**. Also, if operating in a region where DFS is required, ensure that the SM's **Frequency Carrier List** contains the frequencies configured in the AP's **DFS Alternate Frequency Carrier 1** and **DFS Alternate Frequency Carrier 2** fields.
2. Check that the **Channel Bandwidth** is configured the same at the AP and the SM.
3. On the AP, verify that the **Max Range** setting is configured to a distance slightly greater than the distance between the AP and the furthest SM that must register to the AP.

4. Check that the AP's **Synchronization Source** is configured properly based on the network configuration.
5. Verify the authentication settings on the AP and SM. If **Authentication Type** is set to **WPA2**, verify that the **Pre-shared Key** matches between the AP and the SM **Preferred AP List**.
6. Check that the software at each end of the link has the same version.
7. Check that the desired AP's SSID is configured in the SM **Preferred AP List**.
8. On the SM, check the **DL RSSI** and **DL CINR** values. Verify that for the SM installed distance, that the values are consistent with the values reported by the LINKPlanner tool.
9. Check Tx Power on the AP and SM.
10. Check that the link is not obstructed or the AP/SM misaligned.
11. Check the DFS status page (**Monitor, System Status**) at each end of the link and establish that there is a quiet wireless channel to use.
12. If there are no faults found in the configuration and there is absolutely no wireless signal, retry the installation procedure.
13. If this does not work then report a suspected AP/SM fault to Cambium Networks.

Link is unreliable or does not achieve data rates required

If there is some activity but the link is unreliable or does not achieve the data rates required, proceed as follows:

Procedure:

1. Check that the interference has not increased by monitoring the uplink and downlink CINR values reported in the AP page **Monitor, Wireless Status**.
2. Check that the RSSI values reported at the AP and SM are proper based on the distance of the link – the LINKPlanner tool is designed to estimate these values.
3. Check that the path loss is low enough for the communication rates required.
4. Check that the AP or SM has not become misaligned.
5. Review your Quality of Service configuration and ensure that traffic is properly classified and prioritized.

Module Has Lost or Does Not Gain GPS Synchronization

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

Procedure:

1. If the AP is receiving synchronization via CMM, verify that the CMM is properly receiving sync via its attached GPS antenna (see PMP Synchronization Solutions User Guide). Verify that the cables from the CMM to the network switch are at most 30 Ft (shielded) or 10 Ft (unshielded) and that the network switch is not PoE (802.3af) capable.

2. If the CMM is receiving GPS synchronization pulses, verify that the AP's **Synchronization Source** is set to **CMM** and that the AP's GPS status bar icon is lit green.
3. If the AP is receiving synchronization via its internal GPS module and an external GPS antenna, verify the cabling from the AP to the GPS antenna, and verify that the AP's **Synchronization Source** is set to **GPS**.

Using the device external reset button

ePMP APs and SMs feature an external button that serves two purposes:

- To reset the device (briefly depress the button for more than two seconds but less than ten seconds then release).

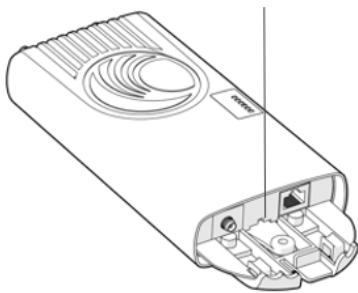


Caution

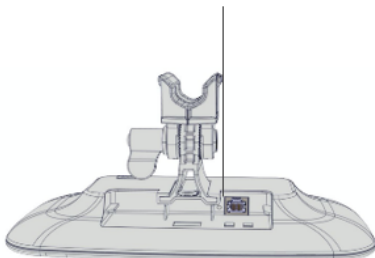
If the reset button is pressed for more than ten seconds while powered on, the device will reset back to its factory default configuration.

- To reset the device to its factory default configuration (depress the button for more than ten seconds then release).

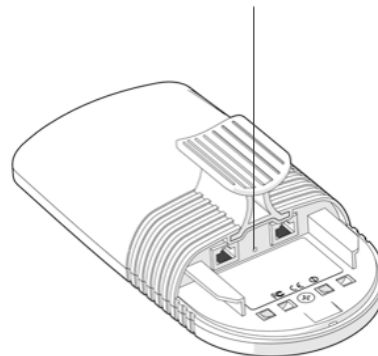
ePMP 1000 Connectorized Radio with Sync / ePMP 1000 Connectorized Radio Reset Button



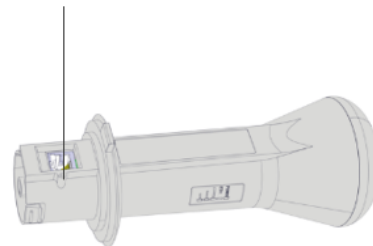
Force 180 Reset Button

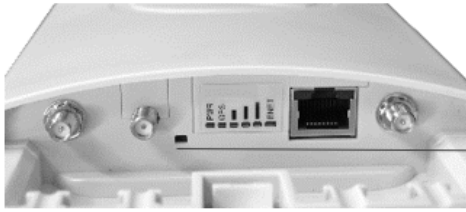


ePMP 1000 Integrated Radio Reset Button



Force 200 Reset Button

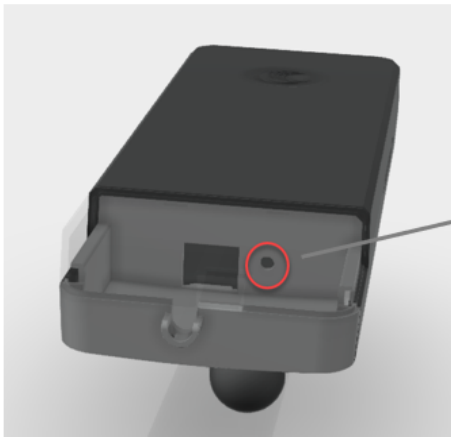




ePMP 2000 Access Point with Intelligent Filtering and Sync Reset Button



Force 190 Reset Button



Force 130 Reset Button

Resetting ePMP to factory defaults by power cycling

Operators may reset an ePMP radio to the default factory configuration by a sequence of power cycling (removing and re-applying power to the device). This procedure allows operators to perform a factory default reset without a tower climb or additional tools. The procedure is depicted in [Figure 91 Power cycle timings](#).

Procedure:

1. Remove the Ethernet cable from the PoE jack of the power supply for at least 10 seconds.
2. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds** and disconnect the cable to power off the ePMP device for **3-5 seconds**. (1st power cycle).
3. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds** and disconnect the cable to power off the ePMP device for **3-5 seconds**. (2nd power cycle).
4. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds** and disconnect the cable to power off the ePMP device for **3-5 seconds**. (3rd power cycle).
5. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds** and disconnect the cable to power off the ePMP device for **3-5 seconds**. (4th power cycle).
6. Reconnect the Ethernet cable to re-supply power to the ePMP device for at least **30 seconds** and allow it to go through the boot-up procedure (Note: Device will go through an additional reset automatically). This will reset the current configuration files to factory default configuration (e.g. IP addresses, Device mode, RF configuration, etc.). The device can be pinged from a PC to check if boot-up is complete (Successful ping replies indicate boot-up is complete).
7. Access the ePMP device using the default IP address of 192.168.0.1 (AP) or 192.168.0.2 (SM).

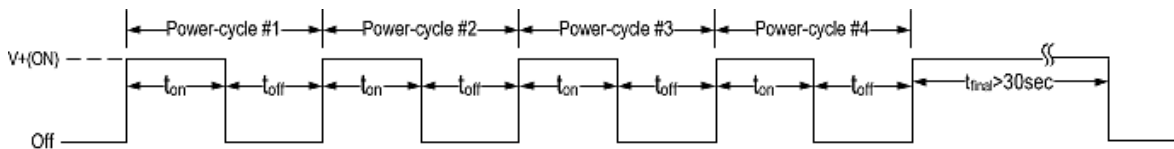


Figure 96: Power cycle timings

Where:	Is:
V+(ON)	Power through PoE has been applied to the device
Off	Power through PoE has been removed from the device
t _{on}	The time duration for which the device has been powered on. This should be 3-5 seconds.
t _{off}	The time duration for which the device has been powered off. This should be 3-5 seconds.

Recovery of flash-corrupted ePMP devices

All ePMP radios, except the Connectorized Radios with Sync, have a single flash bank. There is a high probability that the flash bank can get corrupted when power to the radio is interrupted during a flash write, i.e. software upgrade. This is not an issue with the Sync radio since there are two flash banks in the radio - one active and the other inactive. The inactive bank will take over if the active bank is corrupted.

Beginning with Release 2.6.2, it is now possible to recover an ePMP radio's corrupted flash. To perform the recovery, the ePMP radio **MUST** be running Release 2.6.2 or higher. Recovery is not supported on devices running earlier releases or on Connectorized Radio with Sync (GPS radios).

Procedure:

1. ePMP radio (non-GPS radio) with corrupted flash, i.e. there was a power interruption during a software upgrade and the device is no longer accessible or boots up.
2. The ePMP radio must have already been running Release 2.6.2 (or higher).
3. Laptop or PC with a 3rd party TFTP server (ex: <http://tftpd32.jounin.net>).

To perform the recovery procedure, the following is needed:

Recovery Procedure:

1. Connect the PC/Laptop to the ePMP device (non-GPS radio).
2. The PC/Laptop must be deployed in the same network as the ePMP device.
3. TFTP Server IP address must be set to 192.168.1.10/255.255.255.0.
4. Extract the ePMP recovery image (*firmware.bin*) from the ePMP software bundle (*ePMP-NonGPS_Synced-[Version].tar.gz*) and place it in the TFTP Server's root directory.
5. Reboot the ePMP device.
6. After successful boot-up, the ePMP device will perform the recovery procedure. The procedure will take approximately 5 minutes. Once done, the ePMP device will reboot automatically.
7. After boot-up, the ePMP device will be accessible using the last configured IP address or default local IP of 192.168.0.2 or the fallback IP of 169.254.1.1.

IMPORTANT: Software Upgrade through the GUI must be performed one more time for successful recovery to reflash the broken image.



Note

This recovery procedure will work in cases where the u-boot of the radio is intact. In rare cases where the u-boot may also be corrupted, recovery is not possible.

Flexible License Generation Procedure

To set up the Cambium Networks licensing portal to host ePMP Elevate licenses, follow this procedure:

Procedure:

1. Purchase the desired license product Entitlements from your Cambium Networks distributor (C060900S501A – one Elevate license, C050900S510A – 10 ePMP Elevate licenses).
2. Cambium Networks will email your Entitlements to the provided email address. An example of the email is displayed below:

Cambium Networks is pleased to deliver an Entitlement Certificate that you may use to redeem your recent purchase of software license key(s). To redeem this entitlement, please go to the [Cambium Support Center](#) and follow the instructions. If you need any assistance with this process, please contact Cambium Networks Support by [phone](#) or support@cambiumnetworks.com.

Entitlement Details			
Entitlement ID:	[REDACTED]	Start Date:	08/04/2017
Company:	[REDACTED]	End Date:	Never expires
Contact:	[REDACTED]		
Cambium Order Reference:			
Your Order Reference:			
Associated Products			
Product Number	Description	Quantity Ordered	Remaining Quantity
C050900S501A 1	ePMP Elevate: 1 Subscriber License	200	200
C050900S510A 1	ePMP Elevate: 10 Subscriber License	5	5

Cambium Networks Support

- Log into support.cambiumnetworks.com/licensekeys and navigate to Activate Entitlements. Enter your provided Entitlement ID in the Check Entitlements section and click the **Check** button. Entitlement details are listed in the dialogue below. Click **Activate** to activate the Entitlement's corresponding licenses.

The screenshot shows the 'License Keys' web interface. On the left, there is a sidebar with 'Entitlements' (containing 'Activate Entitlements', 'Recent Activations', and 'My Entitlements') and 'License Keys' (listing various product models like ePMP 1000/2000, PMP / PTP 450, etc.). The main content area is titled 'License Keys' and features a 'Check Entitlements' section with a text input field and a 'Check' button. Below this, an 'Entitlement:' section displays a table with the following data:

Part Number	Description	Available Quantity	
C050900S501A	ePMP Elevate: 1 Subscriber License	10 of 10	Activate

At the bottom right, there is a 'Chat' button and a link to 'Terms and Conditions | Privacy Policy'.

- Select Use Flexible Licensing.

Cambium Networks | Support Center Submit a request Martin Gray ▾

Knowledge Base Downloads Warranty License Keys Beta FAQ My Requests

License Keys

Entitlements

- Activate Entitlements
- Recent Activations
- My Entitlements

License Keys

- ePMP 1000/2000**
- PMP / PTP 450
- PTP 300/400/500/600/800
- PTP 650
- PTP 670
- PTP 700
- PTP 810
- PTP 820

ePMP Elevate Licensing

Part Number	Description	Quantity Available
C0509005501A	ePMP Elevate: 1 Subscriber License	10 of 10

ePMP Elevate Licenses can be bound to the MAC address of a single Access Point, or they can be deployed to a License Server and shared between multiple Access Points. How would you like to manage your licenses?

Flexible Licensing

With Flexible Licensing, your licenses are stored in a license server and can be shared among all your Access Points. Each Access Point will only use as many licenses as it has connected subscribers. When a subscriber disconnects, a license is returned to the pool and can be used by any other Access Point.

In order to use Flexible Licensing, your Access Points must:

- be able to make HTTPS requests out to the Internet.
- be running firmware version 3.5 or greater.
- have an accurate NTP time source.

[Use Flexible Licensing →](#)

Fixed Licensing

With Fixed Licensing, you will generate a license key for a specific MAC address, and load that license key into the Access Point. The license key represents the number of Elevate Subscribers that can be supported by that Access Point. The license key may not be transferred to any other Access Point.

You should use Fixed Licensing if your Access Points:

- are unable to make HTTPS requests to the Internet, or
- are running firmware version 3.4.1 or earlier, or
- don't have an accurate NTP time source.

[Use Fixed Licensing →](#)

Terms and Conditions | Privacy Policy [Chat](#)

5. Click **Activate** on the resulting page to activate your company account.

License Keys

Entitlements

- Activate Entitlements**
- Recent Activations
- My Entitlements

License Keys

- ePMP 1000/2000
- PMP / PTP 450
- PTP 300/400/500/600/800
- PTP 650
- PTP 670
- PTP 700
- PTP 810
- PTP 820

Cloud Licensing

Part Number	Description	Quantity Available
C0509005501A	ePMP Elevate: 1 Subscriber License	10 of 10

Cloud licenses must be associated with a company account. Please select the account you would like to use, or [create a new one](#).

Cambium ID	Name	Cloud Licensing ID
[Redacted]	[Redacted]	not assigned Activate →

[+ New Company Account](#)

6. On the resulting dialogue, enter the number of licenses to activate then click **Activate**.

License Keys

Cloud Licensing

You are going to activate cloud licenses for this Company account:

Cambium ID	Name	Cloud Licensing ID
MARTIN_GRAY	Martin Gray	60a62...

Please enter the quantity you would like to activate from the entitlement:

Description	Quantity Available	Quantity to Activate
ePMP Elevate: 1 Subscriber License	9 of 10	<input type="text" value="1"/>

[Activate](#)

- The recently-activated license keys are displayed, click **Details** to display the corresponding license key information.

License Keys

Serial Number, Part Number or Description 10 results [Search](#)

Date	Description	Serial Number	License
2017-08-21	ePMP Elevate: 1 Subscriber License	-	Details

- To use licenses from the pool, enter the corresponding Cloud Licensing ID on the AP's License Management page. See [AP Backup/Restore page](#) for more information.



Caution

Keep your **Cloud Licensing ID** secret to avoid unintended license pool usage!

Cambium Networks | Support Center

Submit a request Martin Gray

Knowledge Base Downloads Warranty License Keys Beta FAQ My Requests

License Keys

Entitlements

- Activate Entitlements
- Recent Activations
- My Entitlements

License Keys

- ePMP 1000/2000
- PMP / PTP 450
- PTP 300/400/500/600/800
- PTP 650
- PTP 670
- PTP 700
- PTP 810
- PTP 820

License Request: ePMP Elevate: 1 Subscriber License

State: Complete
Date: 2017-08-21
Entitlement ID: [redacted]
Quantity: 1
Cloud Licensing ID: [redacted]
Company Account: [redacted]

These licenses have been loaded into the Cambium Cloud Licensing system. To access them, enter the Cloud Licensing ID above into your device.

Enabling AP Flexible License Management

to configure the ePMP Access Point to retrieve Elevate licensing information from the Flexible license server, follow the following procedure.

Procedure:



Note

To use flexible licensing, the AP must:

1. be able to make HTTPS requests out to the Internet
2. be running firmware version 3.5.1 or greater
3. have an accurate NTP time source

1. Follow the steps in section [Flexible License Generation Procedure](#) to activate the applicable licenses on the Cambium Networks Support Center.
2. Copy the Cloud Licensing ID generated on the Support Center website:

License Request: ePMP Elevate: 1 Subscriber License

State: Complete
Date: 2017-08-21
Entitlement ID: [REDACTED]
Quantity: 1
Cloud Licensing ID: [REDACTED]
Company Account: [REDACTED]

These licenses have been loaded into the Cambium Cloud Licensing system. To access them, enter the Cloud Licensing ID above into your device.

3. Log into the ePMP AP and navigate to **Tools > License Management**.
4. Set License Server Agent to Enabled.
5. Paste the Cloud Licensing ID from Step 2 into the Cloud Licensing ID field.
6. Verify the license server connection in with field **Connection Status**.
7. Verify the enacted licensing in field **ePMP Elevate Subscriber Module Limit**

Flexible License Management

License Server Agent Disabled Enabled

Cloud Licensing ID [REDACTED]

Connection Status Connected. ePMP Elevate Subscriber Module Limit synced with License Server

Enable Proxy Disabled Enabled

Proxy Server IP Address [REDACTED]

Proxy Server Port 8080 min: 1 | max: 65535

Refresh Requests Failed 0

Update Requests Failed 0

NTP Status NTP Enabled, Date and Time is obtained from NTP Server

Date and Time 09 Jul 2018, 14:38:43 GMT

ePMP Elevate Subscriber Module Limit 1

Glossary

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
CINR	Carrier to Interference plus Noise Ratio
CMM	Cluster Management Module
CNSS	Cambium Network Services Server
DFS	Dynamic Frequency Selection
EIRP	Equivalent Isotropically Radiated Power
EMC	Electromagnetic Compatibility
EMD	Electromagnetic Discharge
ETH	Ethernet
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEC	Forward Error Correction
GPS	Global Positioning System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IC	Industry Canada
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LOS	Line of Sight
MIMO	Multiple In Multiple Out
MTU	Maximum Transmission Unit
nLOS	Near Line of Sight
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing

Term	Definition
PC	Personal Computer
PMP	Point to Multipoint
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keyed
RF	Radio Frequency
RMA	Return Merchandise Authorization
RSSI	Received Signal Strength Indication
RTTT	Road Transport and Traffic Telematics
RX	Receive
SAR	Standard Absorption Rate
SNMP	Simple Network Management Protocol
SM	Subscriber Module
SW	Software
TDD	Time Division Duplex
TDWR	Terminal Doppler Weather Radar
TX	Transmit
UNII	Unlicensed National Information Infrastructure
URL	Uniform Resource Locator