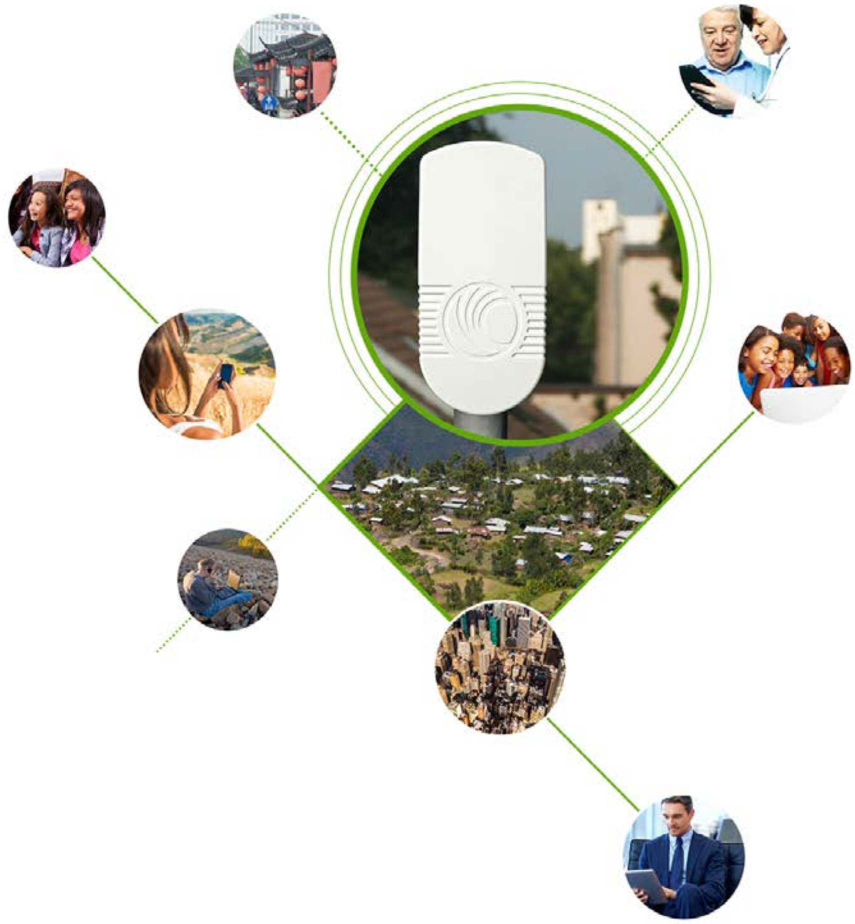
Cambium Networks



ePMP™

User Guide

System Release 1.4.3

- Product Description
- System Planning
- Configuration
- Operation and Troubleshooting
- Legal and Reference Information

Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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"). 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.

Safety and regulatory information

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

IMPORTANT SAFETY INFORMATION

Warning

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

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

Grounding and protective earth

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

Powering down before servicing

Always power down and unplug the equipment before servicing.

Primary disconnect device

The ePMP power supply is the primary disconnect device.

External cables

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

RF exposure near the antenna

Strong radio frequency (RF) fields will be present close to the antenna when the transmitter is on. Always turn off the power to the ePMP device before undertaking maintenance activities in front of the antenna.

Minimum separation distances

Install the ePMP device so as to provide and maintain the minimum separation distances from all persons.

The minimum separation distances for each frequency variant are specified in Calculated distances and power compliance margins on page 263.

IMPORTANT REGULATORY INFORMATION

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

Radar avoidance

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

The ePMP provides detect and avoid functionality for countries and frequency bands requiring protection for radar systems.

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

Contact the Cambium helpdesk if more guidance is required.

USA and Canada specific information

The USA Federal Communications Commission (FCC) has asked manufacturers to implement special features to prevent interference to weather radar systems that operate in the band 5600 MHz to 5650 MHz. These features must be implemented in all products able to operate outdoors in the band 5470 MHz to 5725 MHz.

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

In order to comply with these FCC requirements, Cambium supplies variants of the ePMP for operation in the USA or Canada. These variants are only allowed to operate with license keys and country codes that comply with FCC/IC rules. In particular, operation of radio channels overlapping the band 5600-5650 MHz is not allowed and these channels are permanently barred.

In addition, other channels may also need to be barred when operating close to weather radar installations.

Note

To ensure compliance with FCC rules (KDB 443999: Interim Plans to Approve UNII Devices Operating in the 5470 - 5725 MHz Band with Radar Detection and DFS Capabilities), follow Avoidance of weather radars on page 64.

Other variants of the ePMP are available for use in the rest of the world, but these variants are not supplied to the USA or Canada except under strict controls, when they are needed for export and deployment outside the USA or Canada.

Specific expertise and training required for professional installers

To ensure that the ePMP is installed and configured in compliance with the requirements of Industry Canada and the FCC, installers must have the radio engineering skills and training described in this section. This is particularly important when installing and configuring an ePMP system for operation in the 5.4 GHz UNII band.

Avoidance of weather radars

The installer must be familiar with the requirements in FCC KDB 443999. Essentially, the installer must be able to:

- Access the FCC data base of weather radar location and channel frequencies.
- Use this information to correctly configure the product (using the GUI) to avoid operation on channels that must be avoided according to the guidelines that are contained in the KDB and explained in detail in this user guide.

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

External antennas

When using a connectorized version of the product (as compared to the version with an integrated antenna), the conducted transmit power must be reduced to ensure the regulatory limit on transmitter EIRP is not exceeded. The installer must have an understanding of how to compute the effective antenna gain from the actual antenna gain and the antenna cable losses.

The product GUI automatically applies the correct conducted power limit to ensure that it is not possible for the installation to exceed the EIRP limit, when the appropriate values for antenna gain are entered into the GUI.

Ethernet networking skills

The installer must have the ability to configure IP addressing on a PC and to set up and control products using a web browser interface.

Lightning protection

To protect outdoor radio installations from the impact of lightning strikes, the installer must be familiar with the normal procedures for site selection, bonding and grounding. Installation guidelines for the ePMP can be found in section System planning on page 60.

Training

The installer needs to have basic competence in radio and IP network installation. The specific requirements applicable to the ePMP must be gained by reading this user guide and by performing sample set ups at base workshop before live deployments.

Contents

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

For radio equipment installation, refer the following guides:

- The *ePMP Quick Start Guide*
- The *ePMP Installation Guide*

Note

The *ePMP Installation Guide* is reproduced as an addendum to this user guide.

General information

VERSION INFORMATION

The following shows the issue status of this document:

Issue	Date of issue	Remarks
001v000	October 2013	System Release 1.0 (Software Release 1.1.6)
002v000	December 2013	System Release 1.0 (Software Release 1.2.3)
003v000	January 2014	System Release 1.0 (Software Release 1.3.4)
004v000	March 2014	System Release 1.0 (Software Release 1.4.1)
005v000	March 2014	System Release 1.0 (Software Release 1.4.3)

CONTACTING CAMBIUM NETWORKS

Support website:	http://www.cambiumnetworks.com/support
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	support@cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/support/contact-support/
Address:	Cambium Networks Limited, 3800 Golf Road, Suite 360 Rolling Meadows, IL 60008

Purpose

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

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

Cross references

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

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents.

For feedback, send mail to support@cambiumnetworks.com.

Problems and warranty

Reporting problems

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

1. Search this document and the software release notes of supported releases.
2. Visit the support website:
   http://www.cambiumnetworks.com/support/epmp
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 deployment.

Warnings, cautions, and notes

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

Warnings

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

Warning

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

Cautions

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

Caution

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

Notes

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

Note

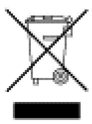
Note text.

Caring for the environment

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

In EU countries

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



Disposal of Cambium equipment

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

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, see http://www.cambiumnetworks.com/support

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.

Product description

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

The following topics are described in this chapter:

- Overview of ePMP on page 19 introduces the key features, typical uses, product variants and components of the ePMP.
- Wireless operation on page 21 describes how the ePMP wireless link is operated, including modulation modes, power control and security.
- System management on page 25 introduces the ePMP management system, including the web interface, installation, configuration, alerts and upgrades.

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 5 GHz and 2.4 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 Station. 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 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. This integrated PTP and PMP solution features an efficient GPS synchronized operational mode that permits highly scalable frequency reuse.

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

The wireless link is primarily TDD based. System Release 1.2.3 added 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 in order to support a primary and a secondary (future release) Ethernet port on the Station.

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 Stations. 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.

Table 1 gives a summary of the main ePMP characteristics.

Table 1 Main characteristics of the ePMP Series

Characteristic	Value
Topology	PMP or PTP
Wireless link condition	LOS, near LOS
Range	20 MHz: Up to 13 mi 40 MHz: Up to 9 mi
Scheduler	TDD or Flexible
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz and 2.4 GHz
Channel bandwidth	20 MHz, 40 MHz
Data rate	200+ Mbps

TYPICAL DEPLOYMENT EQUIPMENT

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

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

- **Connectorized Radio with GPS Sync:** A connectorized outdoor transceiver unit containing all the radio, networking, and surge suppression electronics.
- **Connectorized Radio Power Supply:** An indoor power supply module providing Power-over-Ethernet (PoE) supply and 1000/100/10 Base-TX to the Access Point.
- **Connectorized Radio Cabling and lightning protection:** Shielded Cat 5e cables, grounding cables, and connectors.
- **Integrated Radio:** An integrated-antenna outdoor transceiver unit containing all the radio, networking, antenna, and surge suppression electronics.
- **Un-synced 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 100/10 Base-TX to the Subscriber Module.
- **Integrated Radio Cabling and lightning protection:** Cat 5e cables and connectors

For more information about these components, including interfaces, specifications and Cambium part numbers, see System hardware on page 29.

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 STAs 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 sub carrier 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 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 in order to successfully demodulate a given modulation mode. Although the more complex modulations such as 64QAM 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) techniques provide protection against fading and increase the probability that the receiver will decode a usable signal.

The ePMP transmits two signals on the same radio frequency, one of which is vertically polarized and the other horizontally polarized.

RADAR AVOIDANCE

In regions where 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 actually interference on them.

Note

When operating in a region which requires DFS, ensure that the AP is configured with alternate frequencies and that the STA 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 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 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

PMP NETWORKS

Using frequency planning

Frequency planning is the exercise of assigning operating channels to PMP units so as 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 use of 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, or contact your Cambium distributor or re-seller.

FURTHER READING ON WIRELESS OPERATION

For information on planning wireless operation, see:

- Radio spectrum planning on page 61 describes the regulatory restrictions that affect radio spectrum usage, such as frequency range and radar avoidance.
- Link planning on page 65 describes factors to be taken into account when planning links, such as range, path loss and data throughput.
- Compliance with safety standards on page 261 lists the safety specifications against which the ePMP has been tested, and describes how to keep RF exposure within safe limits.
- Compliance with radio regulations on page 266 describes how the ePMP complies with the radio regulations that are enforced in various countries.
- Notifications on page 278 refer to compliance with the radio regulations that are enforced in various regions.
- Data throughput tables on page 287 contains tables and graphs to support calculation of the data rate capacity that can be provided by ePMP configurations.

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

- Configuration on page 70 describes the configuration parameters of the ePMP devices
- Operation and Troubleshooting on page 197 describes post-installation procedures and troubleshooting tips.

System management

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

The management agent supports the following interfaces:

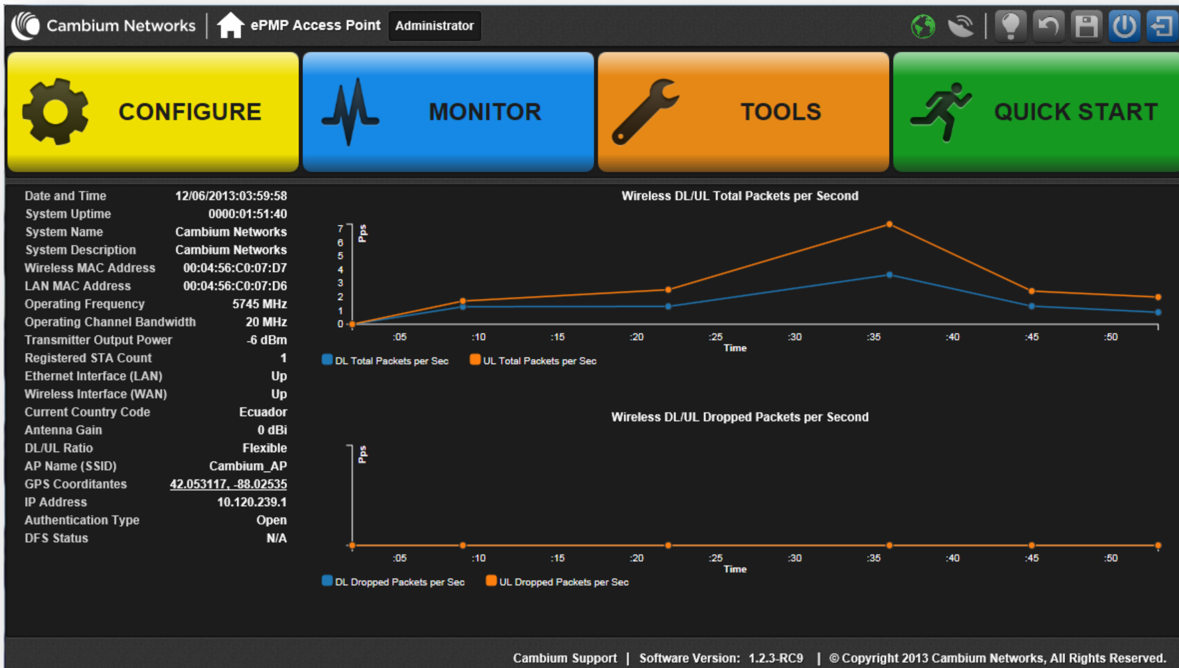
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol secure (HTTPs)
- Simple Network Management Protocol (SNMP)
- Network Time Protocol (NTP)
- System logging (Syslog)
- Cambium Network Services Server (CNSS) software
- Dynamic Host Configuration Protocol (DHCP)

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 installation of ePMP, and for the majority of ePMP configuration management tasks.

Figure 1 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 Station 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 by means of 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.

CAMBIUM NETWORK SERVICES SERVER

The Cambium Network Services Server (CNSS) may be used to monitor, configure, and upgrade Cambium network equipment.

For Cambium Network Services Server download, see
https://support.cambiumnetworks.com/files/cnss.

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 on page 104
- STA System page on page 148
- Operation and Troubleshooting on page 197

System hardware

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

The following topics are described in this chapter:

- Site planning on page 30 describes factors to be considered when planning the proposed network.
- Connectorized Module on page 32 describes the connectorized module hardware, part numbers, mounting equipment, and specifications.
- Integrated Module on page 40 describes the STA hardware, part numbers, mounting equipment, and specifications.
- Un-synced Connectorized Radio on page 46 describes the hardware, part numbers, mounting equipment, and specifications.
- Power supply on page 54 describes the power supply hardware, part numbers, and specifications.
- Connectorized module antennas and antenna cabling on page 39 describes the AP antenna and part numbers.
- Ethernet cabling on page 57 describes cable standards and lengths
- Surge Suppression unit on page 58 describes surge suppression requirements and recommendations.

Site planning

Conduct a site survey to ensure that the proposed AP and STA 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 STA.

There is only one Ethernet interface, a copper Cat5e connection from the AP or STA to the AP/STA power supply and network terminating equipment. If a 1000 Base-TX (Gigabit) Ethernet connection is required at the AP, ensure that power supply N000900L001A is utilized.

GROUNDING AND LIGHTNING PROTECTION

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.

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

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

Note

International and national standards take precedence over the requirements in this guide.

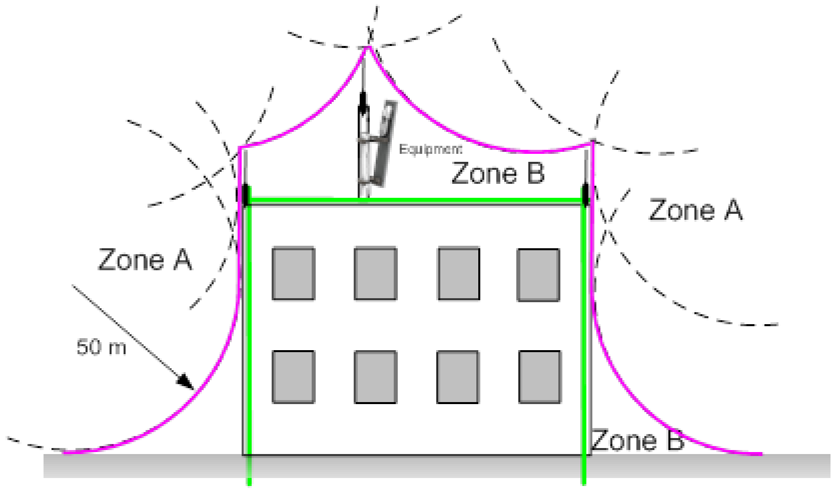
LIGHTNING PROTECTION ZONES

Use the rolling sphere method (Figure 2) to determine where it is safe to mount equipment. An imaginary sphere, typically 50 meters in radius, is rolled over the structure. Where the sphere rests against the ground and a strike termination device (such as a finial or ground bar), all the space under the sphere is considered to be in the zone of protection (Zone B). Similarly, where the sphere rests on two finials, the space under the sphere is considered to be in the zone of protection.

Figure 2 Rolling sphere method to determine the lightning protection zones

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

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



⚠ Warning

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

Connectorized Module

For details of the ePMP connectorized hardware, see:

CONNECTORIZED MODULE 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 Station (STA) in a Point-To-Multipoint (PMP) or in a Point-To-Point (PTP) network topology.

Figure 3 ePMP Series Connectorized Radio with Sync

Note

To select antennas, RF cables and connectors for connectorized units, see Connectorized module antennas and antenna cabling on page 39.

CONNECTORIZED PART NUMBERS

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

Each of the parts listed in Table 2 includes the following items:

- One connectorized unit
- One power supply 1000/100/10 Base-TX LAN injector

The GPS-capable parts listed in Table 2 also ship with a GPS antenna.

Table 2 Connectorized part numbers

Cambium description	Cambium part number
ePMP GPS, Conn - 5 GHz - no power cord	C050900A011A
ePMP GPS, Conn - 5 GHz - US power cord - FCC version	C058900A112A
ePMP Conn - 5 GHz - no power cord	C050900A021A
ePMP Conn - 5 GHz - US power cord - FCC version	C058900A122A
ePMP GPS, Conn - 2.4 GHz - US power cord	C024900A011A

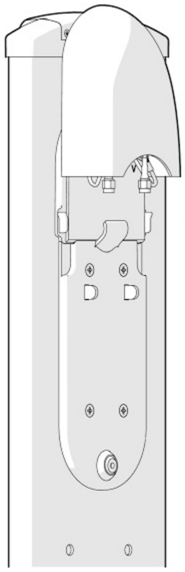
Table 3 AP accessory part numbers

Cambium description	Cambium part number
ePMP Power Supply for GPS Radio - no cord (spare)	N000900L001A
ePMP Power Supply for non-GPS Radio - no cord (spare)	N000900L002A

CONNECTORIZED MODULE MOUNTING BRACKET

The connectorized unit is designed to be attached to a Cambium ePMP sector antenna (see Table 10). The Cambium ePMP sector antenna contains all of the mounting brackets, antenna cabling, and GPS antenna mounting for device deployment.

Figure 4 Connectorized module sector antenna



CONNECTORIZED MODULE INTERFACES

The connectorized module interfaces are illustrated in Figure 5 and described in Table 4.

Figure 5 Connectorized module interfaces

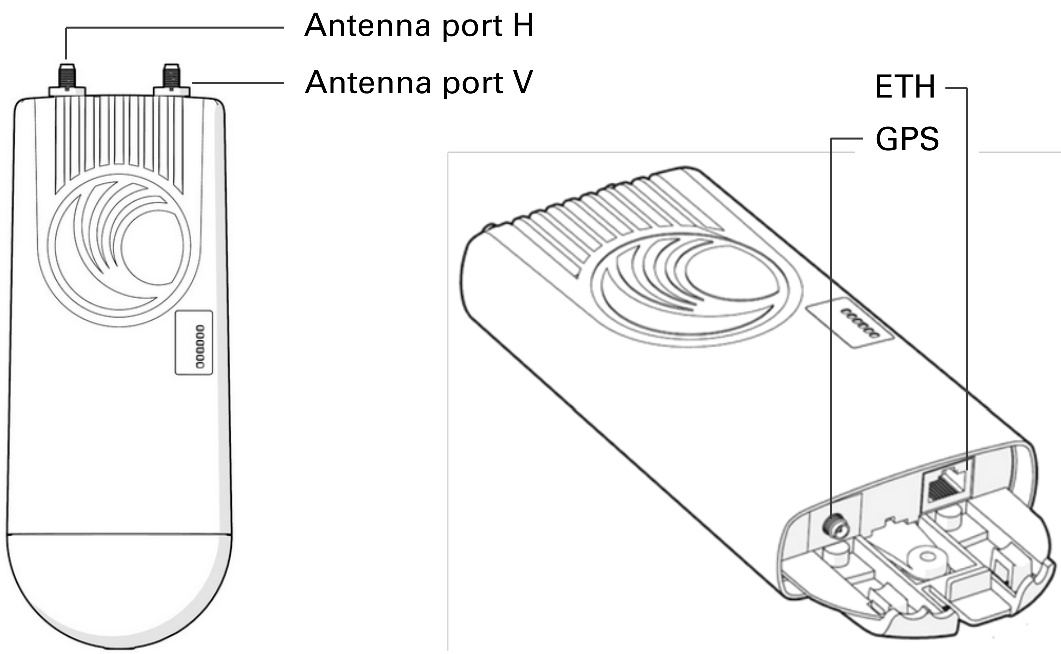
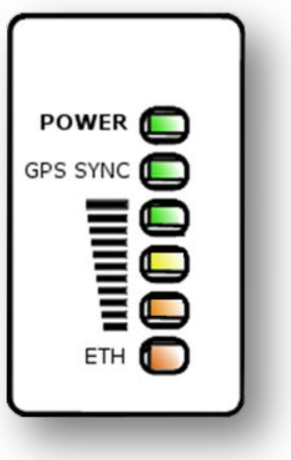


Table 4 Connectorized module interfaces

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
ETH	RJ45	PoE input	802.3af PoE Standard, as well as Proprietary power over Ethernet (PoE) twisted pair (for powering via CMM3/CMM4)
		10/100/1000 Base-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 on page 206.

CONNECTORIZED MODULE LEDS



LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
GPS SYNC	Orange: AP has acquired a 1PPS GPS synchronization pulse either from the internal GPS module and antenna or from a connected CMM Unlit: 1PPS GPS not acquired, or **Synchronization Source** set to **Internal** (AP generating sync, not GPS-based)
	Reserved for future release
ETH	Once lit, blinking indicates Ethernet activity Red: 10BaseTX link Green: 100BaseTX link Orange: 1000BaseTX link Unlit: No Ethernet link established

CONNECTORIZED MODULE SPECIFICATIONS

The ePMP connectorized module conforms to the specifications listed in Table 5 and Table 6.

The connectorized meets the low level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page 261 and provides internal surge suppression but does not provide lightning suppression.

For a full listing of connectorized radio specifications, see Connectorized Radio Specifications on page 288.

Table 5 Connectorized module 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	.521 kg (1.15 lbs) without antenna 4.5 kg (10 lbs) with antenna

Table 6 Connectorized module environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)
Wind loading	118 mph (190 kph) maximum. See Connectorized Module wind loading on page 38 for a full description.
Humidity	95% condensing
Environmental	IP55

CONNECTORIZED MODULE HEATER

Upon power on, if the ePMP connectorized module temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device is able to 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 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 7.

Table 7 Connectorized module 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 minutes, 30 seconds

CONNECTORIZED MODULE 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 on page 263.
- 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 Connectorized Module wind loading on page 38.

CONNECTORIZED MODULE 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 is 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 surface area of the device. Wind loading is estimated using the following formulae:

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

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

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

Where:	Is:
A	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 8 and Table 9.

Table 8 Connectorized module 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 9 Connectorized module 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 MODULE 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-v1.4.3.tar.gz

Connectorized module 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:

- Antenna requirements on page 39
- FCC and IC approved antennas on page 39

ANTENNA REQUIREMENTS

For connectorized units operating in the USA or Canada 2.4 GHz, 5.4 GHz or 5.8 GHz bands, choose external antennas from those listed in FCC and IC approved antennas on page 39. For installations in other countries, the listed antennas are advisory, not mandatory.

FCC AND IC APPROVED ANTENNAS

For connectorized units operating in the USA or Canada, choose external antennas from Table 10. 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.

⚠ Caution

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 Allowed antennas for deployment in USA/Canada

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

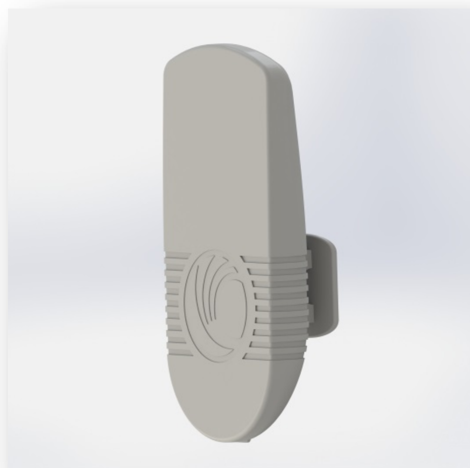
Integrated Module

For details of the ePMP integrated hardware, see:

- Integrated Module description on page 40
- Integrated Module part numbers on page 41
- Integrated Module mounting bracket on page 41
- Integrated Module interfaces on page 42
- Integrated Module specifications on page 43
- Integrated Module heater on page 44
- Integrated Module wind loading on page 44
- Integrated Module software packages on page 45.

INTEGRATED MODULE DESCRIPTION

Figure 6 ePMP Series Integrated Radio



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

INTEGRATED MODULE PART NUMBERS

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), and the other is for use in ETSI countries or the rest of the world (ETSI/RoW).

Each of the parts listed in Table 11 includes the following items:

- One integrated module (with mounting bracket)
- One metal mounting strap

Table 11 Integrated module part numbers

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

Table 12 Integrated module accessory part numbers

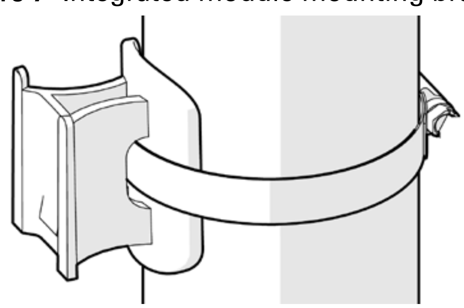
Cambium description	Cambium part number
ePMP Power Supply for non-GPS Radio - no cord (spare)	N000900L002A

INTEGRATED MODULE MOUNTING BRACKET

The integrated module is designed to be pole-mounted for use with a non-Cambium antenna.

Order integrated module mounting brackets from Cambium Networks.

Figure 7 Integrated module mounting bracket



INTEGRATED MODULE INTERFACES

The integrated module interfaces are illustrated in Figure 8 and described in Table 13.

Figure 8 Integrated module interfaces

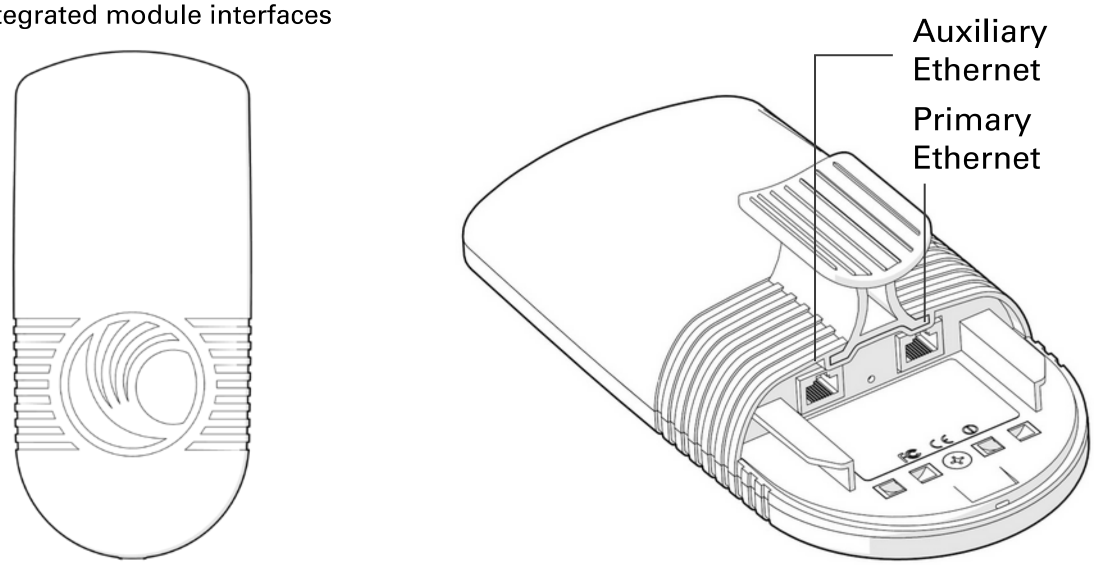
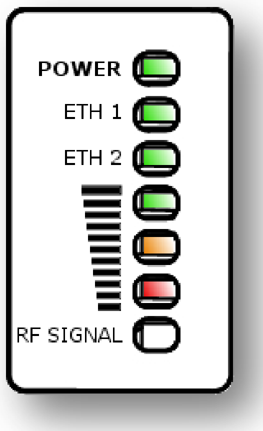
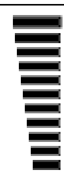


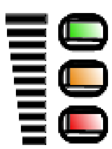
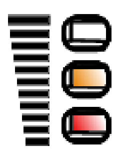
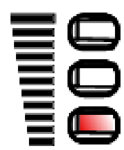
Table 13 Integrated module interfaces

Port name	Connector	Interface	Description
Primary Ethernet	RJ45	PoE input	Proprietary power over Ethernet (PoE) twisted pair (for powering via CMM3/CMM4)
		10/100 Base-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)

INTEGRATED MODULE 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: 10/100BaseTX link
ETH 2	Auxiliary/Secondary Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100BaseTX 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

INTEGRATED MODULE SPECIFICATIONS

The ePMP integrated module conforms to the specifications listed in Table 14 and Table 15.

The integrated device meets the low level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page 261 and provides internal surge suppression but does not provide lightning suppression.

For a full listing of integrated radio specifications, see Error! Reference source not found. on page Error! Bookmark not defined..

Table 14 Integrated module 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 15 Integrated module environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (131°F)
Wind loading	90 mph (145 kph) maximum. See Integrated Module wind loading on page 44 for a full description.
Humidity	95% condensing
Environmental	IP55

INTEGRATED MODULE 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 is able to 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 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 16.

Table 16 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 minutes, 30 seconds

INTEGRATED MODULE 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 surface area of the integrated module. Wind loading is estimated using the following formulae:

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

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

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

Where:	**Is:**
A	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 17 and Table 18.

Table 17 Integrated module 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 18 Integrated module 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

INTEGRATED MODULE 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-v1.4.3.tar.gz

Un-synced Connectorized Radio

For details of the ePMP connectorized hardware, see the following:

UN-SYNCED CONNECTORIZED RADIO 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 Station (STA) in a Point-To-Multipoint (PMP) or in a Point-To-Point (PTP) network topology.

Figure 9 ePMP Series Un-synced Connectorized Radio

Note

To select antennas, RF cables and connectors for connectorized units, see

Un-synced connectorized radio antennas and antenna cabling on page 53.

UN-SYNCED CONNECTORIZED RADIO PART NUMBERS

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

Each of the parts listed in Table 19 includes the following items:

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

Table 19 Un-synced Connectorized Radio part numbers

Cambium description	Cambium part number
ePMP 1000: 5 GHz Connectorized Radio (EU)	C050900A023A
ePMP 1000: 5 GHz Connectorized Radio (FCC)	C058900A122A
ePMP 1000: 5 GHz Connectorized Radio (ROW)	C050900A021A
ePMP 1000: 2.4 GHz Connectorized Radio	C024900A021A

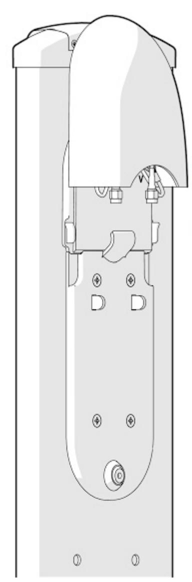
Table 20 AP accessory part numbers

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

UN-SYNCED CONNECTORIZED RADIO MOUNTING BRACKET

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

Figure 10 Un-synced connectorized radio sector antenna



UN-SYNCED CONNECTORIZED RADIO INTERFACES

The un-synced connectorized radio with interfaces are illustrated in Figure 11 and described in Table 21.

Figure 11 Un-synced connectorized radio interfaces

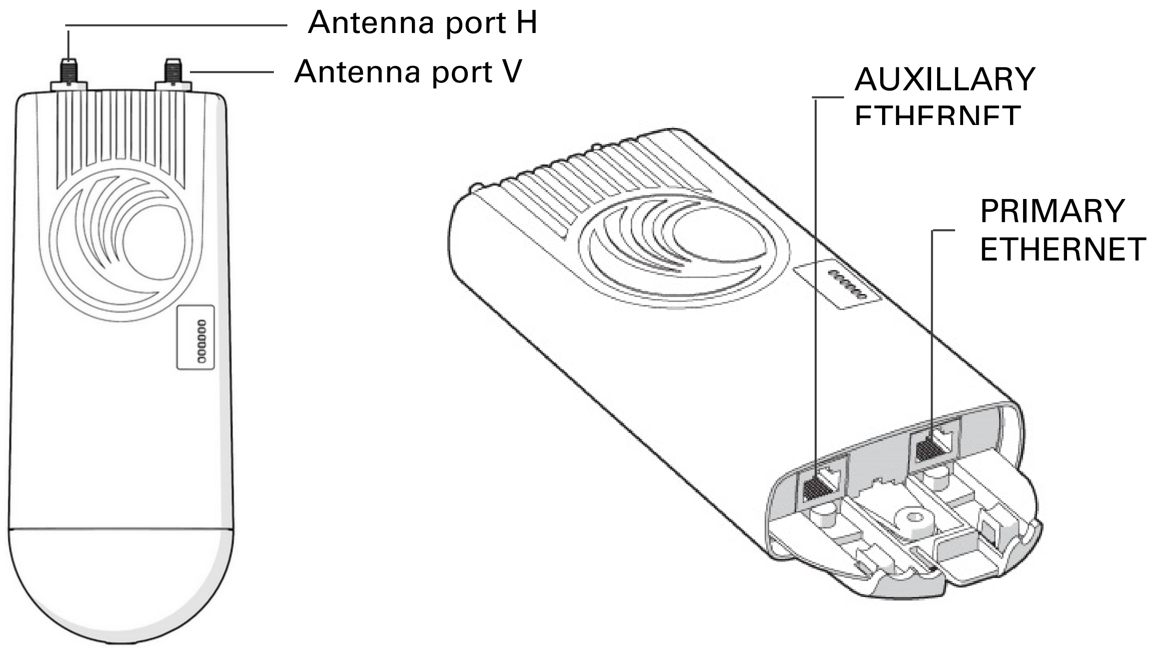
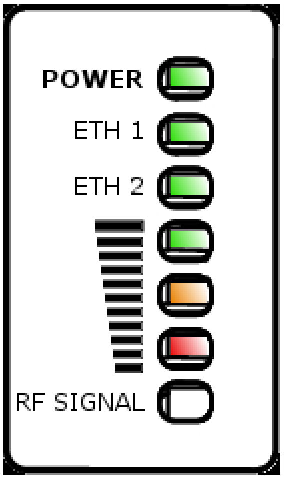


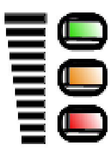
Table 21 Un-synced connectorized radio interfaces

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)
		10/100 Base-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 standard 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 on page 206.

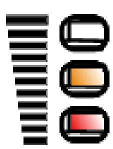
UN-SYNCED CONNECTORIZED RADIO LEDS



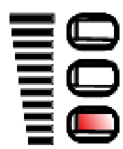
LED	Function
POWER	Green: Power is applied to the device Unlit: No power is applied to the device or improper power source
ETH 1	Main/Primary Ethernet port indicator Once lit, blinking indicates Ethernet activity Green: 10/100BaseTX link
ETH 2	Auxiliary/Secondary Ethernet port indicator Once lit, blinking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



RSSI
> -60
dBm



-70 dBm
< RSSI ≤≤
-60 dBm



-80 dBm
< RSSI ≤
-70 dBm

RSSI
≤ -80
dBm

UN-SYNCED CONNECTORIZED RADIO SPECIFICATIONS

The ePMP un-synced connectorized radio conforms to the specifications listed in Table 22 and Table 23.

The connectorized meets the low level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page 261 and provides internal surge suppression but does not provide lightning suppression.

For a full listing of connectorized radio specifications, see Connectorized Radio Specifications on page 288.

Table 22 Un-synced 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	.521 kg (1.15 lbs) without antenna 4.5 kg (10 lbs) with antenna

Table 23 Un-synced connectorized radio environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)
Wind loading	118 mph (190 kph) maximum. See Un-synced connectorized Radio wind loading on page 52 for a full description.
Humidity	95% condensing
Environmental	IP55

UN-SYNCED CONNECTORIZED RADIO HEATER

On startup, if the ePMP un-synced connectorized radio temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device is able to 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 24.

Table 24 Un-synced connectorized radio 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 minutes, 30 seconds

UN-SYNCED 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 on page 263.
- 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 Un-synced connectorized Radio wind loading on page 52.

UN-SYNCED 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:

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

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

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

Where:	Is:
A	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 25 and Table 26.

Table 25 Un-synced 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 26 Un-synced 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

UN-SYNCED CONNECTORIZED RADIO SOFTWARE PACKAGES

Un-synced 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 Un-synced connectorized radio are named:

- ePMP-NonGPS_Synced-v1.4.3.tar.gz

UN-SYNCED CONNECTORIZED RADIO ANTENNAS AND ANTENNA CABLING

Un-synced 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:

- Antenna requirements on page 39
- FCC and IC approved antennas on page 39

ANTENNA REQUIREMENTS

For connectorized units operating in the USA or Canada 2.4 GHz, 5.4 GHz or 5.8 GHz bands, choose external antennas from those listed in FCC and IC approved antennas on page 39. For installations in other countries, the listed antennas are advisory, not mandatory.

FCC AND IC APPROVED ANTENNAS

For connectorized units operating in the USA or Canada, choose external antennas from Table 27. 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.

Caution

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 27 Allowed antennas for deployment 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

Power supply

For details of the ePMP power supply units, see:

- Power supply description on page 54
- Power supply part numbers on page 54
- Power supply interfaces on page 55
- Power supply specifications on page 56
- Power supply location on page 56

POWER SUPPLY DESCRIPTION

The power supply is an indoor unit that is connected to the connectorized or integrated 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. One can order power supplies and line cords from Cambium Networks (Table 28). The power supplies listed in Table 28 may be used for both connectorized and integrated modules, however, only N000900L001A provides a Gigabit Ethernet interface (connectorized modules only).

Table 28 Power supply component part numbers

Cambium description	Cambium part number
ePMP Pwr Supply for GPS Radio - no cord (spare)	N000900L001A
ePMP Pwr Supply for non-GPS Radio - no cord (spare)	N000900L002A

POWER SUPPLY INTERFACES

The power supply interfaces are illustrated in Figure 12 and described in Table 29 and Table 31.

Figure 12 Power supply interfaces

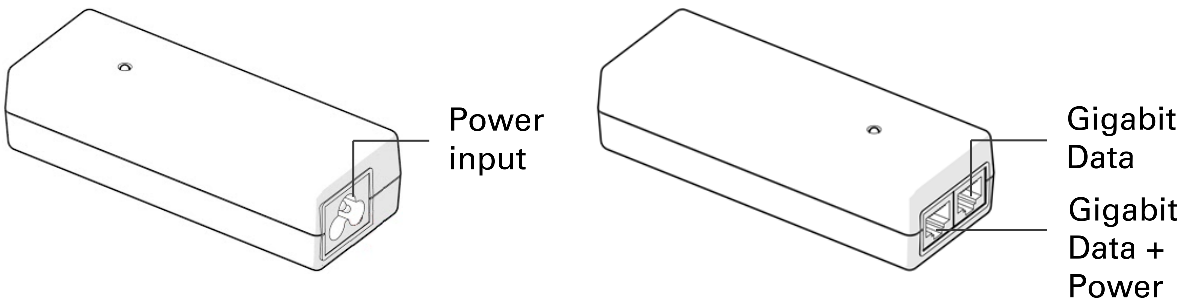


Table 29 Power supply interface functions - N000900L001A

Interface	Function
Power input	Mains power input.
Gigabit Data + Power	RJ45 socket for connecting Cat5e cable to radio Note This port provides a Gigabit Ethernet interface to ePMP connectorized radios. To ePMP integrated radios, this port provides a 100/10 Mbit/sec Ethernet interface.
Gigabit Data	RJ45 socket for connecting Cat5e cable to network.

Table 30 Power supply interface functions - N000900L002A

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

Table 31 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 32, Table 33 and Table 34. These specifications apply to all ePMP product variants.

Table 32 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 33 Power supply environmental specifications

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

Table 34 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 surface.
- The power supply is kept dry, with no possibility of condensation, flooding or rising damp.
- 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 34.

Ethernet cabling

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

- Ethernet standards and cable lengths on page 57
- Outdoor Cat5e cable on page 57

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.

Table 35 specifies, for each power supply, the maximum permitted drop cable length.

Table 35 Power supply drop cable length restrictions

Part number	Description	Maximum cable length (*1)
N000900L001A	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) Maximum length of Ethernet cable from AP/STA to power supply

OUTDOOR CAT5E CABLE

For copper connections from the device to the power supply, use Cat5e cable that is shielded with copper-plated steel.

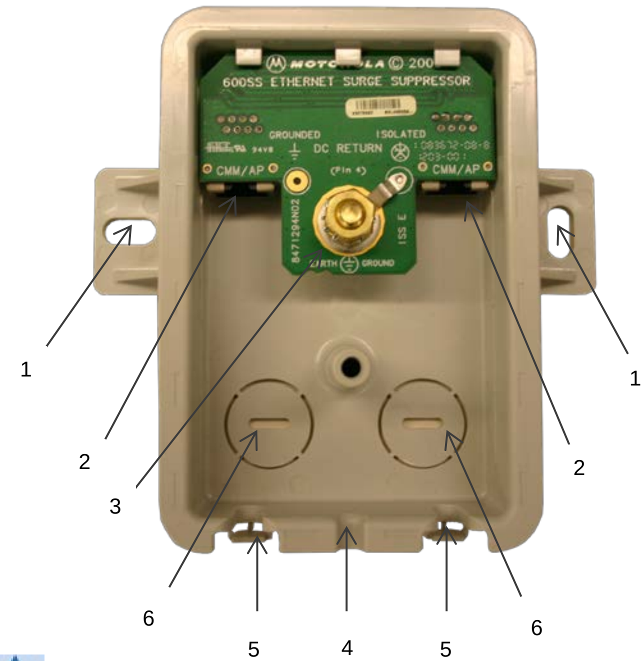
⚠ Caution

Always use Cat5e cable that is shielded with copper-plated steel. Alternative types of Ethernet cable are not supported by Cambium Networks.

Surge Suppression unit

The ePMP integrated and connectorized units both contain 1 Joule-rated surge suppression build into the device. With this built in surge suppression, it is not required to install a surge suppressor at the unit's mounting location. However, it is required to install a surge suppressor at the Ethernet cable's building ingress into the power supply's indoor location. For installations not requiring Gigabit (1000 Mbit/sec) Ethernet, a Cambium 600SSH surge suppressor may be used. See Cambium 600SSH details for information.

CAMBIUM 600SSH DETAILS



Note

For connectorized module installations requiring Gigabit (1000 Mbit/sec) Ethernet surge suppression, utilize the following:

Mfr	Part	Description
L-COM	AL-CAT6JW	Outdoor 10/100/1000 Base-T CAT6 PoE Compatible Lightning Protector
L-COM	AL-CAT6HPJW	Outdoor 10/100/1000 Base-T CAT6 PoE Compatible Lightning Protector – High Power (protection comparable to 600SSH)

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

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

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

Note The 600SSH surge suppressor is shipped in the "isolated" position (pin 4 isolated by 68V from protective earth). If packet error issues occur over the Ethernet link (verify by pinging the device through the 600SSH), configure the 600SSH to "grounded" position (by moving the 600SSH switch from "isolated" to "ground") to avoid ground loops that may be present in the system.

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

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

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

System planning

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

The following topics are described in this chapter:

- Radio spectrum planning on page 61 describes how to plan ePMP links to conform to the regulatory restrictions that apply in the country of operation.
- Link planning on page 65 describes factors to be taken into account when planning links, such as range, path loss and throughput.
- Planning for connectorized units on page 66 describes factors to be taken into account when planning to use connectorized APs with external antennas in ePMP links.
- Grounding and lightning protection on page 30 describes the grounding and lightning protection requirements of a ePMP installation.
- Data network planning on page 68 describes factors to be considered when planning ePMP data networks.

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

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

Note

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

GENERAL WIRELESS SPECIFICATIONS

Table 36 lists the wireless specifications that apply to all ePMP variants. Table 37 lists the wireless specifications that are specific to each frequency variant.

Table 36 ePMP wireless specifications (all variants)

Item	Specification
Channel selection	Manual selection (fixed frequency).
Manual power control	To avoid interference to other users of the band, maximum power can be set lower than the default power limit (AP only).
Integrated device antenna type	Patch antenna
Duplex scheme	Adaptive TDD
Range	13 mi (20 MHz channel bandwidth) 9 mi (40 MHz channel bandwidth)
Over-the-air encryption	AES
Error Correction	FEC

Table 37 ePMP wireless specifications (per frequency band)

Item	5 GHz	2.4 GHz
RF band (GHz)	5150 - 5875 MHz	2402 - 2472 MHz (20 MHz) 2407 - 2472 MHz (40 MHz)
Channel bandwidth	20 MHz 40 MHz	20 MHz 40 MHz
Typical antenna gain	Connectorized antenna – 15 dBi Integrated patch antenna – 13 dBi	Connectorized antenna - 15 dBi Integrated patch antenna - 11 dBi
Antenna beamwidth (integrated)	24° azimuth, 12° elevation	24° azimuth, 12° 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 on page 267.

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 x 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 x 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 x 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 on page 66. When operating in ETSI regions, it is required to enter a license key in the ePMP web management interface to unlock 5.8 GHz band 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 on page 64.

AVAILABLE SPECTRUM

The available spectrum for 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 which requires a general authorization of any 5.4 GHz radio link which is used outside the operator's own premises. It is the responsibility of the installer or operator to have the link authorized. For details, see:

http://www.sviluppoeconomico.gov.it/index.php?option=com_content&view=article&idmenu=672&idarea1=593&andor=AND&idarea2=1052&id=68433&sectionid=1,16&viewType=1&showMenu=1&showCat=1&idarea3=0&andorcat=AND&partebassaType=0&idareaCalendario1=0&MvediT=1&idarea4=0&showArchiveNewsBotton=0&directionidUser=0

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.
- UK and some other 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 on page 267.

Where regulatory restrictions apply to certain channels, these channels are barred automatically by the use of the correct country code. For example, at 5.8 GHz in the UK and some other 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 is dependent on the channel bandwidth.

For more information about configuring the **Country Code** parameter, see on AP Radio page on page 91 and STA Radio page on page 141.

CHANNEL BANDWIDTH

Select the required channel bandwidth for the link. The selection depends upon the ePMP frequency variant and country code, as specified in Examples of regulatory limits on page 267.

The wider the channel bandwidth, the greater its capacity. As narrower channel bandwidths take up lesser 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. In addition, 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 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 in order 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:

System Operating Margin (fade margin) dB = Rx signal level (dB) – Rx sensitivity (dB)

Thus, the fade margin is the difference between 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:

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

Where:	**Is:**
Maximum Power Level (dBm)	the highest permissible setting of the Maximum Power Level attribute in the 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, 5.4 GHz and 5.8 GHz have an operating bandwidth of 20 MHz or 40 MHz then the maximum allowed EIRP depends on the operating bandwidth of the radio as shown in Table 38.

Table 38 Normal EIRP limits with operating channel bandwidth

Operating bandwidth (MHz)	Allowed EIRP (dBm) at 5.2 GHz	Allowed EIRP (dBm) at 5.4 GHz	Allowed EIRP (dBm) at 5.8 GHz	Allowed EIRP (dBm) at 2.4 GHz
20, 40	30	30	36	36

The settings to be used for regions with the EIRP limits in Table 38 are shown in Table 39.

Table 39 Setting maximum transmit power to meet general EIRP limits

Antenna	Maximum available antenna gain (dBi)	Operating bandwidth (MHz)	Transmitter Output Power parameter setting (dBm)			
			5.2 GHz	5.4 GHz	5.8 GHz	2.4 GHz
Connectorized module sector	15	20, 40	15	15	21	21

antenna

Note

Table 39 is calculated on the basis of 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 40.

Table 40 ePMP 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	10/100/1000BaseT (RJ-45)
Data Rates	See Data throughput tables on page 287.
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/STA 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.

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

QUALITY OF SERVICE FOR BRIDGED ETHERNET TRAFFIC

Decide how 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.

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 on page 71
- Connecting to the unit on page 72
- Using the web interface on page 74
- Configuring connectorized radios using the Quick Start menu on page 83
- Configuring STA units using the Quick Start menu on page 86
- Using the AP menu options on page 89
- Using the STA menu options on page 139

Preparing for configuration

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

SAFETY PRECAUTIONS

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

Warning

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate as soon as they are powered up. Respect the safety standards defined in Compliance with safety standards on page 261, 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, see Compliance with radio regulations on page 264.

Connecting to the unit

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

- Configuring the management PC on page 72
- Connecting to the PC and powering up on page 73

CONFIGURING THE MANAGEMENT PC

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

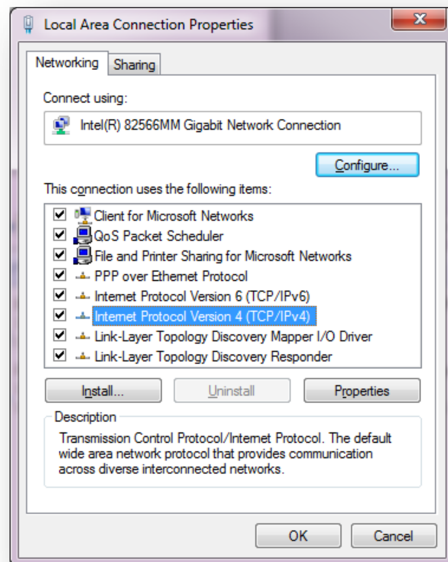
Procedure:

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:

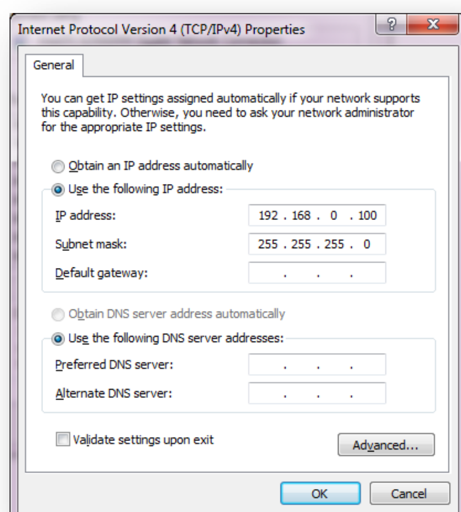
192.168.0.1, 192.168.0.2, and 192.168.03

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, 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 – see the *ePMP Installation Guide* for more information).
2. Connect the PC Ethernet port to the LAN (AP: "Gigabit Data", STA: "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 on page 201.

Using the web interface

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

- Logging into the web interface on page 75
- Layout of the web interface on page 76
- Configuring connectorized radios using the Quick Start menu on page 83
- Configuring STA units using the Quick Start menu on page 86
- Using the AP menu options on page 89
- Using the STA menu options on page 139

LOGGING INTO THE WEB INTERFACE

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

Equipment and tools:

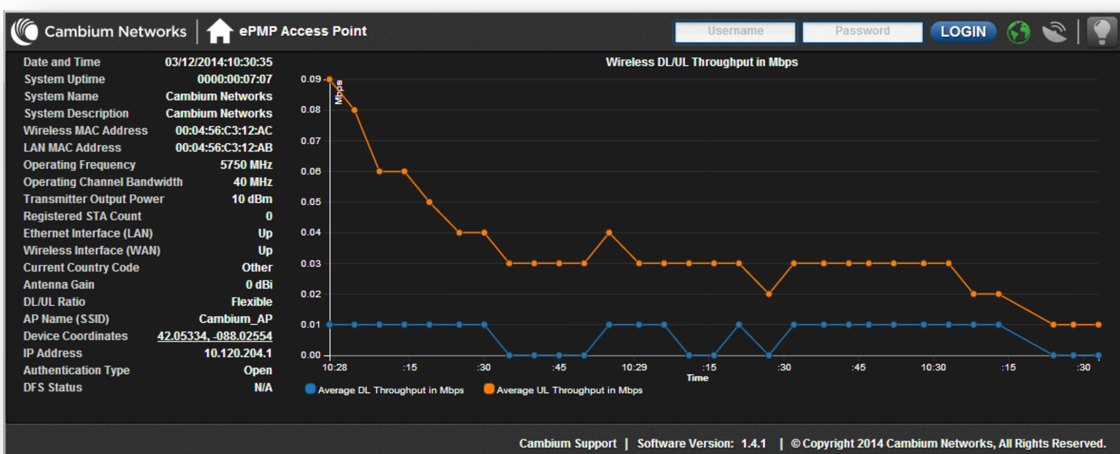
- Connectorized or integrated device connected to power supply by Ethernet cable.
- PC connected to power supply by Ethernet cable.
- Power Supply powered up.
- Supported browser – Chrome v29, Firefox v24, Internet Explorer 10, Safari v5

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** (connectorized radio) or **192.168.0.2** (integrated radio). Press ENTER. The web interface dashboard and login input is 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 (STA 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 10.1.1.254.



3. In the upper-right corner of the GUI, enter Username (default: admin) and Password (default:admin).
4. Click **Login**.

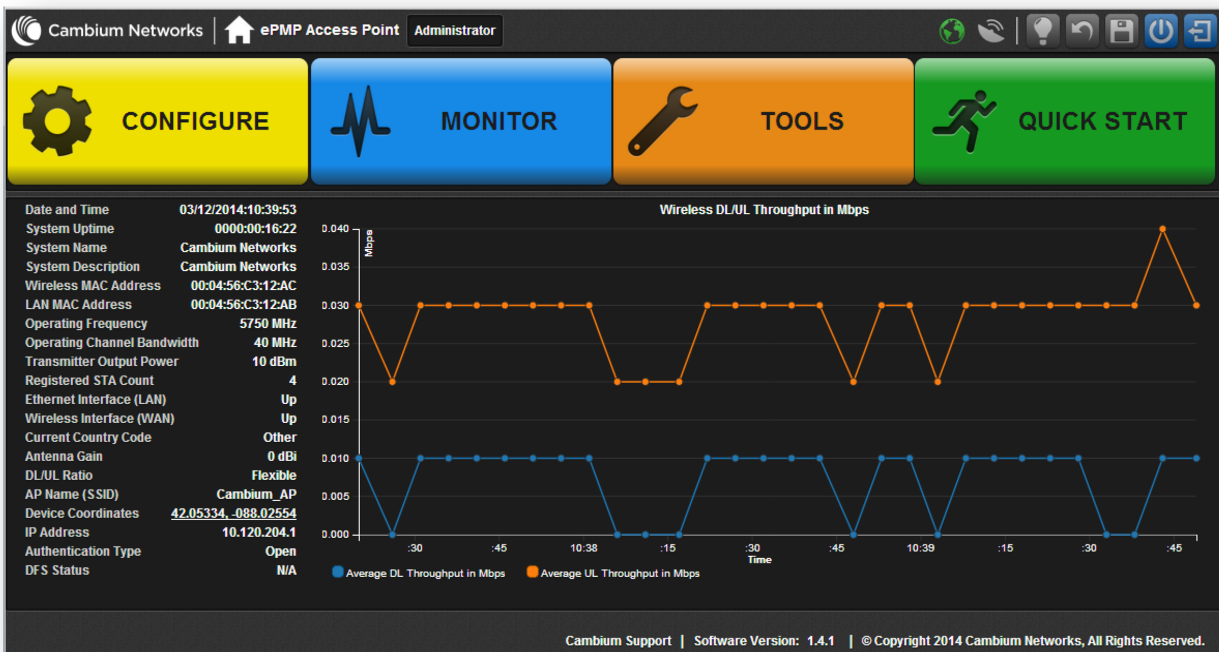
Note

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 **Configure**, **System**, **User 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**). To return to this display at any time, click the Home icon or device name (i.e. "ePMP Access Point")

Figure 13 GUI dashboard



The top of the interface contains the following attributes:

Table 41 GUI status bar attributes

Icon	Attribute	Meaning
	Cambium Networks logo	Hyperlink to the Cambium Networks website.
	Home Icon	Link to the device dashboard.
Administrator	Login Level indicator	Displays the current user login level.
	Internet Connectivity Indicator	**Green** indicates that the AP has IP connectivity to the configured DNS server. **Grey** indicates that the AP has no IP connectivity to the configured DNS server. Note The Internet Connectivity Indicator state is determined by receipt of ping responses from the configured DNS server.
	GPS Synchronization Receive Indicator	**Green** indicates that the AP is receiving a valid GPS synchronization timing pulse via a connected GPS antenna or a CMM. **Red** indicates that the AP is not receiving GPS synchronization due to lack of satellite fix. **Grey** indicates that the AP is not receiving GPS synchronization due to configuration of **Synchronization Source** to **Internal**.
	Notifications Button	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: **Green**: Successful operation has completed (i.e. Changes successfully saved) **Grey**: Informational message (i.e. tips regarding GUI operation) **Blue**: Operations information message (i.e. Initializing upgrade…) **Orange**: Warning message (i.e. Login session has expired) **Red**: Error message (i.e. Software update file download failed)

Icon	Attribute	Meaning
	Undo Button	The Undo button may be used to undo changes prior to 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.
	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 42 GUI footer attributes

Attribute	Meaning
Cambium Support link	Hyperlink to the Cambium Networks support website.
Software Version link	The current software version is reported in the footer bar, and may be clicked to navigate to the Cambium Networks software support website.
Copyright	Copyright information.

The AP dashboard contains the following attributes:

Table 43 AP dashboard attributes

Attribute	Meaning
Date and Time	The current date and time on the device, subject to the configuration of parameter **Time Zone**
System Uptime	The total uptime of the radio since the last reset.
System Name	The current configured system name.
System Description	The current configured system description.
Wireless MAC Address	The MAC address of the device wireless interface.
LAN MAC Address	The MAC address of the device LAN (Ethernet) interface.

Attribute	Meaning
Operating Frequency	The current frequency carrier used for radio transmission, based on the configuration of the **Frequency Carrier** parameter (in DFS regions, if a 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.
Registered STA Count	The total number of STAs currently registered to the STA.
Ethernet Interface (LAN)	**Up**: The Ethernet (LAN) interface is functioning properly **Down**: The Ethernet (LAN) interface has encountered an error and is not servicing traffic.
Wireless Interface (LAN)	**Up**: The radio (WAN) interface is functioning properly **Down**: The radio (WAN) interface has encountered an error and is not servicing traffic.
Current Country Code	The current configured country code, which has an effect on DFS operation and transmit power restrictions. Registered Stations will inherit this country code when registration is complete (unless STA is locked to US region).
Antenna Gain	The configured gain of the external antenna.
DL/UL 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.
AP Name (SSID)	The current configured name/SSID of the AP.
Device Coordinates	The current configured Latitude and Longitude coordinates in decimal format.
IP Address	The current configured device IP address (LAN) used for management access.
Authentication Type	The current configured authentication type used for radio link encryption as well as STA authentication.
DFS Status	Current DFS operational status.

The STA dashboard consists of the following attributes:

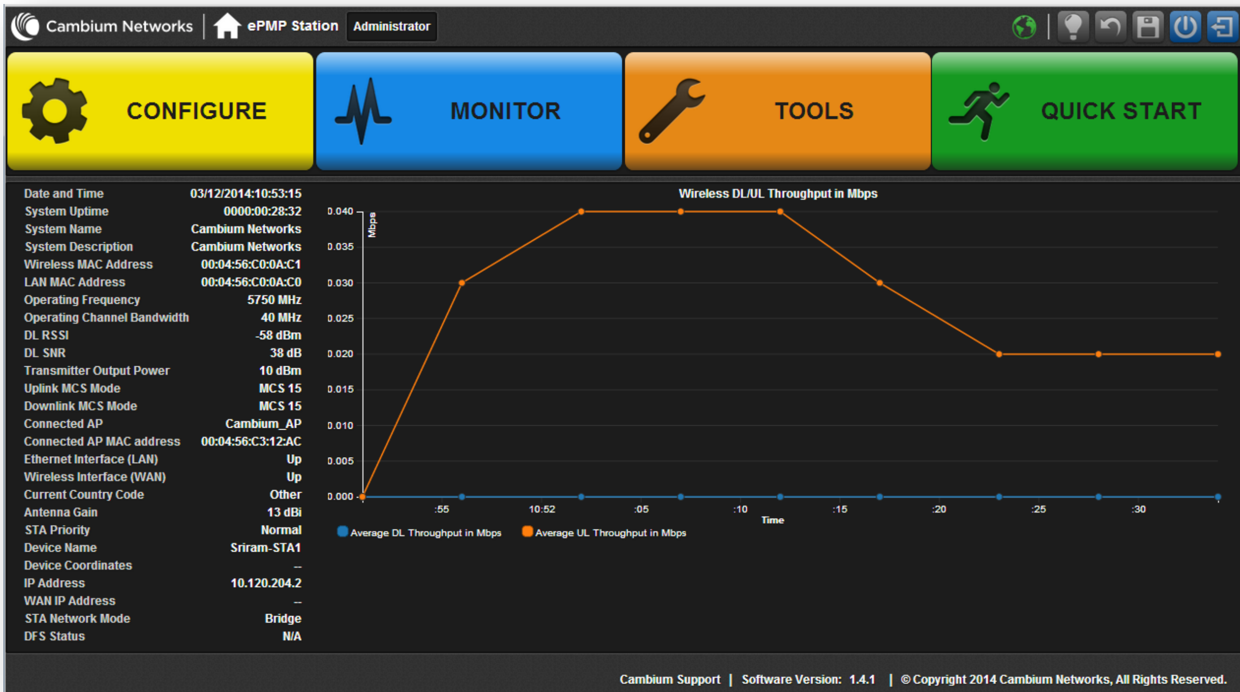


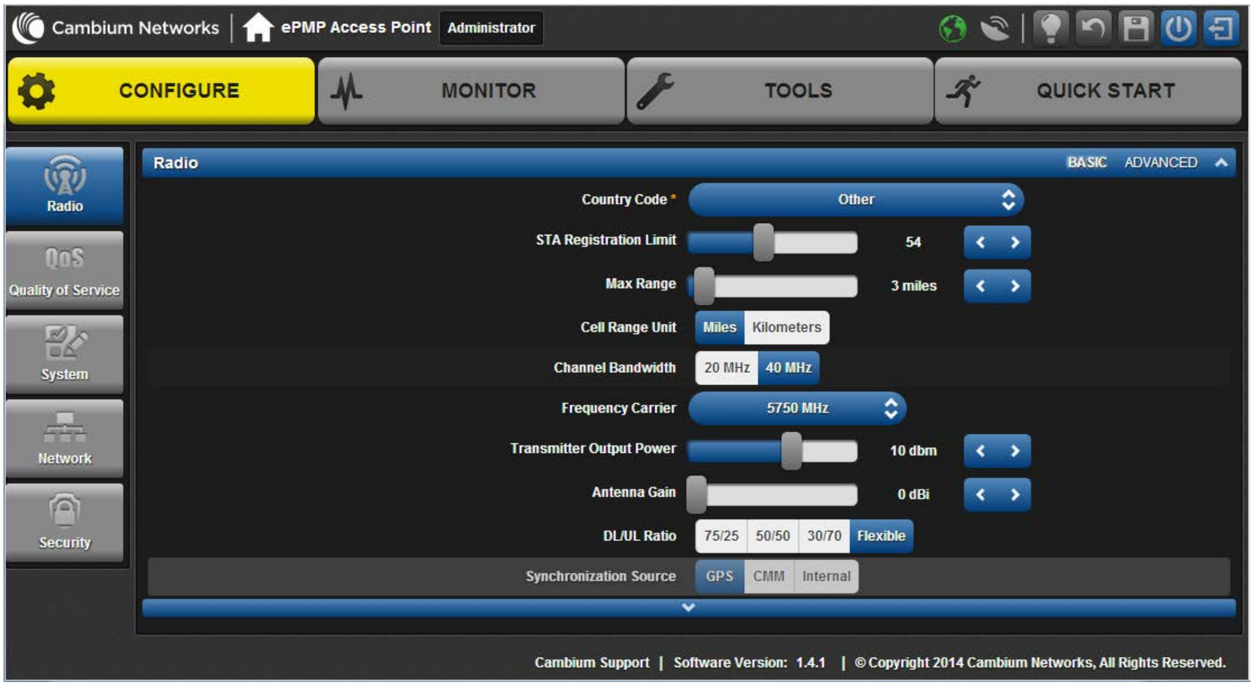
Table 44 STA dashboard attributes

Attribute	Meaning
Date and Time	The current date and time on the device, subject to the configuration of 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 Name	The current configured system name.
System Description	The current configured system description
Wireless MAC Address	The MAC address of the device Wireless interface.
LAN MAC Address	The MAC address of the device LAN (Ethernet) interface.
Operating Frequency	The current operating frequency.
Operating Channel Bandwidth	The current operating width of the channel used for the radio link.
DL RSSI	The Received Signal Strength Indicator, which is a measurement of the power level being received by the STA's antenna.

Attribute	Meaning
DL SNR	The Signal to Noise Ratio, which is an expression of the carrier signal quality with respect to signal noise and co-channel interference (or both).
Transmitter Output Power	The current power level at which the STA is transmitting (which is adjusted dynamically by the AP based on radio conditions).
Uplink MCS Mode	Modulation and Coding Scheme – indicates the modulation mode used for the radio uplink, based on radio conditions (MCS 1-7, 9-15).
Downlink MCS Mode	Modulation and Coding Scheme – indicates the modulation mode used for the radio downlink, based on radio conditions (MCS 1-7, 9-15).
Connected AP	The AP Name or SSID of the AP to which the STA is registered
Connected AP MAC Address	The Wireless MAC Address of the AP to which the STA is registered.
Ethernet Interface (LAN)	**Up**: The Ethernet (LAN) interface is functioning properly. **Down**: The Ethernet (LAN) interface has encountered an error and is not servicing traffic.
Wireless Interface (WAN)	**Up**: The radio (WAN) interface is functioning properly. **Down**: The radio (WAN) interface has encountered an error and is not servicing traffic.
Current Country Code	The current configured country code, which has an effect on DFS operation and transmit power restrictions. Registered Stations will inherit this country code when registration is complete (unless STA is locked to US region).
Antenna Gain	The configured gain of the external antenna.
STA Priority	The configured priority of the STA in the sector.
Device Name	The configured device name of the STA, used for identifying the device in an NMS such as the Cambium Network Services Server (CNSS).
Device Coordinates	The current configured Latitude and Longitude coordinates in decimal format.
IP Address	The current configured device IP address (LAN, Ethernet interface) used for management access.
WAN IP Address	The current configured device IP address (Wireless interface).
STA Network Mode	**Bridge:** The STA will act as a switch, and packets are forwarded or filtered based on their MAC destination address. **NAT:** The STA will act 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.
DFS Status	Current DFS operational status.

The GUI interface consists of two levels of navigation – the first-level navigation buttons on the top (**Configure**, **Monitor**, **Tools**, and **Quick Start**) as well as the context-based second-level navigations on the left-hand side of the interface. After a second-level navigation section has been chosen, the resulting configuration parameters are displayed in the main GUI pane. Each subsection of parameters may be configured to display a clean view of only basic parameters, or the display may also be configured to display a comprehensive listing of advanced parameters.

Figure 14 GUI first-level and second-level navigation



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 and STA and resetting both devices, the STA will be ready to associate (register) to the AP.

Figure 15 AP Quick Start menu

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

Procedure:

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

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

4 Configure parameter **Country Code**:

Country Code settings affect the radios in the following ways:

- Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain)
- DFS operation is enabled based on the configured country code, if applicable
- Frequency selection limiting (based on valid frequencies for the configured **Country Code**)

Select the country in which your network will be operating.

5 Configure 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 prior to configuring this parameter.

6 Configure parameter **AP Name (SSID)**:

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

7 Configure parameter **DL/UL Ratio**:

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

Caution

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

8 Configure 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 **CMM** 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**, then this parameter will be greyed out.

9 Configure parameter **Device IP address Mode**:

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**.

10 Configure parameter **Device 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).

11 Configure parameter **Device IP 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).

12 Configure parameter **Device Gateway IP Address***:*

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. To configure a simple test network, this parameter may be left at default (blank).

13 Configure parameter **Authentication Type**

Open: All STAs requesting network entry are allowed registration.

WPA2: The WPA2 mechanism provides AES radio link encryption and STA network entry authentication. When enabled, the STA must register using the **Authentication Pre-shared Key** configured on the AP and STA.

14 Configure parameter **Authentication Pre-shared Key**

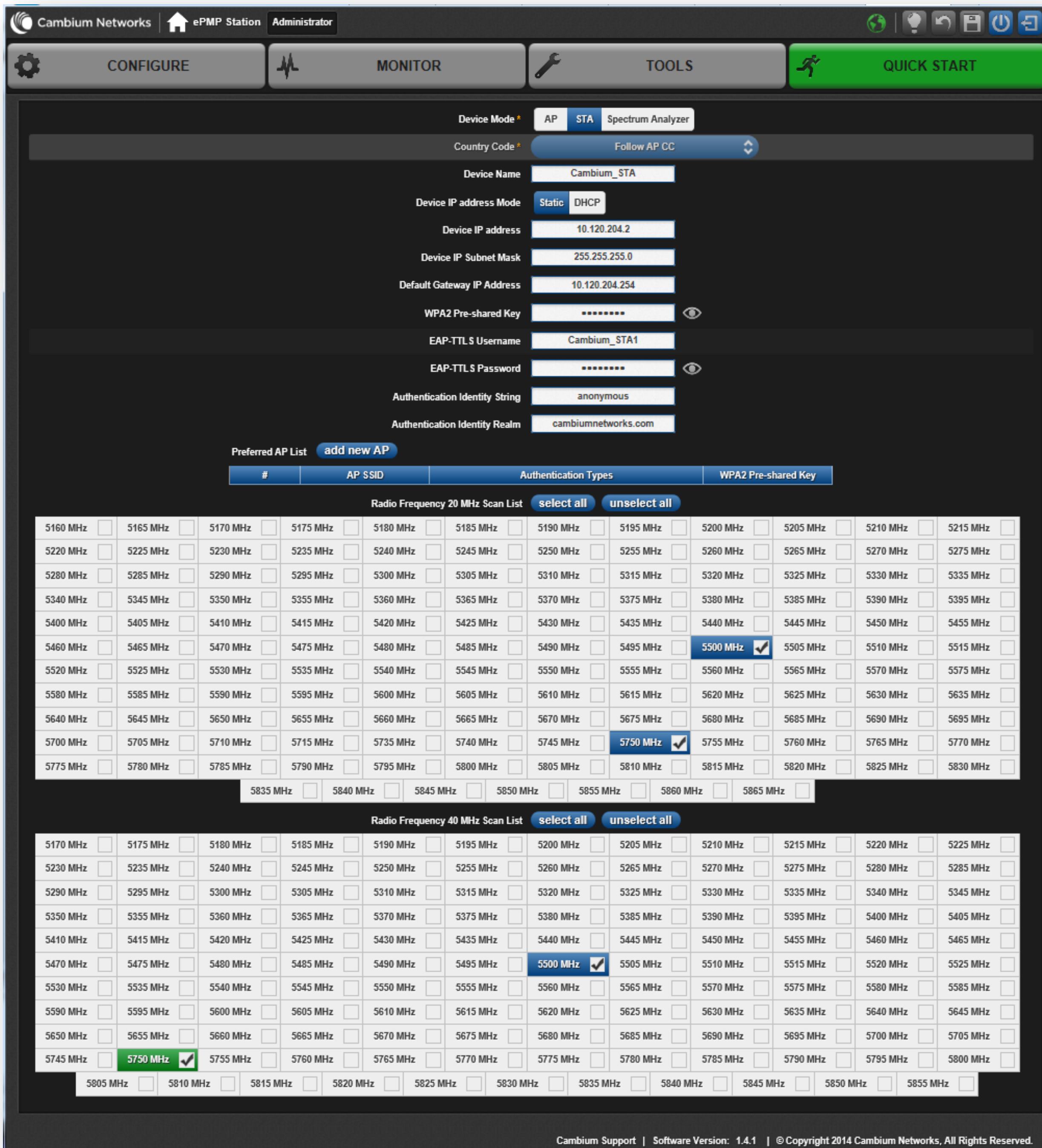
Configure this key on the AP, then configure each of the network STAs with this key to complete the authentication configuration. This key must be between 8 to 128 symbols. Click the visibility icon to toggle the display of the key's contents.

15 Click the **Save** icon, then click the **Reset** icon

Configuring STA 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 16 STA Quick Start menu



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

Procedure:

1 Start the web browser from the management PC.

2 Navigate to menu **Quick Start**

3 Configure parameter **Device Mode*:***

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

4 The **Country Code** is automatically retrieved from the AP, and does not require configuration.

Country Code settings affect the radios in the following ways:

- Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain)
- DFS operation is enabled based on the configured country code, if applicable
- Frequency range of operation depending on local limitations

5 Configure parameter **Device Name*:***

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

6 Configure parameter **Device IP Address Mode*:***

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.**

7 Configure parameter **Device 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.

8 Configure parameter **Device IP 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).

9 Configure parameter **Device Gateway IP Address*:***

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. To configure a simple test network, this parameter may be left at default (blank).

10 Configure parameter **WPA2 Pre-shared Key:**

Configure each of the network STAs 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.

11 Configure parameter **EAP-TTLS Username:**

Configure each of the network STAs with this EAP-TTLS Username (matching the credentials on the Radius server being used for the network).

12 Configure parameter **EAP-TTLS Password:**

Configure each of the network STAs 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.

13 Configure parameter **Authentication Identity String:**

Configure each of the network STAs with this Identity string (matching the credentials on the Radius server being used for the network). Default value for this parameter is "anonymous".

14 Configure parameter **Authentication Identity Realm:**

Configure each of the network STAs with this Identity realm (matching the credentials on the Radius server being used for the network). Default value for this parameter is "cambiumnetworks.com".

15 Configure the **Preferred AP List**

The **Preferred AP List** is comprised of a list of up to 16 APs to which the STA 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 STA will scan and register to the first AP found (with matching radio and/or authentication settings).

16 Configure parameter **Radio Frequency 20 MHz and 40MHz Scan List**:

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

17 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. Table 45 lists the functional areas that may be accessed from each menu option. Some of the parameters are only displayed for specific system configurations.

Table 45 Functional areas accessed from each menu option

Menu option	Menu Details
Configure	AP Configure menu on page 90
Radio	AP Radio page on page 91
Quality of Service	AP Quality of Service page on page 100
System	AP System page on page 104
Network	AP Network page on page 108
Security	AP Security page on page 111
Monitor	AP Monitor menu on page 116
Performance	AP Performance page on page 117
System Status	AP System Status page on page 120
Wireless Status	AP Wireless Status page on page 122
GPS Status	AP GPS Status page on page 124
Network Status	AP Network Status page on page 126
System Log	AP System Log page on page 128
Tools	AP Tools menu on page 129
Software Upgrade	AP Software Upgrade page on page 130
Factory Default	AP Factory Default page on page 132
Spectrum Analyzer	AP Spectrum Analyzer page on page 133
Throughput Test	AP Throughput Test page on page 136
Ping	AP Ping page on page 137
Traceroute	AP Traceroute page on page 138
Quick Start	Configuring connectorized radios using the Quick Start menu on page 83

AP CONFIGURE MENU

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

- AP Radio page on page 91
- AP Quality of Service page on page 100
- AP System page on page 104
- AP Network page on page 108
- AP Security page on page 111

AP 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.

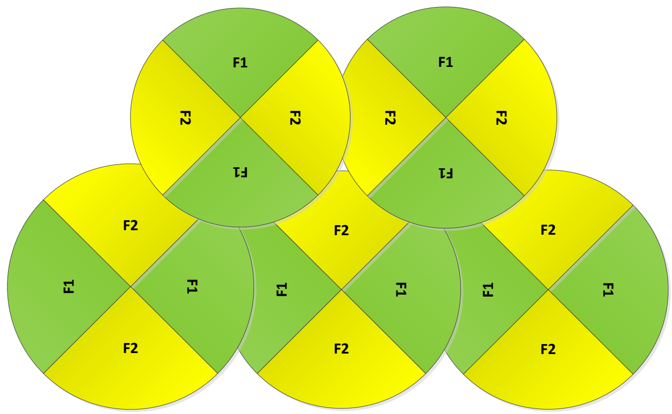
Figure 17 AP Radio page

Table 46 AP Radio Configuration attributes

Attribute	Meaning
Country Code	From the drop-down list, select the country in which the radio is operating. Country Code settings affect the radios in the following ways: • Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain) • DFS operation is enabled based on the configured country code, if applicable • Frequency selection limiting, based on regional limitations
STA Registration Limit	Based on sector/network planning and STA service level implementations, set the **STA Registration Limit** to the maximum allowed number of STAs that are allowed network entry. Default 60.
Max Range	Enter a number of miles or kilometers for the furthest distance from which an STA is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance • does not increase the power of transmission from the AP. • can reduce aggregate throughput. Regardless of this distance, the STA must meet the minimum requirements for an acceptable link. The AP will reject any STA network entry attempts from outside the configured maximum range. Default 3 miles. Caution If the AP is in cluster or is in range of another AP, then you *must* set this parameter on all other APs in the cluster and in range exactly the same. Otherwise, overlapping RF transmissions will introduce system interference.
Cell Range Unit	**Miles**: The **Max Range** setting and resulting frame calculations are configured in units of miles **Kilometers**: The **Kilometers** setting and resulting frame calculations are configured in units of kilometers
Channel Bandwidth	Configure the channel size used by the radio for RF transmission. This value must match between the AP and STAs.
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 Mode	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. Figure 18 depicts a network in which two frequencies "F`1" and "F2" are reused throughout the deployment.

Figure 18 Frequency reuse deployment



The set of APs to configure the **Frequency Reuse Mode** option on is dependent on the GPS synchronization sources in the whole network, CMM3, CMM4 or "onboard GPS" (GUI options are: **GPS** or **CMM**).

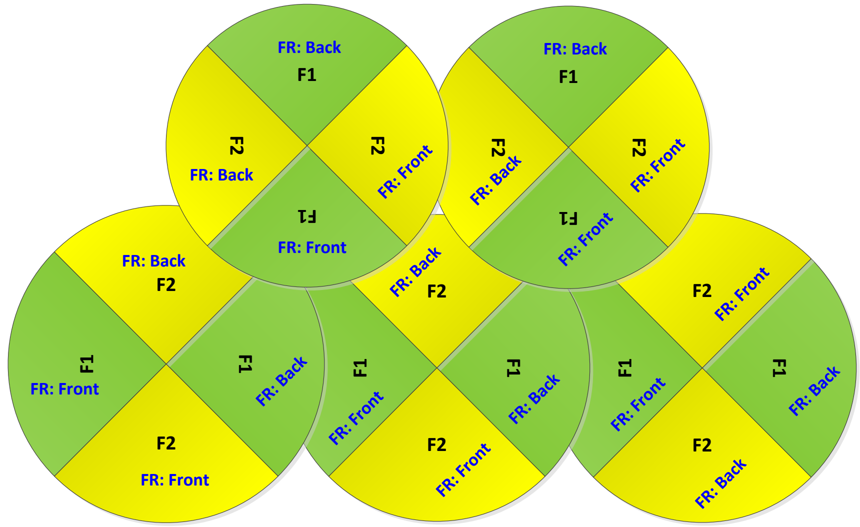
The GPS sync source is the same on all APs or is a combination of "onboard GPS" and CMM4

In this configuration the GPS synchronization source in the whole network is one of the following:

1- "onboard GPS" or
2- CMM4 or
3- CMM3 or
4- Mix of "onboard GPS" and CMM4 (but NOT CMM3)

Figure 19 demonstrates how to configure **Frequency Reuse Mode** to ensure that interference is reduced throughout the deployment:

Figure 19 Frequency reuse configuration example



The rules in selecting the APs to enabling the **Frequency Reuse Mode** in this deployment are:

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 shall be configured with **Frequency Reuse Mode** set to **Frequency-Reuse-Front.**

2- Only ONE of the APs on different towers facing each other with overlapped coverage must be configured with **Frequency Reuse Mode** set to **Frequency-Reuse-Back.**

The GPS sync source is a mixture of all types (CMM3, CMM4 & "onboard GPS")

In this configuration the GPS sync source in the whole network is one of the following:

1- (CMM3 and "onboard GPS") or

2- (CMM3 and CMM4) or

3- (CMM3 and CMM4 and "onboard GPS")

Figure 20 and Figure 21 show examples of which APs to enable the **Frequency Reuse Mode** feature in this mixture of sync sources.

Figure 20 Example 1 - Frequency reuse configuration, mixture of GPS synchronization sources

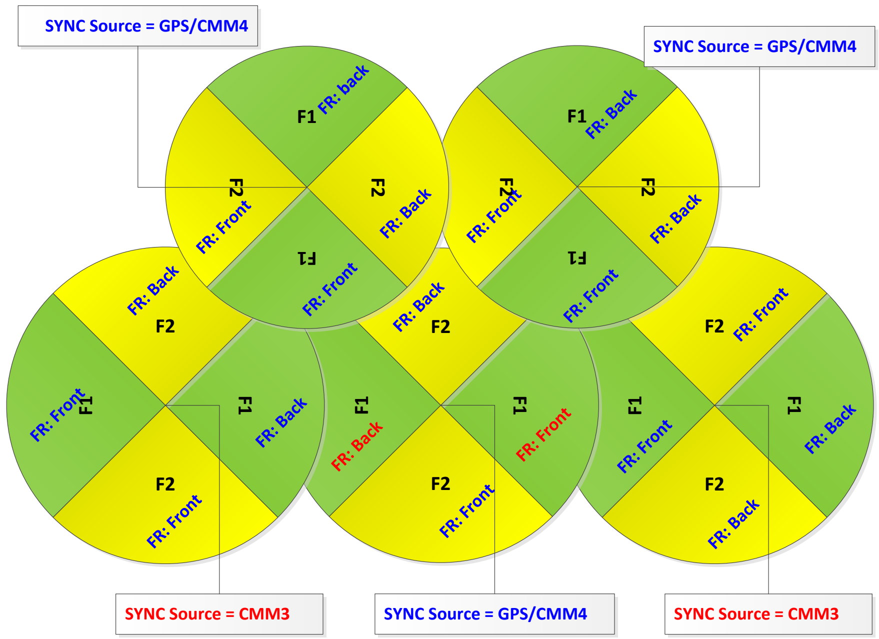
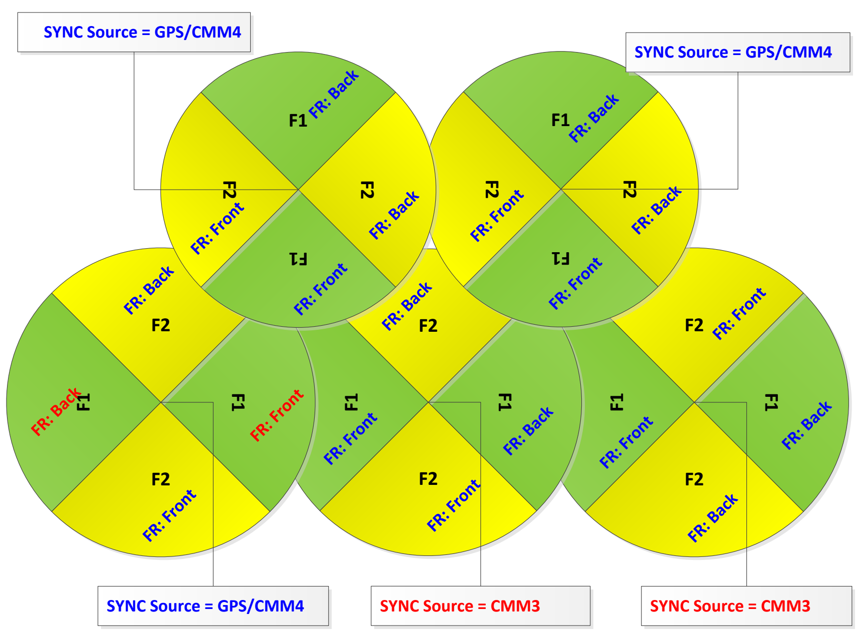


Figure 21 Example 2 - Frequency Reuse Configuration with Mixture of GPS sources



	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 deployments are: 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 shall have the **Frequency-Reuse-Front** ON. 2- For the APs on different towers facing each other with overlapped coverage: 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: i. 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. ii. 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.**
DFS 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**.
DFS 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 **STA Scan List**.
DFS Alternate Frequency Carrier 2	Configure the second channel bandwidth configuration that will be used for RF transmission if a DFS detection causes the radio to switch from

Channel Bandwidth	using the channel bandwidth configured in **Channel Bandwidth**.
DFS Alternate Frequency Carrier 2	Configure the second frequency that will be used for RF transmission if a DFS detection causes the radio to switch from using the frequencies configured in **Frequency Carrier** and **DFS Alternate Frequency Carrier 2** . It is important to set this frequency also in the **STA Scan List**.
PTP Access	**Off**: The system is configured to operate in PMP mode (i.e. more than one STA may connect to the AP) **Connect 1st STA**: The system is configured to accept only the 1st registered STA. Network entry will be denied for all subsequent STA network entry requests. **MAC Limited**: The system is configured to accept only one STA registration, and this registration is limited by STA MAC Address (the STA Wireless MAC Address).
PTP MAC Address	Configure the Wireless MAC Address of the sole STA which will be granted registration to the AP. All other network entry attempts will be rejected by the AP. The STA's **Preferred AP List** may be configured with the destination point-to-point AP to ensure that the STA connects with the intended AP.
Transmitter Output Power	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 Code.** Nations and regions may regulate transmitter output power. For example • 2.4 GHz and 5 GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. The professional installer of the equipment has the responsibility to • 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 • 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.
AP Management Packet Rate	**MCS0**: The system is configured to use MCS0 rate for all management messages. This allows for improved link stability and range in high interference environment.

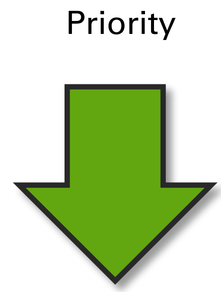
	MCS1: The system is configured to use MCS1 rate for all management messages. This allows for slightly higher sector throughput. This is the default setting.
DL/UL Ratio	Configure the schedule of downlink traffic to uplink traffic on the radio link. The first three options, **75/25**, **50/50** and **30/70**, 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 will be used for downlink and uplink resources, every frame. Caution Setting this parameter to **Flexible** causes the radio to operate in unsychronized mode. For all other settings, if the AP is in cluster or is in range of another AP, then you *must* set this parameter on all other APs in the cluster and in range exactly the same. Otherwise, overlapping RF transmissions will introduce system interference.
Beacon Interval	**500 msec**: Radio beacons will be sent by the AP every 500 milliseconds. Effectively, this configuration allows quicker STA network entry since more beacons are available when the STA is scanning. In large network deployments, a 500 millisecond beacon interval configuration will allow STAs to enter the network more quickly. **1000 msec**: (Default) Radio beacons will be sent by the AP every 1000 milliseconds. In small network deployments, this setting may be applicable as beacons are scheduled half as often as a 500 millisecond configuration. This reduction in beacon scheduling results in a minor increase in user data traffic rates (by ~1 packet per second).
STA Target Received Power Level	Each STA's transmitter output power is automatically set by the AP. The AP monitors the received power from each STA, and adjusts each STA's transmitter output power so that the received power at the AP from the STA is not greater what is configured in **STA Target Received Power Level**. These automatic power adjustments ensure that the STA is not transmitting excessive energy (raising system noise level) and that the STA is able to achieve an optimal modulation state (and maximum achievable throughput). Target receive levels must be set to lesser than -60 dBm nominally in order to prevent interference from co-located co-channel sectors.
High Interference Channel Estimation	When this feature is enabled, the receiver uses alternate channel estimation method to improve receiver sensitivity especially at lower MCSs in high interference environment.
Synchronization	**GPS**: Synchronization timing is received via the AP's connected GPS

Source	antenna. Co-located or in-range APs receiving synchronization via GPS or CMM will transmit and receive at the same time, thereby reducing self-interference. **CMM**: 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, see the *PMP Synchronization Solutions User Guide*. Caution 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). **Internal**: Synchronization timing is generated by the AP, and timing is not based on GPS pulses. Caution APs using **Synchronization Source** of **Internal** will not transmit and receive in sync with other co-located or in-range APs, which introduces interference into the system.
Synchronization Holdoff Time (sec)	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 STA 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 30 seconds.

AP Quality of Service page

The ePMP platform supports three QoS priority levels using air fairness, priority-based starvation avoidance scheduling algorithm:

Priority Level	**ePMP Traffic Priority Label**
Highest Priority (Served first)	VOIP (only utilized when **VOIP Enable** is set to **Enabled**)
Medium Priority (Served once highest priority traffic is sent)	High
Lowest Priority (Serviced once Highest and Medium priority traffic is sent)	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 STA field **MIR Profile Setting** is used to configure the appropriate MIR profile for limiting the STA's data rate.

Figure 22 AP Quality of Service page

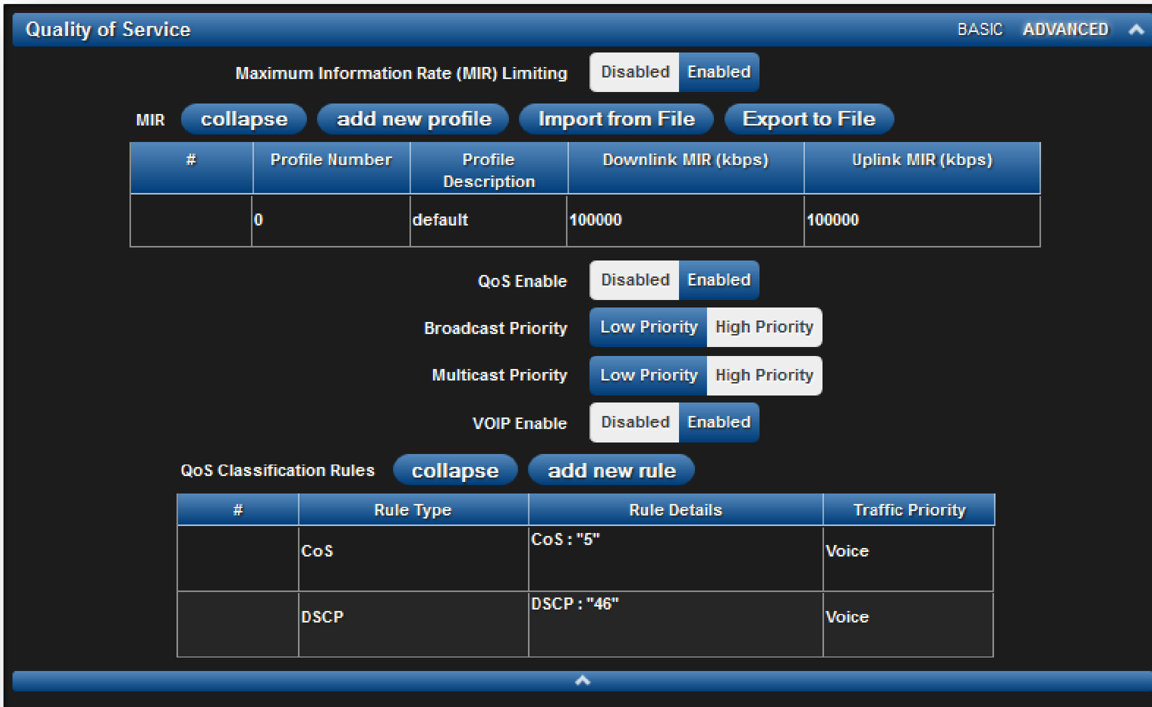


Table 47 AP Radio Configuration attributes

Attribute	Meaning
Maximum Information Rate (MIR) Limiting	**Disabled:** When disabled, RF transmission is only limited by the capacity of the link (and any active QoS classification rules). **Enabled:** When enabled, all downlink and uplink traffic is limited based on the profiles configured in the MIR table.
MIR	The MIR (Maximum Information Rate) table is comprised of up to sixteen profiles which, after configured, may be set on the STA to employ a certain service level or data rate.
Profile Number	Assign a profile number to each row in the AP MIR table. This profile number is then set on each STA to limit data transfer rates based on the operator’s configuration of the MIR table and its profiles.
Profile 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.

Attribute	Meaning
Uplink MIR (kbps)	Specify the uplink rate at which the AP is allowed to transmit for this configured profile.
QoS Enable	**Enabled**: The QoS Classification Rules table is editable and is utilized by the device to classify traffic. **Disabled**: The QoS Classification Rules table is greyed-out and all traffic is sent at one priority level.
Broadcast Priority	**Low Priority**: All Broadcast traffic sent over the downlink is prioritized as low priority, and will be delivered to the STA after scheduled high priority and VoIP traffic. **High Priority**: All Broadcast traffic sent over the downlink is prioritized as high priority, and will be scheduled for delivery to STAs before low priority traffic but after VoIP traffic.
Multicast Priority	**Low Priority**: All Multicast traffic sent over the downlink is prioritized as low priority, and will be delivered to the STA after scheduled high priority and VoIP traffic. **High Priority**: All Multicast traffic sent over the downlink is prioritized as high priority, and will be scheduled for delivery to STAs before low priority traffic but after VoIP traffic.
VOIP Enable	**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 highest priority. The **CoS** and **DSCP** values may be modified to accommodate non-standard VoIP equipment. **Disabled**: When disabled, VoIP traffic is scheduled normally along with all other user data.
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**.

Attribute	Meaning
Rule Type	**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 ingressing the AP's Ethernet port. **VLAN ID:** traffic prioritization is based on the VLAN ID of the packet ingressing the AP's Ethernet port. **EtherType:** traffic prioritization is based on the two octet Ethertype field in the Ethernet frame ingressing the AP's Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame. **IP:** traffic prioritization is based on the source and (or) destination IP address of the packet ingressing the AP's Ethernet port. A subnet mask may be included to define a range of IP addresses to match. **MAC:** traffic prioritization is based on the source and (or) destination MAC address of the packet ingressing 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.
Rule Details	The **Rule Details** column is used to configure each classification rule specified in column **Rule Type**.
Traffic Priority	**High**: Traffic ingressing the AP'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). **Low:** Traffic ingressing the AP'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). Voice: VoIP Traffic ingressing the AP's Ethernet port is given highest priority for sending over the radio link.

AP System page

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

Figure 23 AP System page

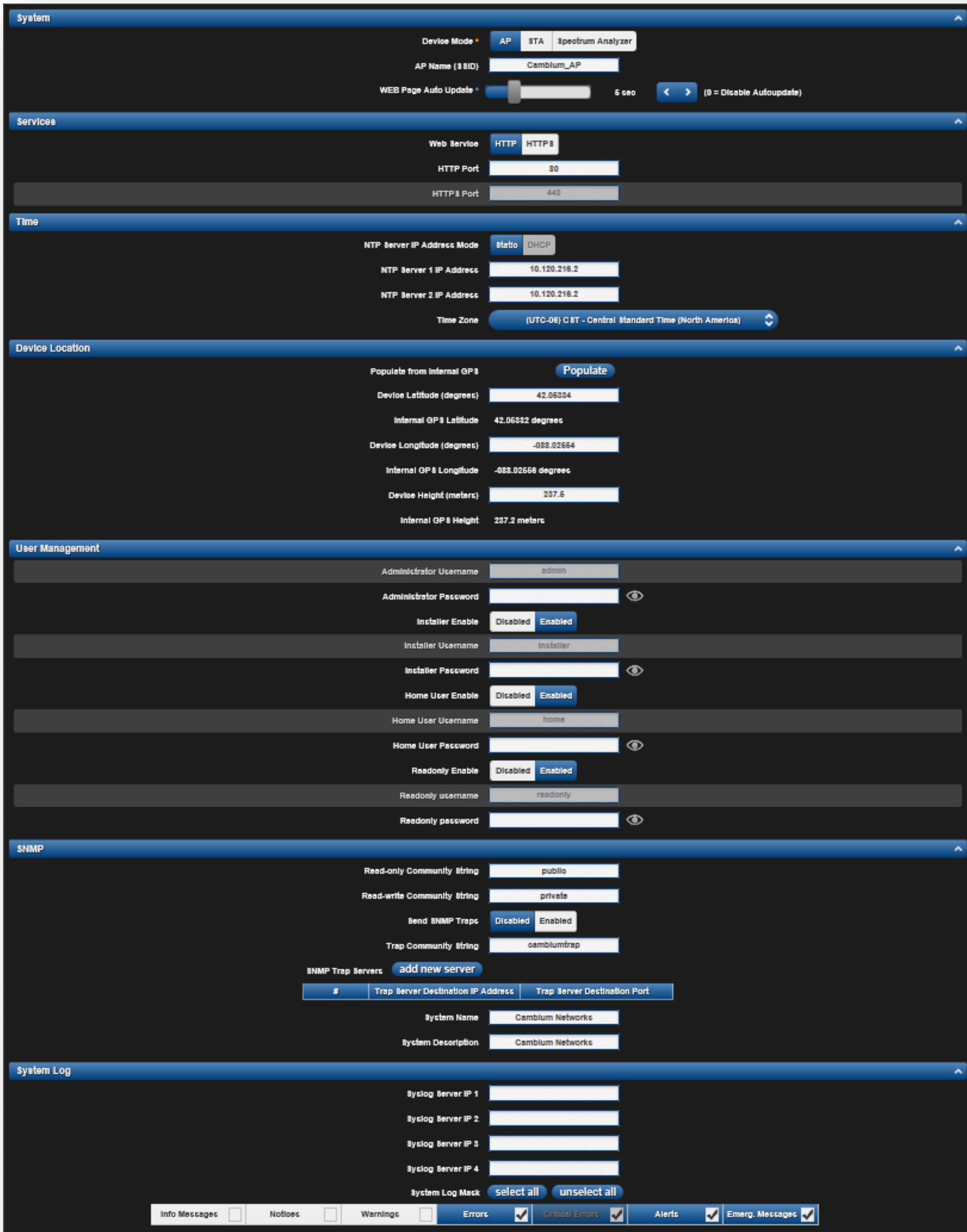


Table 48 AP System attributes

Attribute	Meaning
Device Mode	All ePMP devices (integrated or connectorized) may be configured to operate in one of three modes: **AP:** The device will operate as an AP. **STA**: The device will operate as an STA. **Spectrum Analyzer**: The devices will operate in Spectrum Analyzer mode, allowing the operator to download the spectrum analyzer tool.
AP Name (SSID)	The AP Name (SSID) is used to identify the AP to STAs. This value is configured in the STA to select an AP with which to register. Ensure that this parameter is configured uniquely for each AP in the network.
WEB Page 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).
Web Service	**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.
NTP Server IP Address Mode	**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.
NTP Server 1,2 IP Address	Configure primary and secondary NTP server IP addresses from which the device will retrieve 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.
Populate from Internal GPS	On a GPS Synchronized ePMP radio, the Device coordinates can be populated using the information retrieved from the on-board GPS chip.
Device Latitude (degrees)	Configure Latitude information for the device in decimal format.
Internal GPS Latitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Latitude information from the on-board GPS chip.
Device Longitude (degrees)	Configure Longitude information for the device in decimal format.

Attribute	Meaning
Internal GPS Longitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Longitude information from the on-board GPS chip.
Device Height (meters)	Configure height above sea level for the device in meters.
Internal GPS Height	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device height above sea level from the on-board GPS chip.
Administrator, Installer, Home User, Readonly Username	Read-only listing of available login levels. • 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, only has permissions to view the Monitor page.
Installer, Home User, Readonly Enable	**Disabled**: The disabled user will not be 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.
Administrator, Installer, Home User, Readonly Password	Configure a custom password configuration for each user to secure the device. The password character display may be toggled using the visibility icon .
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 **SNMP 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.
Send SNMP Traps	**Disabled**: SNMP traps for system events will not be sent from the device. **Enabled**: SNMP traps for system events will be sent to the servers configured in table **SNMP Trap Servers**.
Trap Community String	Configure an SNMP Trap Community String which is processed by the servers configured in **SNMP 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).

Attribute	Meaning
SNMP Trap Servers	The **SNMP Trap Servers** table is used to configure trap destinations for SNMP traps generated by the device.
Trap Server Destination IP Address	Configure the IP address of each SNMP trap server target.
Trap Server Destination Port	Configure the port to which SNMP traps are sent from the ePMP device.
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.
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.
Syslog Server IP 1-4	Specify up to four syslog servers to which the device will send syslog messages.
System Log Mask	Configure the levels of syslog messages which the devices send to the servers configured in parameters **Syslog Server IP 1-4.** Caution Choose only the syslog levels appropriate for your deployment. Excessive logging can cause the device log file to fill and begin overwriting previous entries.

AP Network page

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

Figure 24 AP Network page

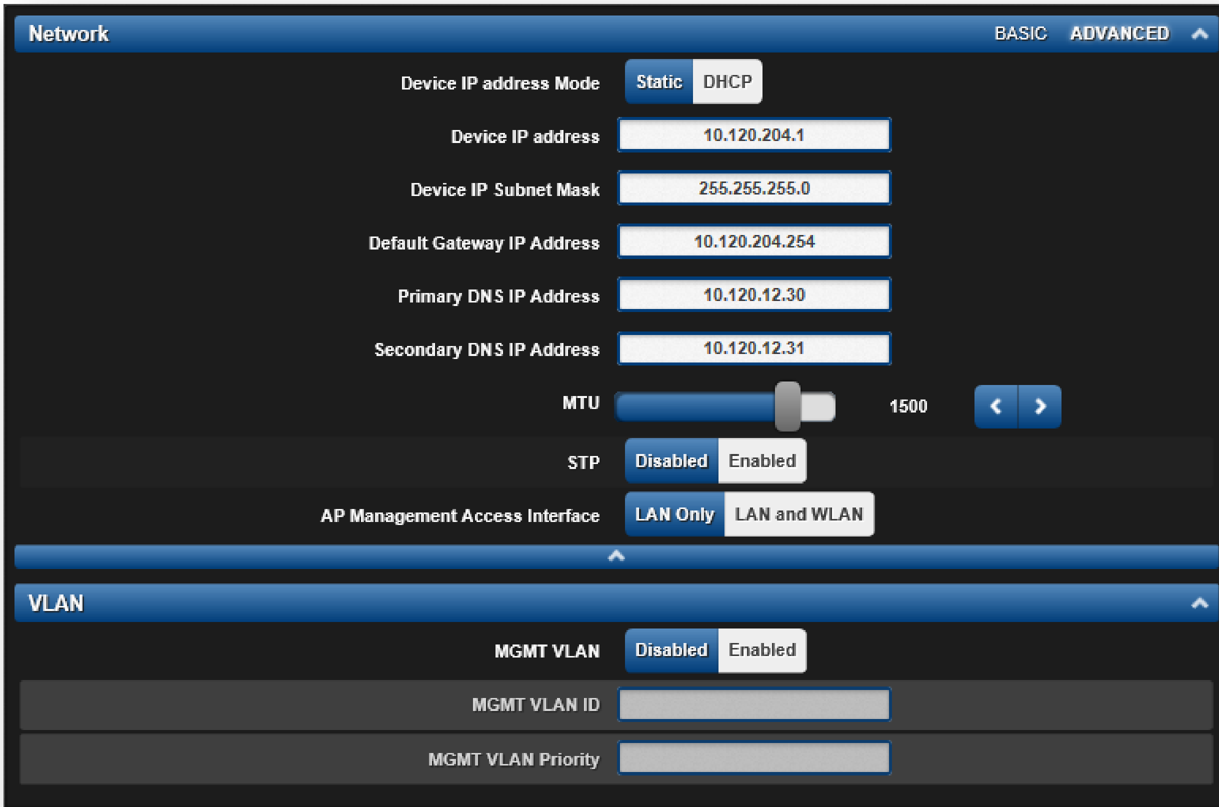


Table 49 AP Network attributes

Attribute	Meaning
Device IP address Mode	**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.

Device IP address	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. 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 (STA 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 10.1.1.254.
Device IP 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.
Device Gateway IP Address	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.
Primary DNS Server IP Address	Configure the primary IP address of the server used for DNS resolution.
Secondary DNS Server IP Address	Configure the secondary IP address of the server used for DNS resolution.
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. Packets received by the device larger than the configured MTU will be dropped.
STP	**Disabled**: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the AP. **Enabled**: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the AP, allowing for the prevention of Ethernet bridge loops.

AP Management Access Interface	**LAN Only:** 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 STA). **LAN and WLAN:** 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 STA). Caution **APs configured with AP Management Access Interface set to LAN and WLAN are susceptible to unauthorized access.**
MGMT VLAN	**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. 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. **Disabled**: When disabled, all IP management traffic is allowed to the device.
MGMT 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.
MGMT VLAN Priority	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 device management traffic. If the **MGMT VLAN Priority** field is configured, to access the AP GUI the accessing switch or end device must be configured to tag Ethernet frames with the **MGMT VLAN ID** value *and* the same priority values as configured in field **MGMT VLAN Priority**. For example, if **MGMT VLAN ID** is set to 100 and **MGMT VLAN Priority** is set to 5, the Ethernet frames sent to the AP to access the GUI must be tagged with a VLAN ID value of 100 and Class of Service priority set to 5. If **MGMT VLAN Priority** is not configured (blank), to access the AP GUI the accessing switch or end device only needs to tag Ethernet frames with the same VLAN ID as is configured in the **MGMT VLAN ID** field.

AP Security page

The AP's Security page is used to configure system security features including STA 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 only **Action** set to **Deny** and **Interface** set to **LAN** or **WAN.** To regain access to the device, perform a factory default.

Figure 25 AP Security page

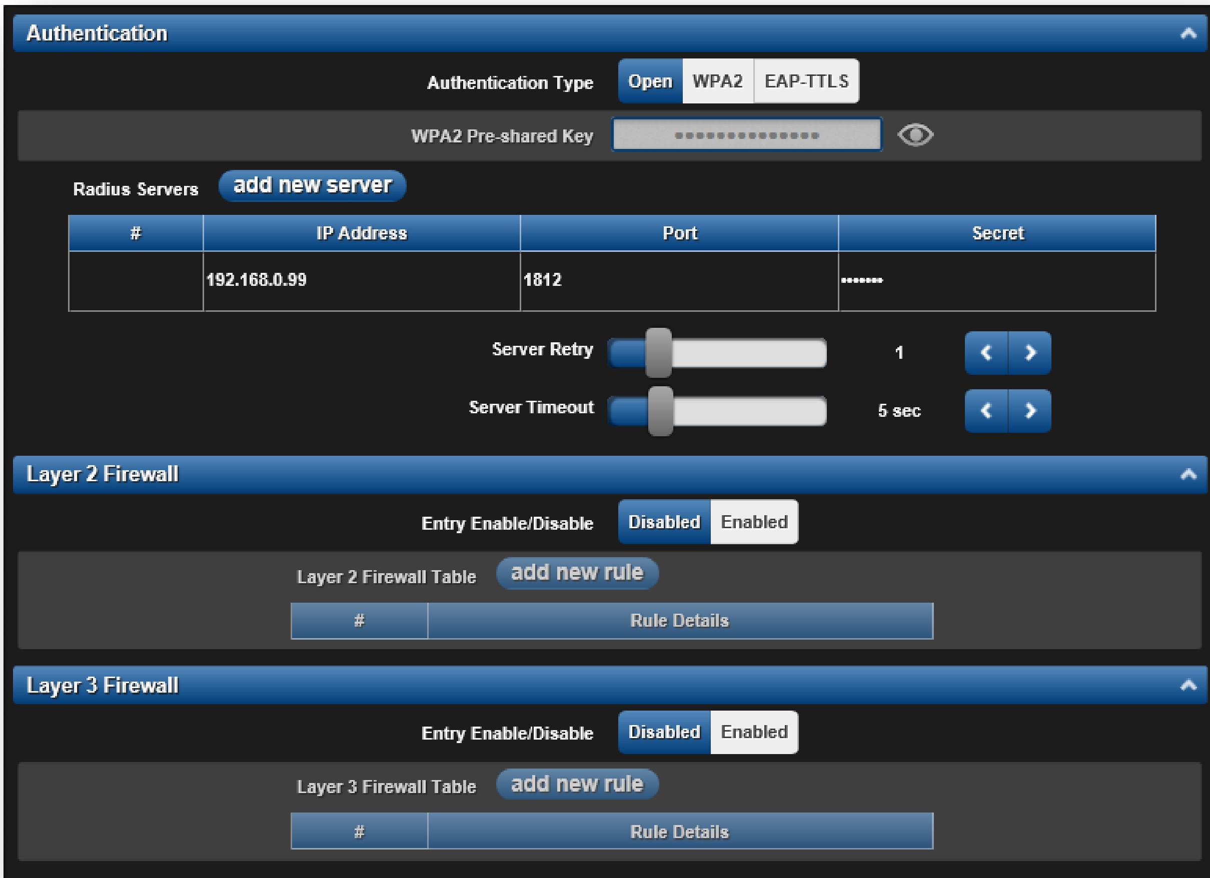


Table 50 AP Security attributes

Attribute	Meaning
Authentication Type	**Open**: All STAs requesting network entry are allowed registration. **WPA2:** The WPA2 mechanism provides AES radio link encryption and STA network entry authentication. When enabled, the STA must register using the **Authentication Pre-shared Key** configured on the AP and STA.
WPA2 Pre-shared Key	Configure this key on the AP, then configure each of the network STAs with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.
Radius Servers	Up to 3 Radius servers can be configured on the device with the following attributes: **IP Address**: IP Address of the Radius server on the network. **Port:** The Radius server port. Default is 1812. **Secret**: The secret key that will be used to communicate with the Radius server.
Server Retry	Number of times the radio will retry authentication with the configured Radius server before it fails authentication of the STA.
Server Timeout	Timeout between each retry with the configured Radius server before it fails authentication of the STA.
Layer 2 Firewall Entry Enable/Disable	**Enabled**: Modifications to the Layer 2 Firewall Table are allowed and rules are enforced. **Disabled**: Modifications to the Layer 2 Firewall Table are not allowed and rules are not enforced.
Layer 2 Firewall Table	When the STA is configured with **STA Network Mode** set to **Bridge**, the Layer 2 firewall table may be used to configure rules matching layer 2 (MAC layer) traffic which result in forwarding or dropping the traffic over the radio link or Ethernet interface.
Rule Details, Name	Assign a logical name to the firewall rule based on the intended rule operation (i.e. “Deny all WLAN traffic from VLAN ID 100”).
Rule Details, Action	**Accept**: Layer 2 traffic matching the rule details is forwarded. **Deny**: Layer 2 traffic matching the rule details is dropped at the device.

Rule Details, Interface	**WLAN**: When this option is selected, firewall rules will be applied to traffic incoming on the device radio interface (WLAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will either be forwarded to the LAN (Ethernet) interface or dropped at the device. **LAN**: When this option is selected, firewall rules will be applied to traffic incoming on the device Ethernet interface (LAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will be either forwarded to the WAN (radio) interface or dropped at the device.
Rule Details, Log	**On**: When a firewall rule is matched, a resulting system log message will be generated. **Off**: When a firewall rule is matched, no system log messaging will be generated.
Rule Details, EtherType	Rule matching is based on the two octet Ethertype field in the Ethernet frame. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame.
Rule Details, VLAN ID	Rule matching is based on the VLAN ID of the packet.
Rule Details, Src MAC	Firewall rule matching is based on the source MAC address of the packet.
Rule Details, Src Mask	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.
Rule Details, Dest MAC	Firewall rule matching is based on the destination MAC address of the packet.
Rule Details, Dest Mask	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.
Layer 3Firewall Entry Enable/Disable	**Enabled**: Modifications to the Layer 3 Firewall Table are allowed and rules are enforced. **Disabled**: Modifications to the Layer 3 Firewall Table are not allowed and rules are not enforced.

Layer 3 Firewall Table	When the STA is configured with **STA Network Mode** set to **NAT**, the Layer 3 firewall table may be used to configure rules matching layer 3 (IP layer) traffic which result in forwarding or dropping the traffic over the radio link or Ethernet interface.
Rule Details, Name	Assign a logical name to the firewall rule based on the intended rule operation (i.e. "Deny all WLAN traffic from Src IP 192.168.2.111").
Rule Details, Action	**Accept**: Layer 3 traffic matching the rule details will be forwarded **Deny**: Layer 3 traffic matching the rule details will be dropped at the device.
Rule Details, Interface	**WLAN**: When this option is selected, firewall rules will be applied to traffic incoming on the device radio interface (WLAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will either be forwarded to the LAN (Ethernet) interface or dropped at the device. **LAN**: When this option is selected, firewall rules will be applied to traffic incoming on the device Ethernet interface (LAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will be either forwarded to the WAN (radio) interface or dropped at the device.
Rule Details, Log	**On**: When a firewall rule is matched, a resulting system log message will be generated. **Off**: When a firewall rule is matched, no system log messaging will be generated.
Rule Details, Protocol	**TCP**: Only TCP packets are matched by the configured rule. **UDP**: Only UDP packets are matched by the configured rule. **TCP+UDP**: Both TCP and UDP packets are matched by the configured rule. **ICMP**: Only ICMP packets are matched by the configured rule. **IP**: Only IP packets are matched by the configured rule.
Rule Details, Port	Rule matching is based on the port value in the incoming packet.
Rule Details, Src IP	Rule matching is based on the Source IP address of the incoming packet.
Rule Details, Src Mask	A subnet mask may be included to define a range of IP addresses to match. For example, if **Src IP** is configured to 192.168.2.0 and **Src Mask** is configured to 255.255.255.0, the rule will match all IP addresses from subnetwork 192.168.2.X.
Rule Details, Dest IP	Rule matching is based on the Destination IP address of the incoming packet.

Rule Details, Dest Mask	A subnet mask may be included to define a range of IP addresses to match. For example, if **Dest IP** is configured to 192.168.2.0 and **Dest Mask** is configured to 255.255.255.0, the rule will match all IP addresses from subnetwork 192.168.2.X.
Rule Details, DSCP	Rule matching is based on the DiffServ CodePoint value of the incoming packet.
Rule Details, TOS	Rule matching is based on the Type Of Service value of the incoming packet.

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

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

Figure 26 AP Performance page

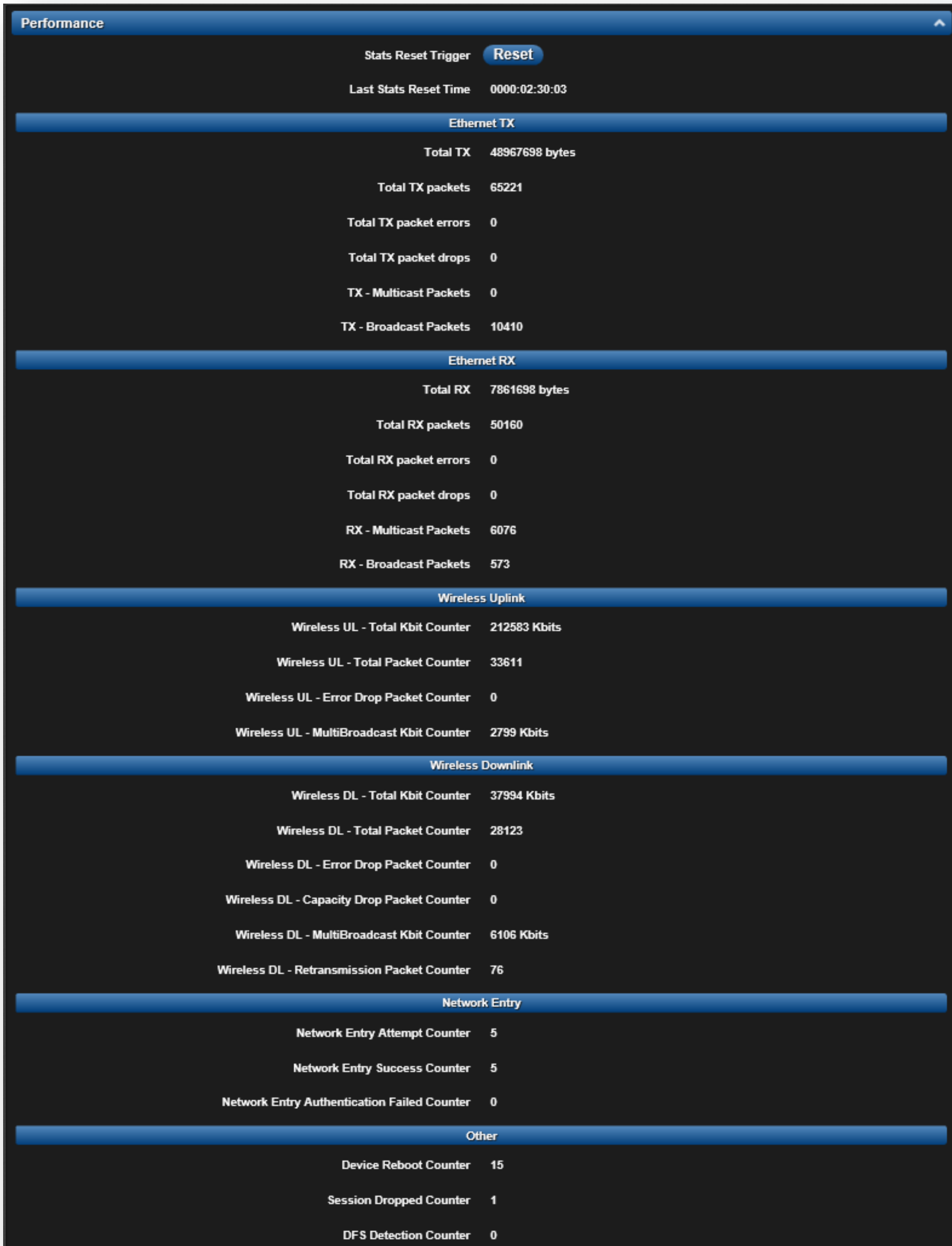


Figure 27 AP Performance page – contd.

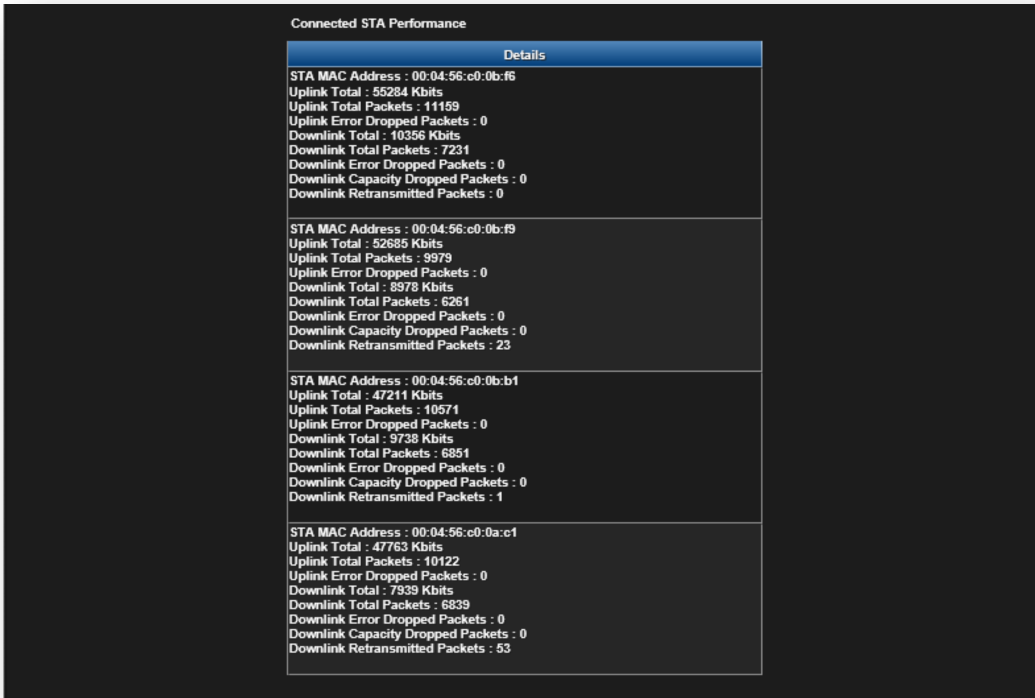


Table 51 AP Performance page attributes

Attribute	Meaning
Stats Reset Trigger	Reset all statistics
Ethernet TX, Total TX	Total count of bytes transferred from the AP's Ethernet interface
Ethernet TX, Total TX packets	Total count of packets transferred from the AP's Ethernet interface
Ethernet TX, Total TX packet errors	Total count of packets transmitted out of the AP's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Ethernet TX, Total TX packet drops	Total count of packets dropped prior to sending out of the AP's Ethernet interface due to Ethernet setup or filtering issues.
Ethernet TX, TX – Multicast Packets	Total count of multicast packets sent via the AP's Ethernet interface
Ethernet TX, TX – Broadcast Packets	Total count of broadcast packets sent via the AP's Ethernet interface
Ethernet RX, Total RX	Total count of bytes received by the AP's Ethernet interface
Ethernet RX, Total RX packets	Total count of packets received by the AP's Ethernet interface

Attribute	Meaning
Ethernet RX, Total RX packet errors	Total count of packets received by the AP's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Ethernet RX, Total RX packet drops	Total count of packets dropped prior to sending out of the AP's wireless interface due to Ethernet setup or filtering issues.
Ethernet RX, RX – Multicast Packets	Total count of multicast packets received via the AP's Ethernet interface.
Ethernet RX, RX – Broadcast Packets	Total count of broadcast packets received via the AP's Ethernet interface.
Wireless Uplink, Total Kbit Counter	Total count of packets received via the AP's wireless interface in Kbits.
Wireless Uplink, Total Packet Counter	Total count of packets received via the AP's wireless interface.
Wireless Uplink, Error Drop Packet Counter	Total count of packets dropped prior to sending out of the AP's Ethernet interface due to RF errors (packet integrity error and other RF related packet error).
Wireless Uplink, MultiBroadcast Kbit Counter	Total count of multicast and broadcast packets received on the AP's wireless interface in Kbits.
Wireless Downlink, Total Kbit Counter	Total count of packets transmitted out of the AP's wireless interface in Kbits.
Wireless Downlink, Total Packet Counter	Total count of packets transmitted out of the AP's wireless interface.
Wireless Downlink, Error Drop Packet Counter	Total count of packets dropped after transmitting out of the AP's Wireless interface due to RF errors (No acknowledgement and other RF related packet error).
Wireless Downlink, Capacity Drop Packet Counter	Total count 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).
Wireless Downlink, MultiBroadcast Kbit Counter	Total count of multicast and broadcast packets transmitted out of the AP's wireless interface in Kbits.
Wireless Downlink, Retransmission Packet Counter	Total count of packets retransmitted after transmitting out of the AP's Wireless interface due to RF errors (No acknowledgement and other RF related packet error).

AP System Status page

Use the System Status page to reference key system information.

Figure 28 AP System Status page

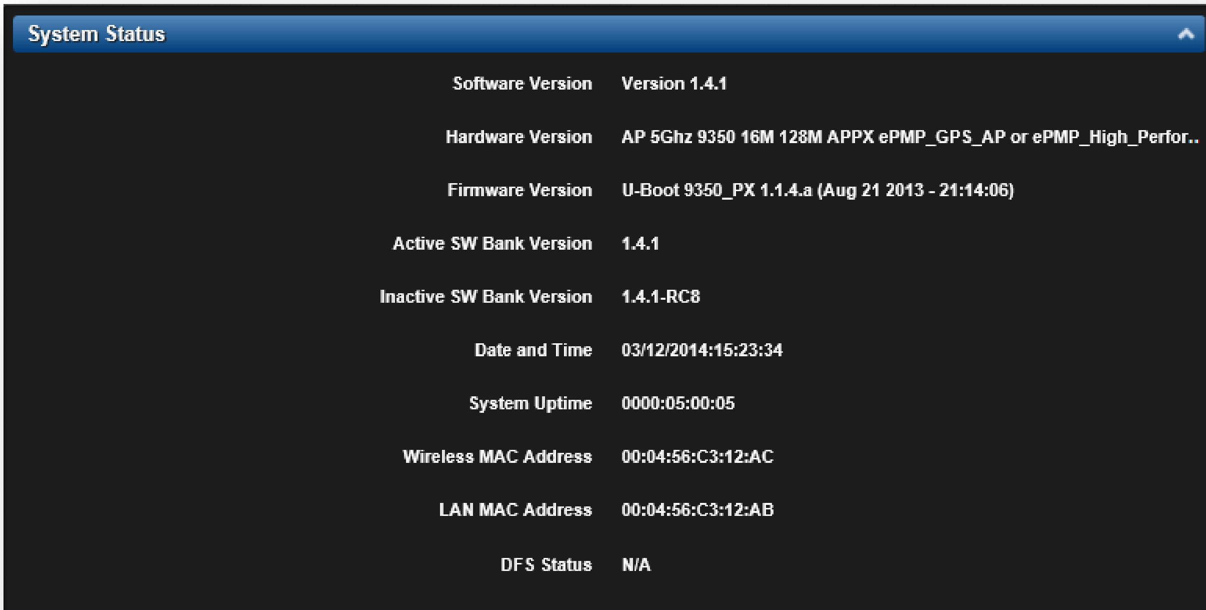


Table 52 AP System Status page attributes

Attribute	Meaning
Software Version	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).
Hardware Version	Board hardware version information.
Firmware Version	U-Boot version information.
Active SW Bank Version	The currently operating version of software on the ePMP device.
Inactive SW Bank Version	The backup software version on the ePMP device, used upon failure of the active bank. Two software upgrades in sequence will update both the **Active SW Bank Version** and the **Inactive SW Bank Version**.
Date and Time	Current date and time, subject to time zone offsets 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.

Attribute	Meaning
Wireless MAC Address	The hardware address of the device wireless interface.
LAN MAC Address	The hardware address of the device LAN (Ethernet) interface.
DFS Status	**N/A:** DFS operation is not required for the region configured in parameter **Country Code.** **Channel Availability Check**: Prior to 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.** **In-Service Monitoring**: Radio is transmitting and receiving normally while monitoring for radar pulses which require a channel move. **Radar Signal Detected**: The receiver has detected a valid radar pulse and is carrying out detect-and-avoid mechanisms (moving to an alternate channel). **In-Service Monitoring at Alternative Channel**: The radio has detected a radar pulse and has moved operation to a frequency configured in **DFS Alternative Frequency Carrier 1** or **DFS Alternative Frequency Carrier 2.** **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.

AP Wireless Status page

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

Figure 29 AP Wireless Status page

Table 53 AP Wireless Status page attributes

Attribute	Meaning
Operating Frequency	The current frequency at which the AP is operating.
Transmitter Output Power	The current power level at which the AP is transmitting.
Registered STA Count	The total count of STAs which are currently registered to the AP.
Ethernet Interface (LAN)	**Up**: The Ethernet (LAN) interface is functioning properly. **Down**: The Ethernet (LAN) interface has encountered an error and is not servicing traffic.

Attribute	Meaning
Wireless Interface (WAN)	**Up**: The radio (WAN) interface is functioning properly. **Down**: The radio (WAN) interface has encountered an error and is not servicing traffic.
Current Country Code	The current country code at which the AP is operating.
Connected STA List	Use the **Connected STA List** table to monitor registered STAs and their key RF status and statistics information.
STA MAC Address	The address of the STA wireless interface.
UL RSSI	The uplink Received Signal Strength Indicator, which is a measurement of the power level being received by the AP's antenna.
Estimated DL RSSI	The downlink Received Signal Strength Indicator, which is an estimated measurement of the power level being received by the STA's antenna.
UL SNR	The uplink Signal to Noise Ratio, which is an expression of the carrier signal quality with respect to signal noise.
DL SNR	The downlink Signal to Noise Ratio, which is an expression of the carrier signal quality with respect to signal noise.
UL MCS Mode	Modulation and Coding Scheme – indicates the modulation mode used for the radio uplink, based on radio conditions (MCS 1, 9-15).
DL MCS Mode	Modulation and Coding Scheme – indicates the modulation mode used for the radio downlink, based on radio conditions (MCS 1, 9-15).
Profile	The current MIR profile number to which the STA is configured.
UL Rate	The current Maximum Information Rate (in Kbps) on the Uplink to which the STA is configured.
DL Rate	The current Maximum Information Rate (in Kbps) on the Downlink to which the STA is configured.

AP GPS Status page

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

Figure 30 AP GPS Status page

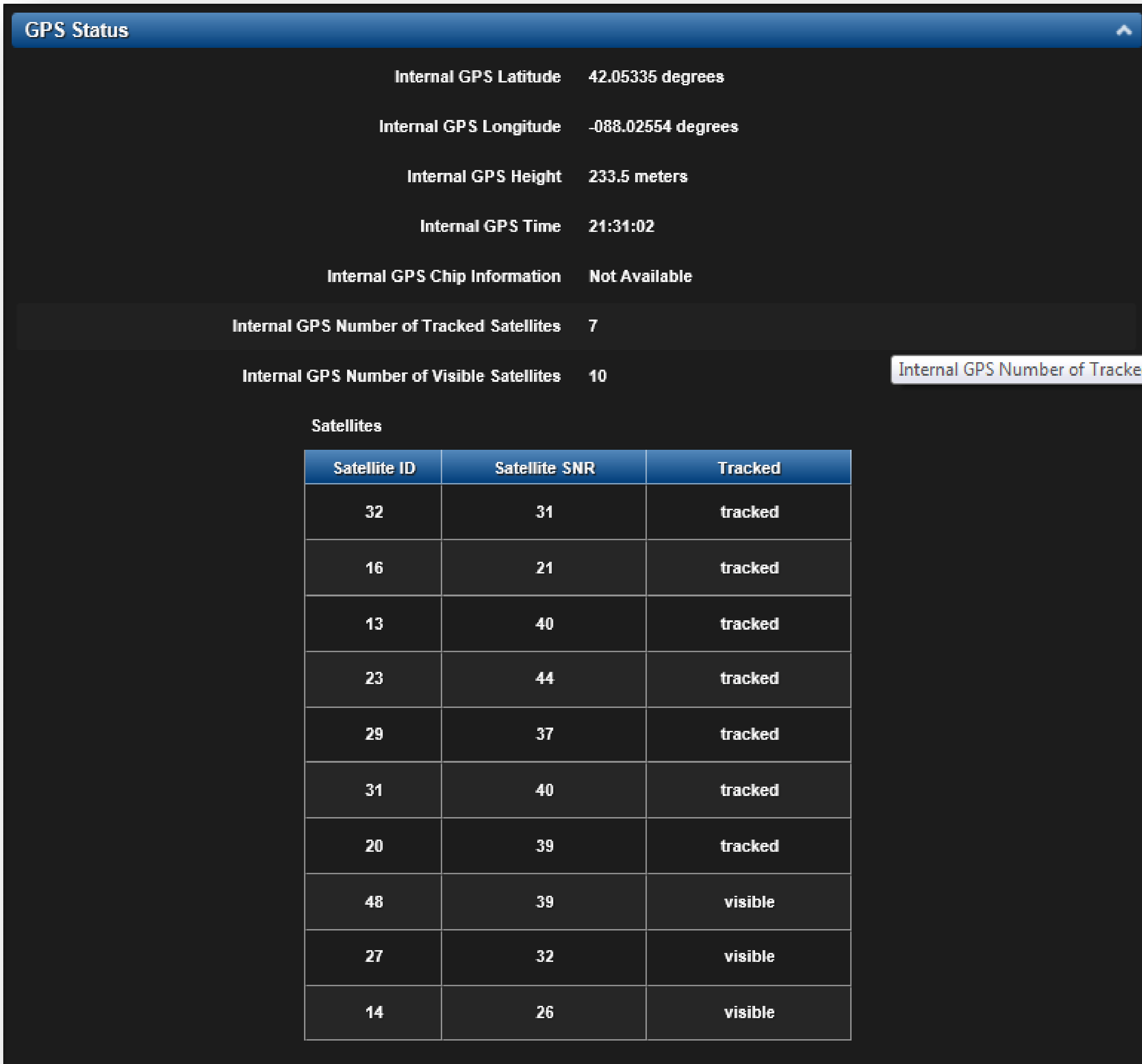


Table 54 AP GPS Status page attributes

Attribute	Meaning
Internal GPS Latitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Latitude information from the on-board GPS chip.

Attribute	Meaning
Internal GPS Longitude	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Longitude information from the on-board GPS chip.
Internal GPS Height	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device height above sea level from the on-board GPS chip.
Internal GPS Time	On a GPS Synchronized ePMP radio, the field is automatically populated with the time from the on-board GPS chip.
Internal GPS Number of Tracked Satellites	On a GPS Synchronized ePMP radio, the field indicates the number of satellites current tracked by the on-board GPS chip.
Internal GPS Number of Visible Satellites	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.

AP Network Status page

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

Figure 31 AP Network Status page

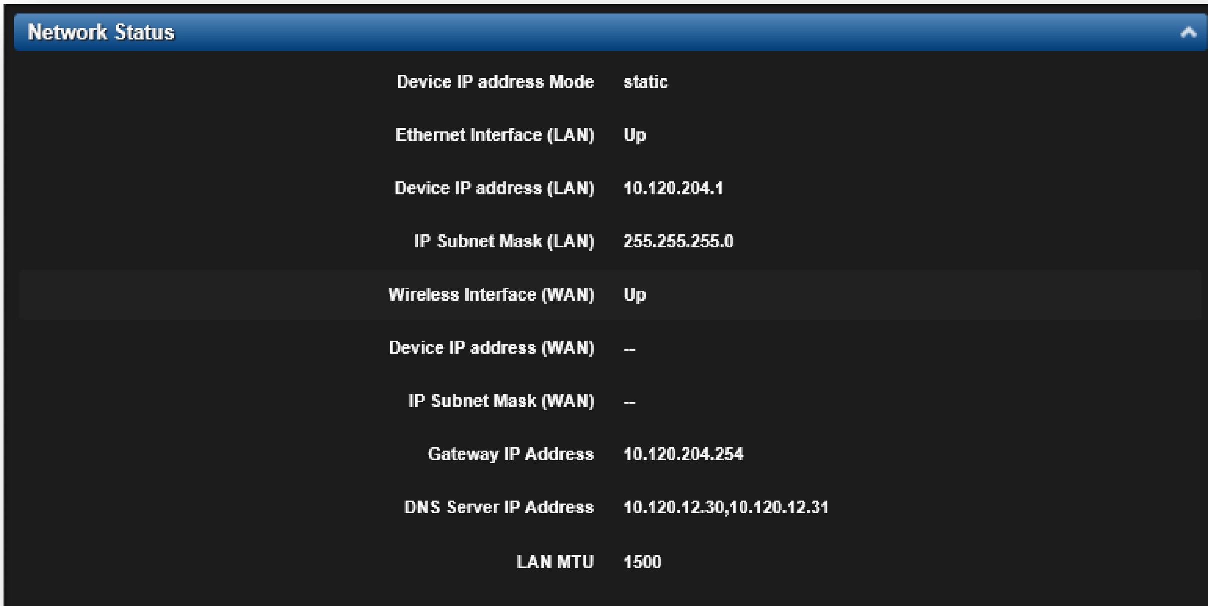


Table 55 AP Network Status page attributes

Attribute	Meaning
Device IP Address Mode	The current IP Address mode of the device (static or DHCP).
Ethernet Interface (LAN)	**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.
Device IP address (LAN)	The currently configured Ethernet IP address, used for device management.
IP Subnet Mask (LAN)	The currently configured device IP subnet mask.
Wireless Interface (WAN)	**Up**: The device wireless interface is functioning and passing data **Down**: The device wireless interface has encountered an error disallowing full operation. Reset the device to reinitiate the wireless interface.

Attribute	Meaning
Device IP address (WAN)	Currently unused.
IP Subnet Mask (WAN)	Currently unused.
Gateway IP Address	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.
DNS Server IP Address	The IP address of the server used for DNS resolution.
LAN MTU	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.

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.

Figure 32 AP System Log page

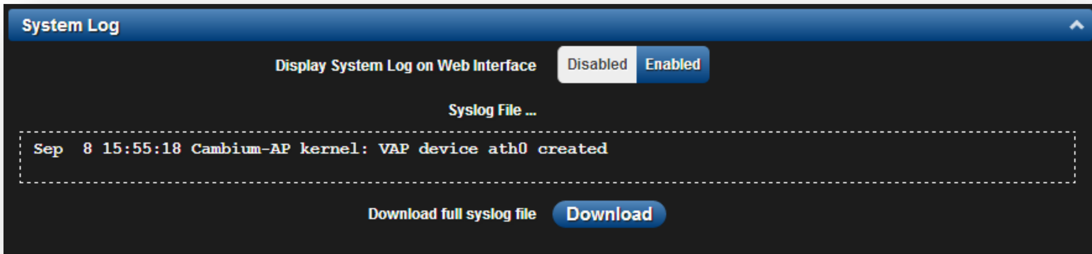


Table 56 AP System Log attributes

Attribute	Meaning
Display System Log on Web Interface	**Enabled**: The system log file is displayed on the management GUI. **Disabled**: The system log file is hidden on the management GUI.
Download full syslog file	Use this button to download the full system log file to a connected PC/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 on page 130
- AP Factory Default page on page 132
- AP Spectrum Analyzer page on page 133
- AP Throughput Test page on page 136
- AP Ping page on page 137
- AP Traceroute page on page 138

AP Software Upgrade page

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

Caution

Read the Release Notes associated with each software release.

Figure 33 AP Software Upgrade page

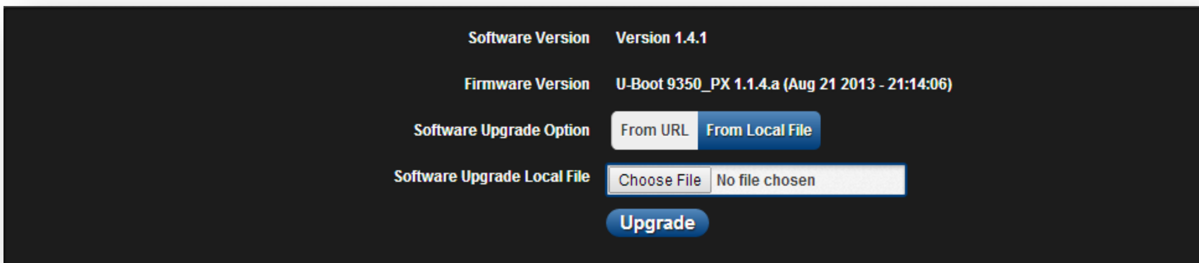


Table 57 AP Software Upgrade attributes

Attribute	Meaning
Software Version	The current operating software version
Firmware Version	The current U-Boot version
SW Upgrade Option	**From URL**: A webserver may be used to retrieve software upgrade packages (downloaded to the device via the webserver). For example, if a webserver is running at IP address 192.168.2.1 and the software upgrade packages are located in the home directory, an operator may select option **From URL** and configure the **Software Upgrade Source Info** field to **http://192.168.2.1/<software_upgrade_package>** **From Local File**: Click Browse to select the local file containing the software upgrade package.
Software Upgrade Local 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 from a local file (or network-accessible file), follow this:

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 **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 completes successfully, click the **Reset** icon

AP Factory Default page

Use the AP Factory Default page to reset the device to its factory default configuration. For more factory defaulting methods, see:

- Using the device external reset button on page 206
- Resetting the AP or STA to factory defaults by power cycling on page 207

Figure 34 AP Factory Default page

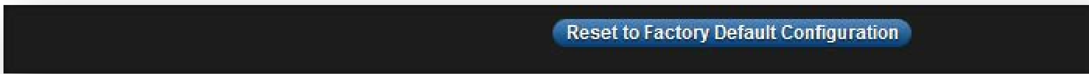


Table 58 AP Software Upgrade attributes

Attribute	Meaning
Reset to Factory Default Configuration	Use this button to reset the device to its factory default configuration Caution A reset to factory default configuration resets all device parameters. The AP will cease to transmit and any registered STAs will lose their session.

AP Spectrum Analyzer page

Use the AP Spectrum Analyzer page to configure AP 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 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 throughout the week.

To conduct a spectrum analysis, follow this:

Required Software:

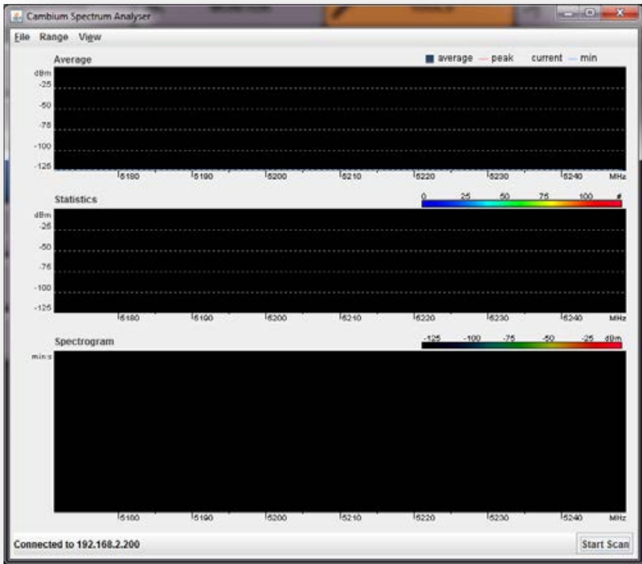
- Java Run-time Environment (JRE)

Procedure:

1. On the AP 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 AP GUI, then 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, tick the checkbox next to "*I accept the risk and want to run this application*"

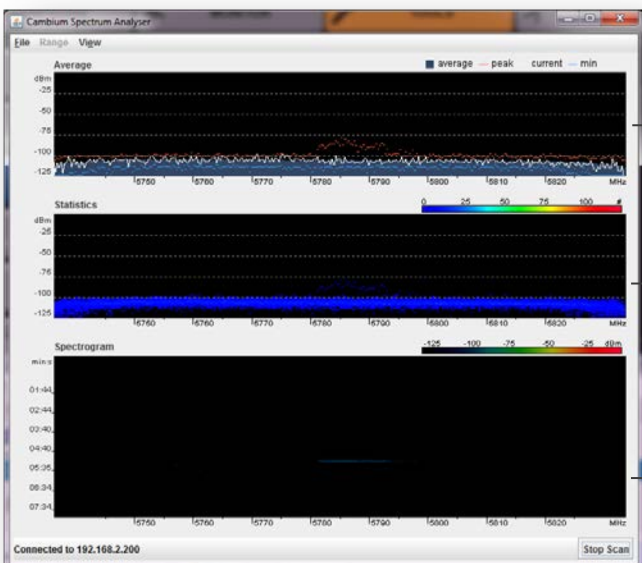
9 In the security warning window, click **Run**

The spectrum analyzer interface is displayed



10 Click **Range** to configure the range of frequencies to scan.

11 Click **Start Scan** to begin scanning



Display of the average, peak, current, and minimum power levels for the configured range

Statistical display of the number of times each frequency in the range was scanned

Spectrogram display of the energy levels detected throughout the configured range, over time

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** => **System**

4 Configure **Device Mode** to **AP**

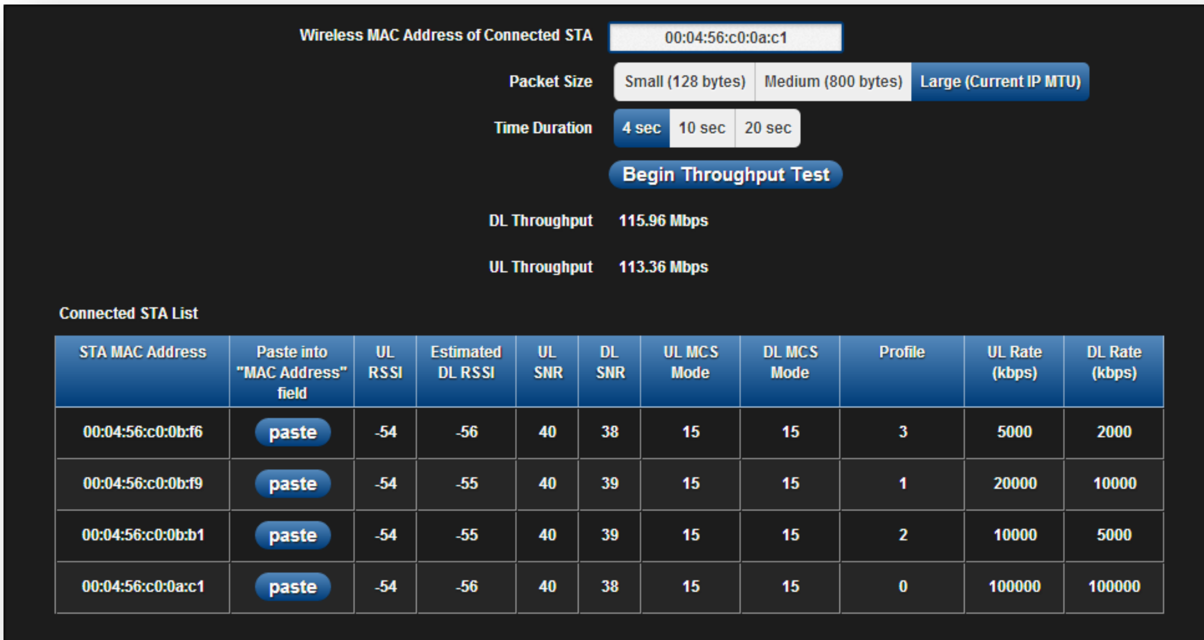
5 Click the **Save** button

6 Click the **Reset** button

AP Throughput Test page

Use the AP Throughput Test page to conduct a simple test of AP wireless throughput to any one of the connected STAs. This allows you to determine the throughput that can be expected on a particular link without having to use external tools.

Figure 35 AP Throughput Test page



STA MAC Address	Paste into "MAC Address" field	UL RSSI	Estimated DL RSSI	UL SNR	DL SNR	UL MCS Mode	DL MCS Mode	Profile	UL Rate (kbps)	DL Rate (kbps)
00:04:56:c0:0b:f6	paste	-54	-56	40	38	15	15	3	5000	2000
00:04:56:c0:0b:f9	paste	-54	-55	40	39	15	15	1	20000	10000
00:04:56:c0:0b:b1	paste	-54	-55	40	39	15	15	2	10000	5000
00:04:56:c0:0a:c1	paste	-54	-56	40	38	15	15	0	100000	100000

Table 59 AP Throughput Test attributes

Attribute	Meaning
Wireless MAC Address of Connected STA	Enter the MAC Address of one of the connected STAs or simply click the "paste" button of the STA desired in the "Connected STA List".
Packet Size	Choose the Packet Size to use for the throughput test.
Time Duration	Choose the Time Duration in seconds to use for the throughput test.
DL Throughput	This field indicates the result of the throughput test on the downlink, in Mbps.
UL Throughput	This field indicates the result of the throughput test on the uplink, in Mbps.
Connected STA list	Use the Connected STA List table to monitor registered STAs and their key RF status and statistics information. Click "paste" on the STA 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 36 AP Ping page

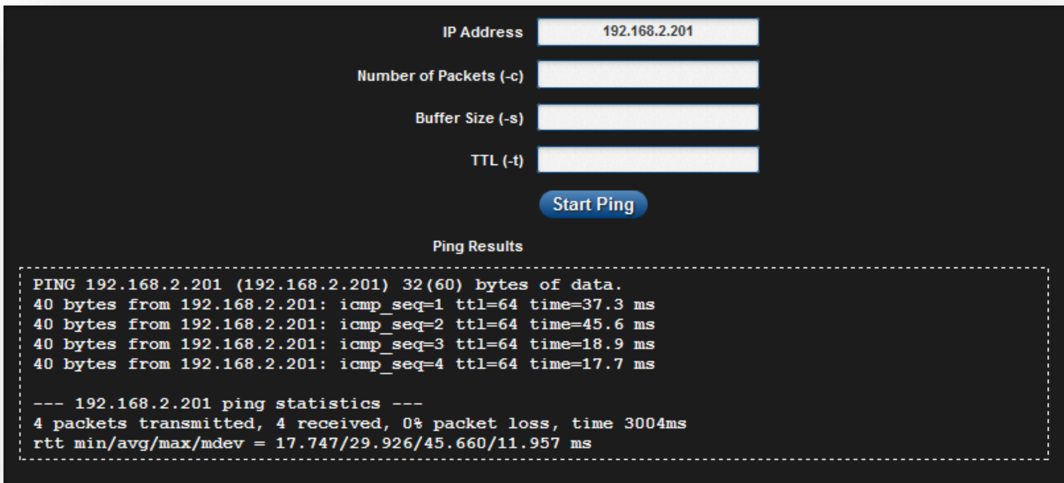


Table 60 AP Ping attributes

Attribute	Meaning
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.

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 37 AP Traceroute page

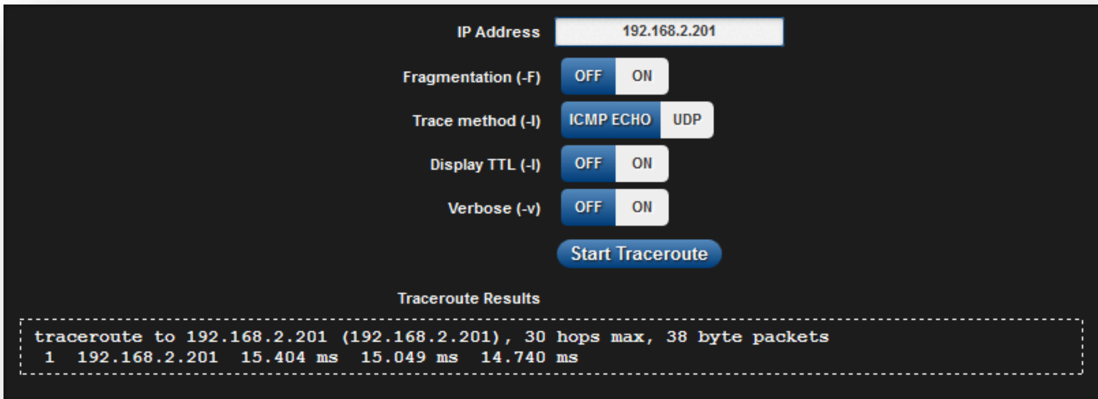


Table 61 AP Traceroute attributes

Attribute	Meaning
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 source or target).
Trace method (-I)	**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.

Using the STA menu options

Use the menu navigation bar in the top and left panels to navigate to each web page. Table 45 lists the functional areas that may be accessed from each menu option. Some of the parameters are only displayed for specific system configurations.

Table 62 Functional areas accessed from each menu option

Menu option	Menu Details
Configure	STA Configuration menu on page 140
Radio	STA Radio page on page 141
Quality of Service	STA Quality of Service page on page 144
System	STA System page on page 148
Network	STA Network page on page 152
Security	STA Security page on page 161
Monitor	STA Monitor menu on page 165
Performance	STA Performance page on page 166
System Status	STA System Status page on page 169
Wireless Status	STA Wireless Status page on page 171
Network Status	STA Network Status page on page 174
System Log	STA System Log page on page 176
Tools	STA Tools menu on page 177
Software Upgrade	STA Software Upgrade page on page 178
Factory Default	STA Factory Default page on page 180
Spectrum Analyzer	STA Spectrum Analyzer page on page 181
Throughput Test	STA Throughput Test page on page 184
Ping	STA Ping page on page 185
Traceroute	STA Traceroute page on page 186
Quick Start	Configuring STA units using the Quick Start menu on page 86

STA CONFIGURATION MENU

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

- STA Radio page on page 141
- STA Quality of Service page on page 144
- STA System page on page 148
- STA Network page on page 152
- STA Security page on page 161

STA 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.

Figure 38 STA Radio page

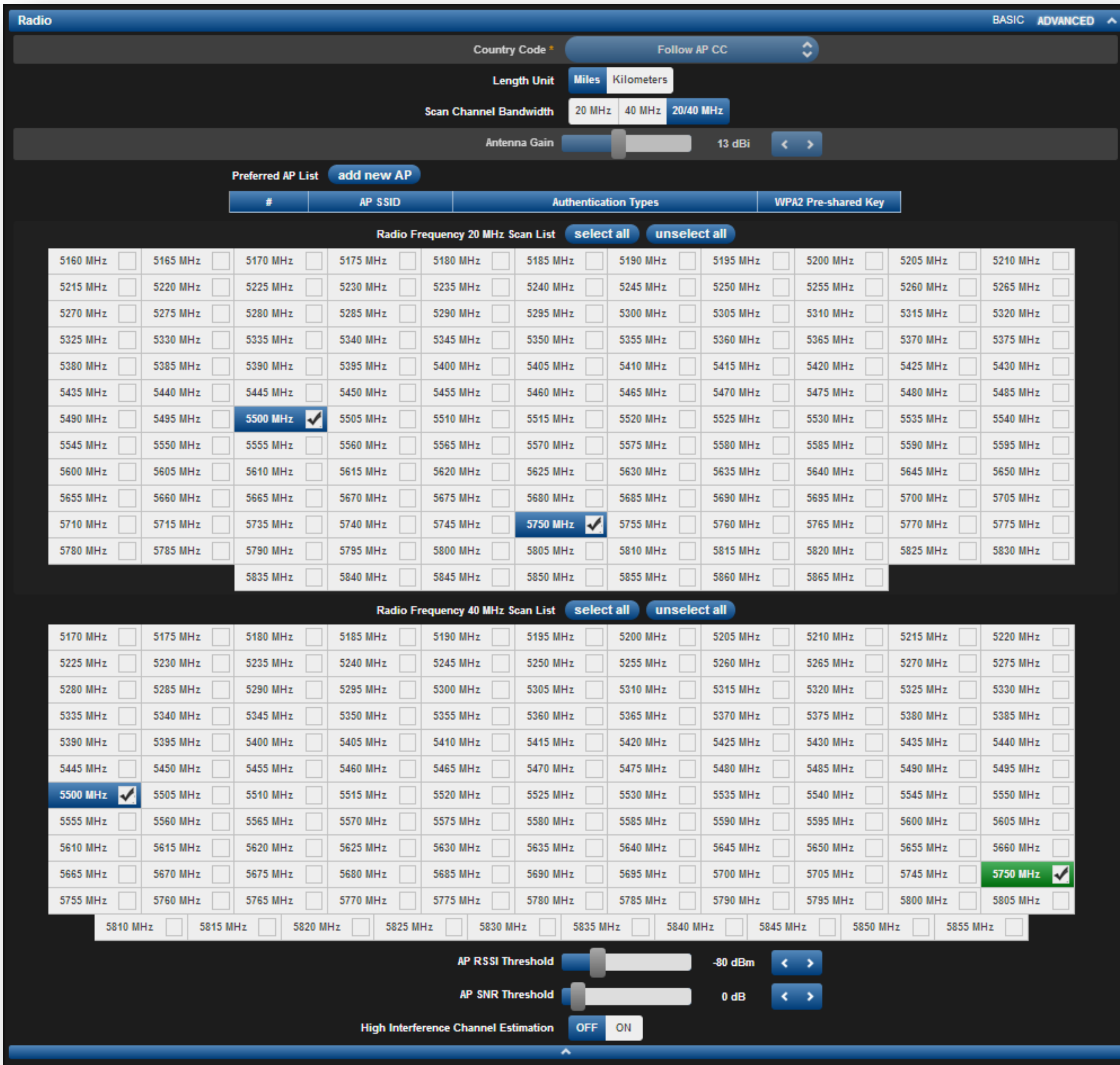


Table 63 STA Radio Configuration attributes

Attribute	Meaning
Country Code	The STA automatically inherits the Country Code setting of the AP (except for US-locked devices). **Country Code** settings affect the radios in the following ways: • Maximum transmit power limiting (based on radio transmitter power plus configured antenna gain) • DFS operation is enabled based on the configured country code, if applicable • Frequency selection is based on local regulatory limits
Length Unit	The unit of measurement used for reporting **Distance from AP**.
Scan Channel Bandwidth	**20 MHz**: The STA scans and operates with a 20 MHz-wide channel. To associate to an AP, the AP must have the same channel bandwidth as the STA. **40 MHz:** The STA scans and operates with a 40 MHz-wide channel. To associate to an AP, the AP must have the same channel bandwidth as the STA. **20/40 MHz:** The STA scans both 20 MHz and 40 MHz wide channels, based on the configured **Radio Frequency 20 MHz Scan List** and the configured **Radio Frequency 40 MHz Scan List**.
Antenna Gain	This value represents the amount of gain introduced by the units internal antenna. This parameter is read-only.
Preferred AP List	The **Preferred AP List** is comprised of a list of up to 16 APs to which the STA sequentially attempts registration. For each AP configured, if authentication is required, enter a **Pre-shared Key** associated with the configured **AP SSID**.
AP SSID	Enter the AP Name (SSID) of the AP to which registration will be attempted.
Authentication Types	Enter the type of authentication preferred, whether **EAP-TTLS**, **WPA2**, **Open** or a combination of the three.
WPA2 Pre-shared Key	If encryption is enabled on the AP, enter the Pre-shared Key which matches the Pre-shared Key configured on the AP.

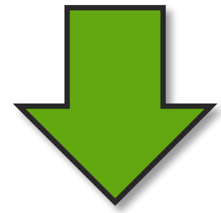
Attribute	Meaning
Radio Frequency 20 MHz Scan List	Select the frequencies for the STA to scan to attempt AP network entry (with 20 MHz wide channel). To register to an AP, the STA must be configured with the same frequency that is configured on the AP (AP parameter **Frequency Carrier**). Note If operating in a DFS-required region, ensure that the STA is also configured with the same frequencies as are configured in the AP's **DFS Alternate Frequency Carrier 1** and **DFS Alternate Frequency Carrier 2** parameters.
Radio Frequency 40 MHz Scan List	Select the frequencies for the STA to scan to attempt AP network entry (with 40 MHz wide channel). To register to an AP, the STA must be configured with the same frequency that is configured on the AP (AP parameter **Frequency Carrier**). Note If operating in a DFS-required region, ensure that the STA is also configured with the same frequencies as are configured in the AP's **DFS Alternate Frequency Carrier 1** and **DFS Alternate Frequency Carrier 2** parameters.
AP RSSI Threshold	Set this parameter to the minimum Received Signal Strength Indicator (RSSI) at the STA required for the STA to attempt registration to an AP. For example, if the **AP RSSI Threshold** is set to -80 dBm, and the STA is receiving the AP signal at -85 dBm (RSSI = -85 dBm), the STA will not attempt to register to the AP.
AP SNR Threshold	Set this parameter to the minimum Signal-to-Noise Ratio (SNR) at the STA required for the STA to attempt registration to an AP. For example, if the **AP SNR Threshold** is set to 30 dB and the STA is calculating its DL CINR as 25 dB, the STA will not attempt to register to the AP.

STA Quality of Service page

The ePMP platform supports three QoS priority levels using an air-fairness, priority-based starvation avoidance scheduling algorithm:

Priority Level	ePMP Traffic Priority Label
Highest Priority (Served first)	VOIP
Medium Priority (Served once highest priority traffic is sent)	High
Lowest Priority (Serviced once Highest and Medium priority traffic is sent)	Low

Priority



- VoIP Priority (only utilized when **VOIP Enable** is set to **Enabled**)
- High Priority
- Low Priority

By default, all traffic passed over the air interface is low priority. The STA'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 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 STA field **MIR Profile Setting** is used to configure the appropriate MIR profile for limiting the STA's data rate.

Figure 39 STA Quality of Service page

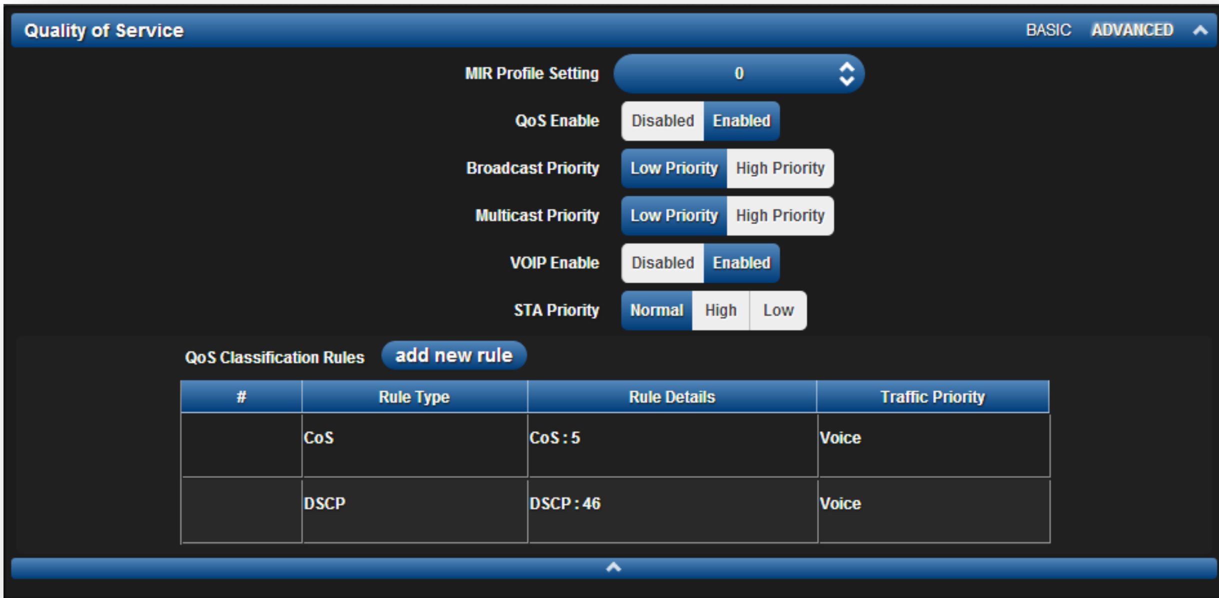


Table 64 STA Radio Configuration attributes

Attribute	Meaning
MIR Profile Setting	Configure the desired MIR (Maximum Information Rate) profile for STA operation. This profile must be configured on the AP, otherwise the default profile (0) is used.
QoS Enable	**Enabled**: The QoS Classification Rules table is editable and is utilized by the device to classify traffic. **Disabled**: The QoS Classification Rules table is greyed-out and all traffic is sent at one priority level.
Broadcast Priority	**Low Priority**: All Broadcast traffic sent over the uplink is prioritized as low priority, and will be delivered to the AP after scheduled high priority and VoIP traffic. **High Priority**: All Broadcast traffic sent over the uplink is prioritized as high priority, and will be scheduled for delivery to the AP before low priority traffic but after VoIP traffic.
Multicast Priority	**Low Priority**: All Multicast traffic sent over the uplink is prioritized as low priority, and will be delivered to the AP after scheduled high priority and VoIP traffic. **High Priority**: All Multicast traffic sent over the uplink is prioritized as high priority, and will be scheduled for delivery to the AP before low priority traffic but after VoIP traffic.

Attribute	Meaning
VOIP Enable	**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 highest priority. The **CoS** and **DSCP** values may be modified to accommodate non-standard VoIP equipment.
STA Priority	**Normal**: STA will give 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". **High**: STA will place all data other than VoIP in the "High" queue. It will be given higher priority than STAs configured with "Low" and "Normal" when there is contention for bandwidth under the AP. **Low**: "Low" priority will place all data that is not VoIP in "Low" priority queue. It will be given lower priority than STAs configured with "High" when there is contention for bandwidth under the same AP. "VoIP" queue is the highest priority queue followed by "High" queue and then by "Low" queue. Higher priority queues have preference over lower priority queues, but will not starve them.
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**.

Attribute	Meaning
Rule Type	**DSCP**: Differentiated Services Code Point; traffic prioritization is based on the 6-bit Differentiated Services field in the IP header present in the Ethernet frame header in the packet ingress of the Ethernet port. **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 ingressing the STA's Ethernet port. **VLAN ID:** Traffic prioritization is based on the VLAN ID of the packet ingressing the STA's Ethernet port. **EtherType:** Traffic prioritization is based on the two octet Ethertype field in the Ethernet frame ingressing the STA's Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame. **IP:** Traffic prioritization is based on the source and/or destination IP addresses of the packet ingress of the STA's Ethernet port. A sub.net mask may be included to define a range of IP addresses to match. **MAC:** Traffic prioritization is based on the source and/or destination MAC addresses of the packet ingress of the STA'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.
Rule Details	The **Rule Details** column is used to configure each classification rule specified in column **Rule Type**.
Traffic Priority	**High**: Traffic ingressing the STA'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) **Low:** Traffic ingressing the STA'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).

STA System page

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

Figure 40 STA System page

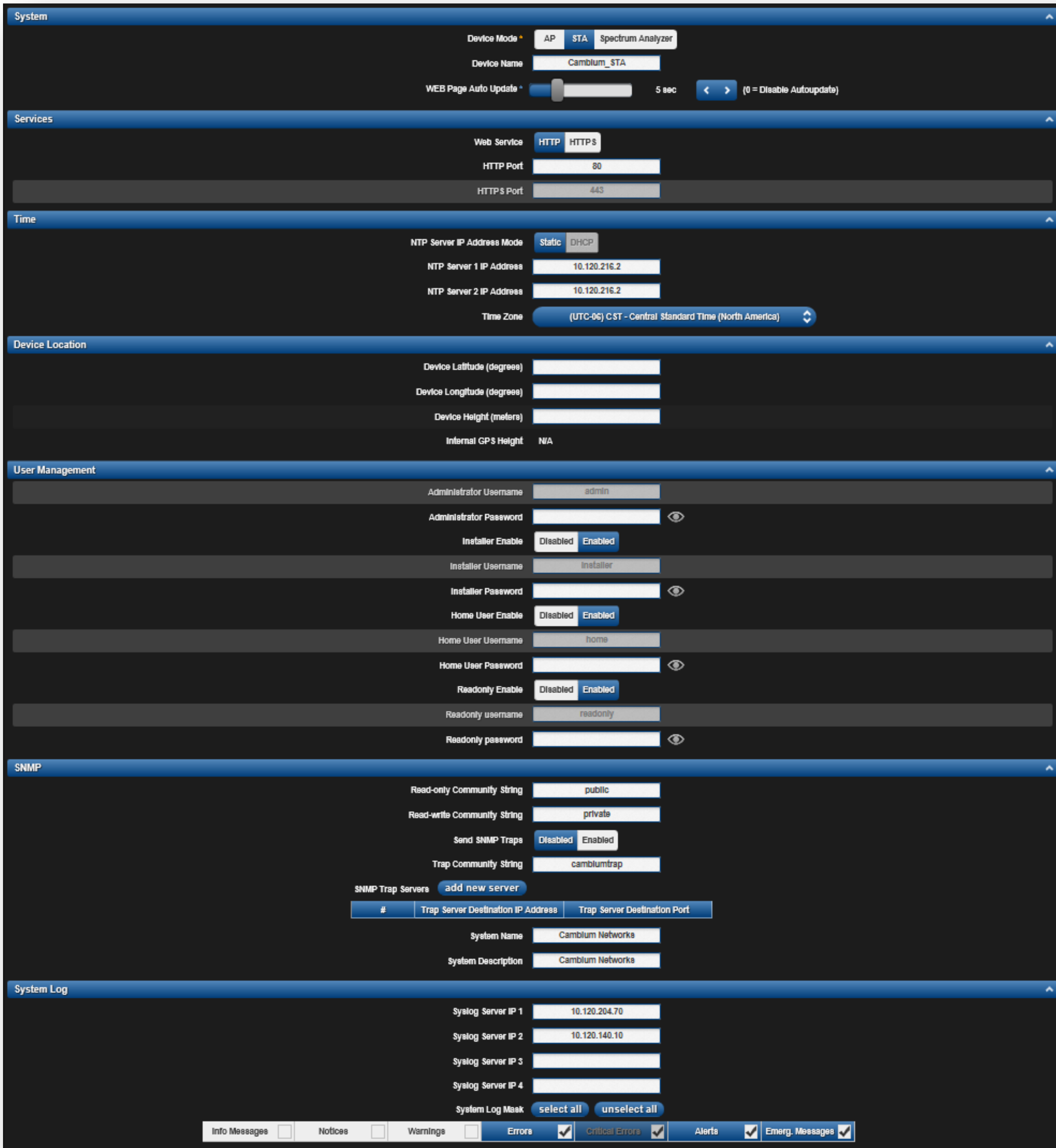


Table 65 STA System attributes

Attribute	Meaning
Device Mode	All ePMP devices may be configured to operate in one of three modes: **AP:** The device will operate as an AP **STA**: The device will operate as an STA **Spectrum Analyzer**: The devices will operate in Spectrum Analyzer mode, allowing the operator to download the spectrum analyzer tool.
Device Name	The **Device Name** is used to identify the STA on the network, and may be retrieved by a NMS such as the Cambium Network Services Server (CNSS).
WEB Page 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.
Web Service	**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.
NTP Server IP Address Mode	**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.
NTP Server 1,2 IP Address	Configure primary and secondary NTP server IP addresses from which the device will retrieve 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.
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 information for the device, in meters.
Internal GPS Height	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device height above sea level from the on-board GPS chip.

Attribute	Meaning
Administrator, Installer, Home User, Readonly Username	Read-only listing of available login levels. • 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, Installer, Home User	**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.
Administrator, Installer, Home User, Readonly Password	Configure a custom password configuration for each user to secure the device. The password character display may be toggled using the visibility icon .
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 **SNMP 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.
Send SNMP Traps	**Disabled**: With this setting, the radio will not send traps **Enabled**: Setting this will enable 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.
SNMP 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.
Trap Server Destination IP Address	Specify up to four SNMP Trap Servers to which the device will send SNMP traps.
Trap Server Destination Port	Configure port which the device uses to send SNMP traps.

Attribute	Meaning
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.
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.
Syslog Server IP 1-4	Specify up to four syslog servers to which the device sends syslog messages.
System Log Mask	Configure the levels of syslog messages which the devices send to the servers configured in parameters **Syslog Server IP 1-4**

STA Network page

The STA's Network page is used to configure system networking parameters and VLAN parameters. Parameter availability is based on the configuration of the **STA Network Mode** parameter.

Figure 41 STA Network page, NAT mode

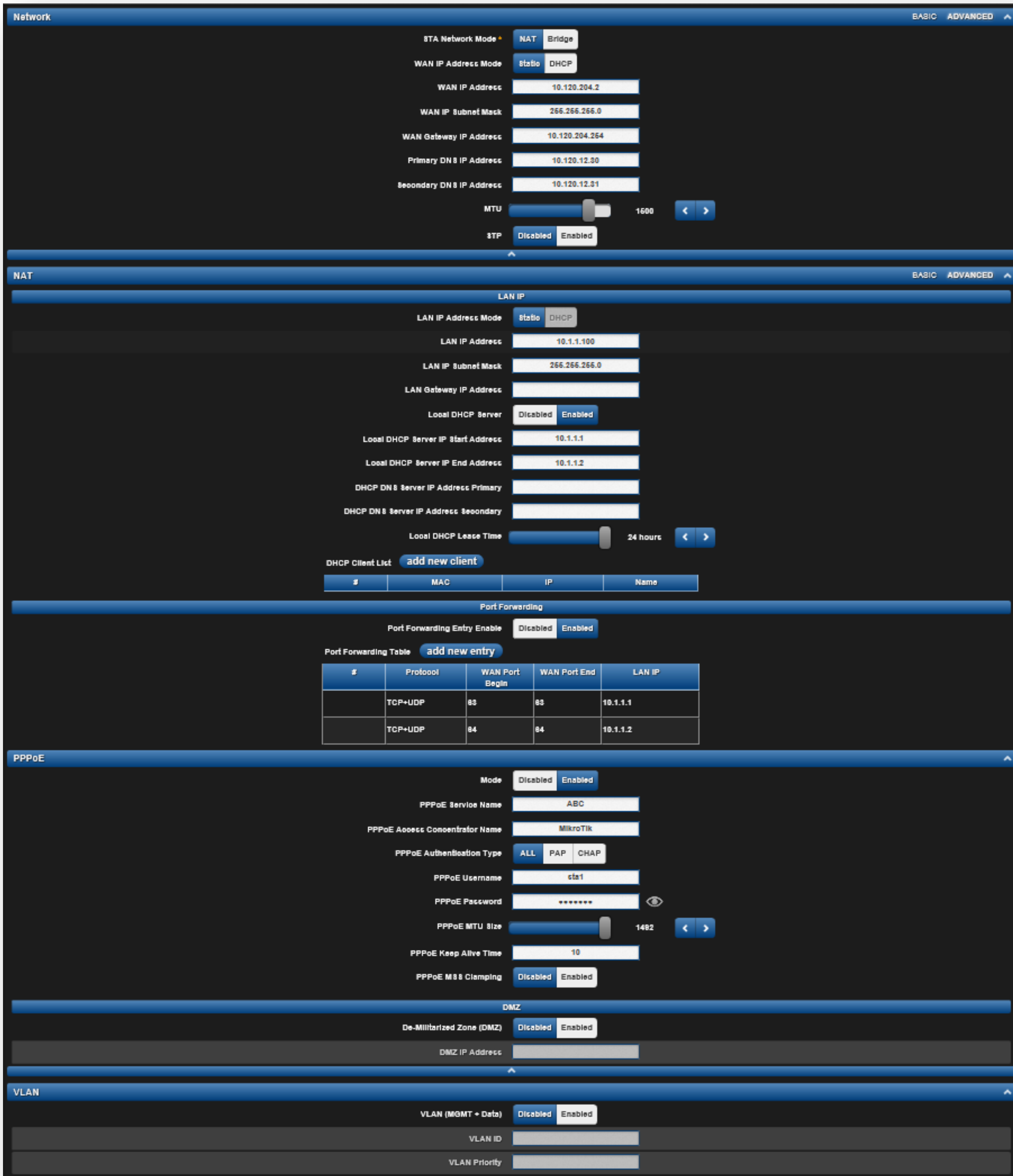


Table 66 STA Network attributes, NAT mode

Attribute	Meaning
STA Network Mode	**NAT**: The STA acts as a router and packets are forwarded or filtered based on their IP header (source or destination). **Bridge**: The STA acts as a switch, and packets are forwarded or filtered based on their MAC destination address.
Device IP Address Mode	**Static**: Wireless IP addressing is configured manually in fields **Device IP Address, Device IP Subnet Mask, Device Gateway IP Address, Primary DNS IP Address** and **Secondary DNS IP Address** **DHCP**: Device management IP addressing (IP address, subnet mask, gateway, and DNS server) is assigned via a network DHCP server.
Device 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.
Device IP Subnet Mask	Defines the address range of the connected IP network. For example, if **Device IP Address** is configured to 192.168.2.1 and **Device IP Subnet Mask** is configured to 255.255.255.0, the device wireless interface will belong to subnet 192.168.2.X.
Device Gateway IP Address	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.
Primary DNS IP Address	Configure The IP address of the primary server used for DNS resolution.
Secondary DNS IP Address	Configure The IP address of the secondary server used for DNS resolution.
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.
STP	**Disabled**: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the STA. **Enabled**: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the STA, allowing for the prevention of Ethernet bridge loops.
LAN IP Address Mode	**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)**
LAN IP Addess	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.

LAN IP 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.
LAN Gateway IP Address	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.
Local DHCP Server	**Disabled**: Use this setting when STA is in NAT mode, to use the DHCP server to hand out IP addresses to its clients. **Enabled**: Use this setting when STA is in NAT mode, to use the STA's local/onboard DHCP server to hand out IP addresses to its clients.
Local DHCP Server IP Start Address	Configure the first address which will be issued to a DHCP client. Upon additional DHCP requests, the **Local DHCP Server IP Start Address** will be incremented until **Local DHCP Server IP End Address** is reached.
Local DHCP Server IP End Address	Configure the final address which will be issued to a DHCP client.
DHCP DNS Server IP Address Primary	Configure the primary DNS Server IP address which will be used to configure DHCP clients (if **Local DHCP Server** is set to **Enabled**)
DHCP DNS Server IP Address Secondary	Configure the secondary DNS Server IP address which will be used to configure DHCP clients (if **Local DHCP Server** is set to **Enabled**)
Local 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 addressing via DHCP request.
DHCP Client List	The DHCP Client List table identifies hardware situated below the STA which shall be issued DHCP IP addressing information. The STA acts as a DHCP server, responding to requests from hardware connected to the STA.
MAC	Configure the physical address of the device which will retrieve DHCP IP addressing information from the STA.
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).
Port Forwarding Entry Enable	The STA port forwarding functionality may be used to configure the STA to route external network services to an internal IP address so that end devices (situated below the STA) are reachable from external networks. Caution Opening ports for forwarding may introduce a network security risk.

Port Forwarding Table	The **Port Forwarding Table** is used to define which range of wireless ports are forwarded to which LAN (STA local network) IP addresses.
Protocol	**UDP**: Packet forwarding decisions are based on UDP packets **TCP**: Packet forwarding decisions are based on TCP packets
WAN Port Begin	Configure the beginning of the range of wireless ports to match for forwarding to **LAN IP**
WAN Port End	Configure the end of the range of wireless ports to match for forwarding to **LAN IP**
LAN IP	Configure the LAN IP of the device situated below the STA which will receive the packets forwarded based on the **Port Forwarding Table** configuration.
PPPoE	**Point-to-Point Protocol over Ethernet**: Used for encapsulating PPP frames inside Ethernet frames.
Mode	**Disabled:** Default. **Enabled**: Configure this field to "Enabled" to setup a PPPoE tunnel on the STA.
PPPoE Service Name	An optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the STA will accept the first service option that comes back from the Access Concentrator specified below, if any. This is limited to 32 characters.
PPPoE Access Concentrator Name	An optional entry to set a specific Access Concentrator to connect to for the PPPoE session. If this is blank, the STA will accept the first Access Concentrator which matches the service name (if specified). This is limited to 32 characters.
PPPoE Authentication Type	**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.
PPPoE Username	This is the CHAP/PAP username that will be used. This is limited to 32 characters.
PPPoE Password	This is the CHAP/PAP password that will be used. This is limited to 32 characters.
PPPoE 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 will use the smaller value as its MTU for the PPPoE link.

PPPoE 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 acknowledgement, it will send the keep alive message to the server 4 more times (for a total or 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 acknowledgement, the client will try for a total of 12 times every 12 seconds before tearing down the PPPoE session.
PPPoE MSS Clamping	**Disabled**: The STA PPPoE session will allow any MTU size determined by other devices in the PPPoE session during the LCP negotiations. **Enabled**: The STA PPPoE session will enforce 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 a MTU setting that is smaller in value.
De-Militarized Zone (DMZ)	**Disabled**: No devices are configured to expose services to the local area network as well as the wide-area network. **Enabled**: When enabled, the device configured in **DMZ IP Address** may provide network services (web servers or FTP servers) to the network internal to the STA as well as the wide-area network (Internet).
DMZ IP Address	Configure the IP address of an STA-connected device which will be allowed to provide network services to the wide-area network.
VLAN	**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 STA is in NAT mode, the VLAN configuration is applicable to both management and user data. **Disabled**: When disabled, all IP management and data traffic is allowed to the device.
VLAN ID	Configure this parameter to include the device's management and user traffic on a separate VLAN network.

VLAN Priority	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 and management data. If the **VLAN Priority** field is configured, for traffic to traverse the device the accessing switch or end device must be configured to tag Ethernet frames with the **VLAN ID** value *and* the same priority values as configured in field **VLAN Priority**. For example, if **VLAN ID** is set to 100 and **VLAN Priority** is set to 5, the Ethernet frames sent to the STA to from a PC situated below the STA must be tagged with a VLAN ID value of 100 and Class of Service priority set to 5 to be sent over the air to the AP. If **VLAN Priority** is not configured (blank), for traffic to traverse the device the accessing switch or end device only needs to tag Ethernet frames with the same VLAN ID as is configured in the **VLAN ID** field.

Figure 42 STA Network page, Bridge mode

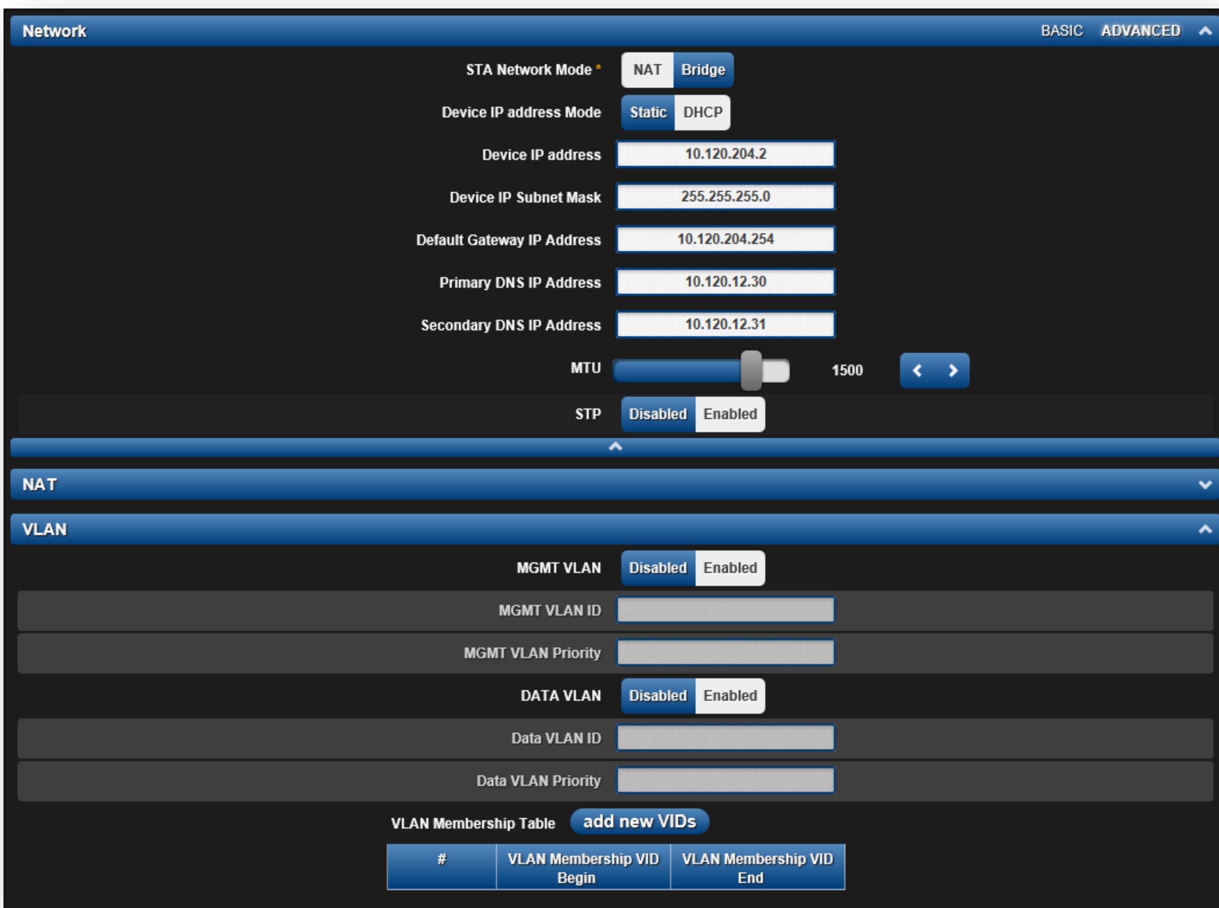


Table 67 STA Network attributes, Bridge mode

Attribute	Meaning
STA Network Mode	**NAT**: The STA acts as a router, and packets are forwarded or filtered based on their IP header (source or destination). **Bridge**: The STA acts as a switch, and packets are forwarded or filtered based on their MAC destination address
Device IP address Mode	**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.
Device IP Address	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. 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 (STA 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 10.1.1.254.
Device IP 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.
Device Gateway IP Address	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.
Primary DNS IP Address	Configure The IP address of the primary server used for DNS resolution.
Secondary DNS IP Address	Configure The IP address of the secondary server used for DNS resolution.
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.

STP	**Disabled**: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the STA. **Enabled**: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the STA, allowing for the prevention of Ethernet bridge loops.
MGMT VLAN	**Enabled**: The STA 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 STA's management interface can be accessed only by packets tagged with a VLAN ID matching the management VLAN ID. 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. **Disabled**: When disabled, all IP management traffic is allowed to the device.
MGMT 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.
MGMT VLAN Priority	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 device management traffic. If the **MGMT VLAN Priority** field is configured, to access the STA GUI the accessing switch or end device must be configured to tag Ethernet frames with the **MGMT VLAN ID** value *and* the same priority values as configured in field **MGMT VLAN Priority**. For example, if **MGMT VLAN ID** is set to 100 and **MGMT VLAN Priority** is set to 5, the Ethernet frames sent to the STA to access the GUI must be tagged with a VLAN ID value of 100 and Class of Service priority set to 5. If **MGMT VLAN Priority** is not configured (blank), to access the STA GUI the accessing switch or end device only needs to tag Ethernet frames with the same VLAN ID as is configured in the **MGMT VLAN ID** field.
Data VLAN ID	Configure this parameter to include the device's user traffic (i.e. Internet browsing, VoIP, or video) on a separate VLAN network. For example, if **Data VLAN ID** is set to 2, user data (i.e. Internet browsing, video) is allowed only from IP packets tagged with VLAN ID 2.

Data VLAN Priority	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. If the **Data VLAN Priority** field is configured, for user traffic to traverse the device the accessing switch or end device must be configured to tag Ethernet frames with the **Data VLAN ID** value *and* the same priority values as configured in field **Data VLAN Priority**. For example, if **Data VLAN ID** is set to 100 and **Data VLAN Priority** is set to 5, the user traffic Ethernet frames sent to the STA to from a PC situated below the STA must be tagged with a VLAN ID value of 100 and Class of Service priority set to 5 to be sent over the air to the AP. If **Data VLAN Priority** is not configured (blank), for user traffic to traverse the device the accessing switch or end device only needs to tag Ethernet frames with the same VLAN ID as is configured in the **Data VLAN ID** field.
VLAN Membership Table	Configure the STA **VLAN Membership Table** to include the STA in one or more VLANs. When the STA receives a packet tagged with a VLAN ID which is contained in the STA **VLAN Membership Table**, the packet is forwarded over the air interface to the AP. When the STA receives a packet tagged with a VLAN ID which is not present in the STA **VLAN Membership Table**, the frame is dropped.

STA Security page

The STA's Security page is used to configure system security features including STA 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 only **Action** set to **Deny** and **Interface** set to **LAN** or **WAN.** To regain access to the device, perform a factory default.

Figure 43 STA Security page

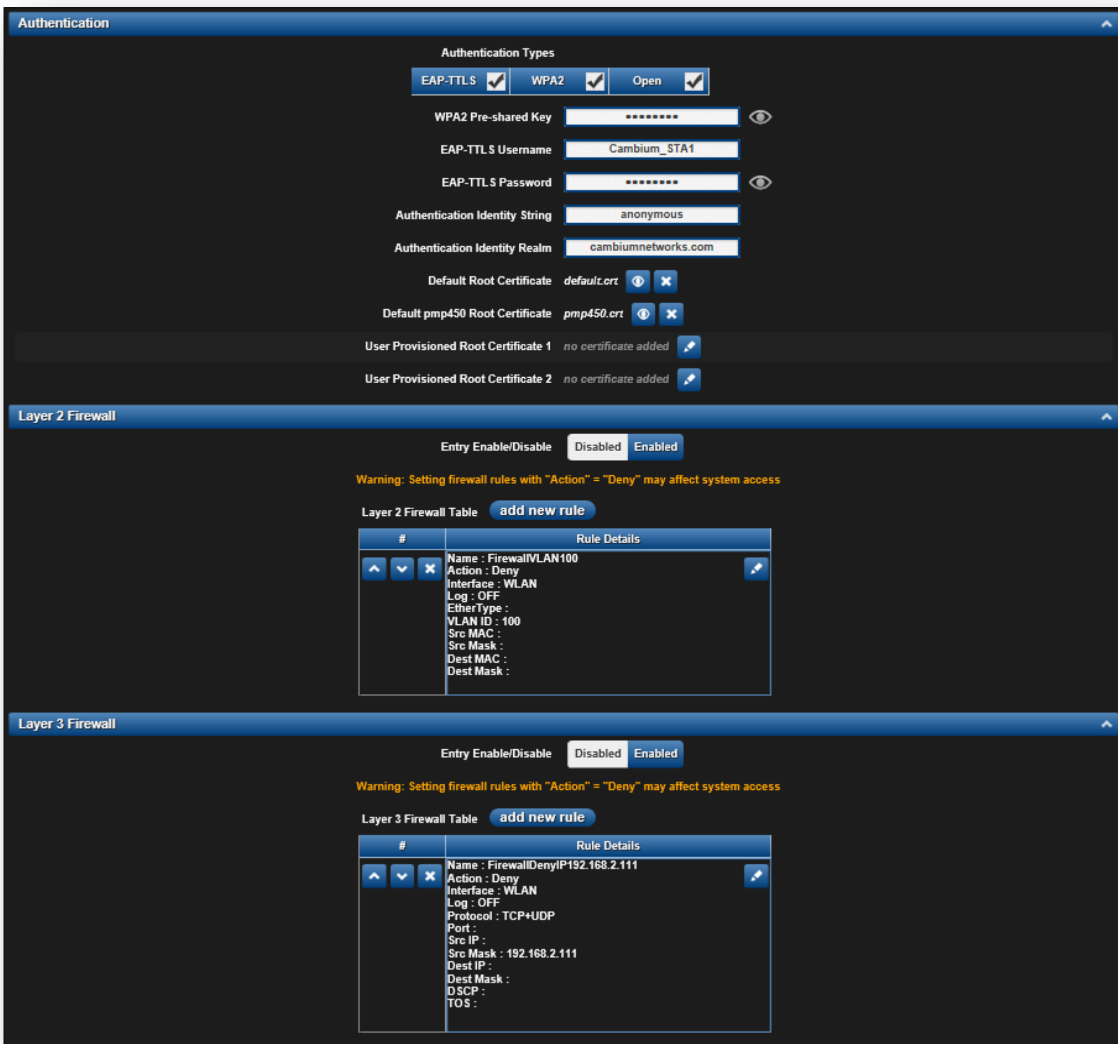


Table 68 STA Security attributes

Attribute	Meaning
Authentication Types	Enter the type of authentication preferred, whether **EAP-TTLS**, **WPA2**, **Open** or a combination of the three.
WPA2 Pre-shared Key	Configure this key on the AP, and then configure each of the network STAs with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.
EAP-TTLS Username	Configure the EAP-TTLS Username to match the credentials on the Radius server being used for the network.
EAP-TTLS Password	Configure the EAP-TTLS Password to match the credentials on the Radius server being used for the network.
Authentication Identity String	Configure this Identity string to match the credentials on the Radius server being used for the network. 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. 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
Default pmp450 Root Certificate	PMP 450 default EAP-TTLS root certificate to match the certificate on the Radius server used with current PMP 450 deployments.
User Provisioned Root Certificate 1	Import a user certificate if a certificate different from the default certificates is needed.
User Provisioned Root Certificate 2	Import a second user certificate if a certificate different from the default or 1st user provisioned certificate is needed.
Layer 2 Firewall Entry Enable/Disable	**Enabled**: Modifications to the Layer 2 Firewall Table are allowed and rules are enforced. **Disabled**: Modifications to the Layer 2 Firewall Table are not allowed and rules are not enforced.
Layer 2 Firewall Table	The Layer 2 firewall table may be used to configure rules matching layer 2 (MAC layer) traffic which result in forwarding or dropping the traffic over the radio link or Ethernet interface.
Rule Details, Name	Assign a logical name to the firewall rule based on the intended rule operation (i.e. "Deny all WLAN traffic from VLAN ID 100").
Rule Details, Action	**Accept**: Layer 2 traffic matching the rule details are forwarded. **Deny**: Layer 2 traffic matching the rule details are dropped at the device.

Rule Details, Interface	**WLAN**: When this option is selected, firewall rules are applied to traffic incoming on the device radio interface (WLAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will either be forwarded to the LAN (Ethernet) interface or dropped at the device. **LAN**: When this option is selected, firewall rules are applied to traffic incoming on the device Ethernet interface (LAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will be either forwarded to the WAN (radio) interface or dropped at the device
Rule Details, Log	**On**: When a firewall rule is matched, a resulting system log message is generated **Off**: When a firewall rule is matched, no system log messaging is generated
Rule Details, EtherType	Rule matching is based on the two octet Ethertype field in the Ethernet frame. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame.
Rule Details, VLAN ID	Rule matching is based on the VLAN ID of the packet
Rule Details, Src MAC	Firewall rule matching is based on the source MAC address of the packet
Rule Details, Src Mask	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.
Rule Details, Dest MAC	Firewall rule matching is based on the destination MAC address of the packet
Rule Details, Dest Mask	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.
Layer 3 Firewall Entry Enable/Disable	**Enabled**: Modifications to the Layer 3 Firewall Table are allowed and rules are enforced **Disabled**: Modifications to the Layer 3 Firewall Table are not allowed and rules are not enforced
Layer 3 Firewall Table	The Layer 3 firewall table may be used to configure rules matching layer 3 (IP layer) traffic which result in forwarding or dropping the traffic over the radio link or Ethernet interface.

Rule Details, Name	Assign a logical name to the firewall rule based on the intended rule operation (i.e. “Deny all WLAN traffic from Src IP 192.168.2.111”).
Rule Details, Action	**Accept**: Layer 3 traffic matching the rule details are forwarded. **Deny**: Layer 3 traffic matching the rule details are dropped at the device.
Rule Details, Interface	**WLAN**: When this option is selected, firewall rules are applied to traffic incoming on the device radio interface (WLAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will either be forwarded to the LAN (Ethernet) interface or dropped at the device. **LAN**: When this option is selected, firewall rules are applied to traffic incoming on the device Ethernet interface (LAN). Depending on the setting of the **Action** parameter, traffic matching the rule details will be either forwarded to the WAN (radio) interface or dropped at the device.
Rule Details, Log	**On**: When a firewall rule is matched, a resulting system log message is generated. **Off**: When a firewall rule is matched, no system log messaging is generated.
Rule Details, Protocol	**TCP**: Only TCP packets will be matched by the configured rule **UDP**: Only UDP packets will be matched by the configured rule **TCP+UDP**: Only TCP and UDP packets will be matched by the configured rule **ICMP**: Only ICMP packets will be matched by the configured rule **IP**: All IP packets will be matched by the configured rule
Rule Details, Port	Rule matching is based on the port value in the incoming packet.
Rule Details, Src IP	Rule matching is based on the Source IP address of the incoming packet.
Rule Details, Src Mask	A subnet mask may be included to define a range of IP addresses to match. For example, if **Src IP** is configured to 192.168.2.0 and **Src Mask** is configured to 255.255.255.0, the rule matches all IP addresses from subnetwork 192.168.2.X.
Rule Details, Dest IP	Rule matching is based on the Destination IP address of the incoming packet.
Rule Details, Dest Mask	A subnet mask may be included to define a range of IP addresses to match. For example, if **Dest IP** is configured to 192.168.2.0 and **Dest Mask** is configured to 255.255.255.0, the rule matches all IP addresses from subnetwork 192.168.2.X.
Rule Details, DSCP	Rule matching is based on the DiffServ CodePoint value of the incoming packet
Rule Details, TOS	Rule matching is based on the Type Of Service value of the incoming packet.

STA 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:

STA Performance page

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

Figure 44 STA Performance page

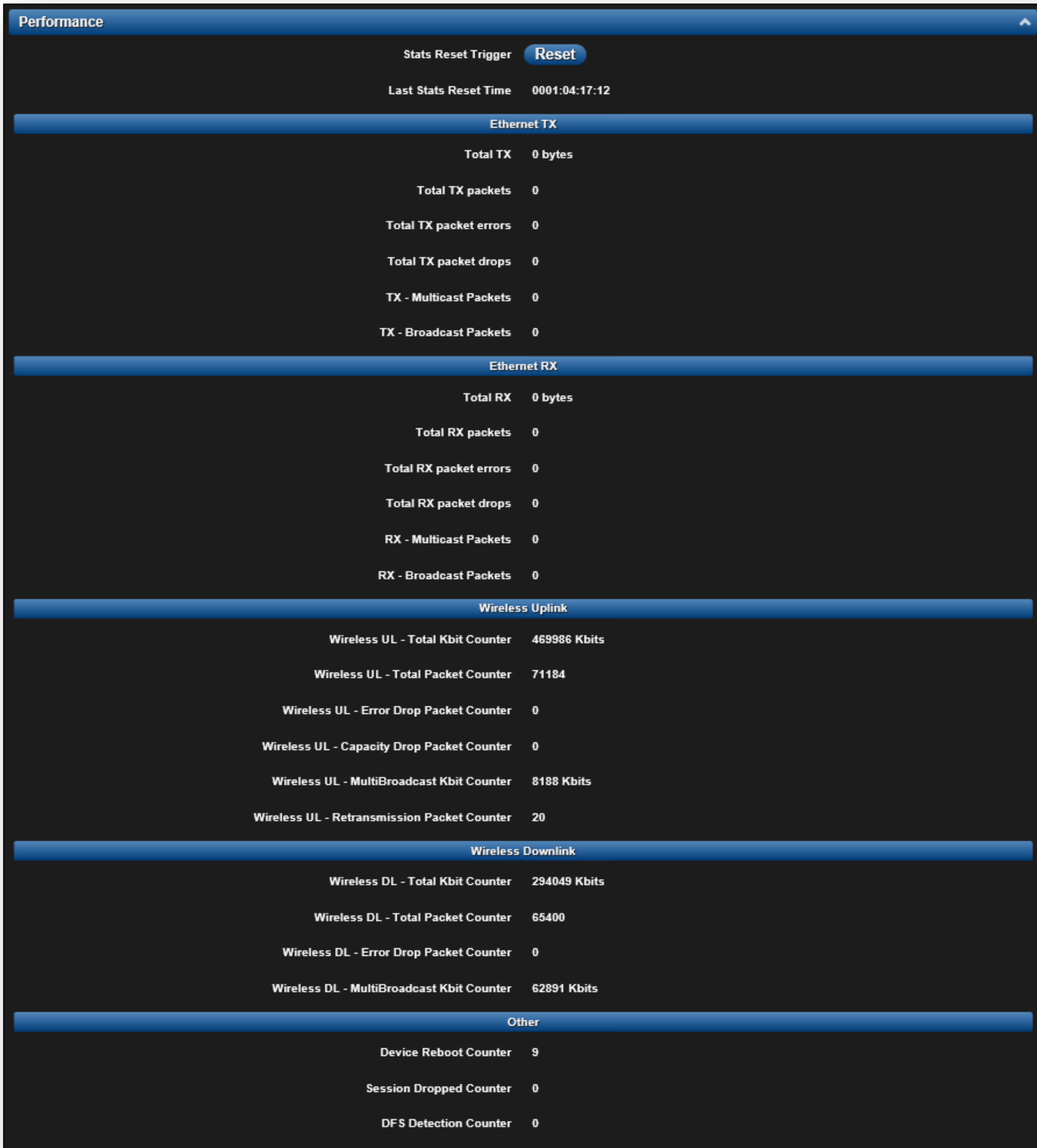


Table 69 STA Performance page attributes

Attribute	Meaning
Stats Reset Trigger	Reset all statistics.
Ethernet TX, Total TX	Total count of bytes transferred from the STA's Ethernet interface.
Ethernet TX, Total TX packets	Total count of packets transferred from the STA's Ethernet interface.
Ethernet TX, Total TX packet errors	Total count of packets transmitted out of the STA's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Ethernet TX, Total TX packet drops	Total count of packets dropped prior to sending out of the AP's Ethernet interface due to Ethernet setup or filtering issues.
Ethernet TX, TX – Multicast Packets	Total count of multicast packets sent via the STA's Ethernet interface.
Ethernet TX, TX – Broadcast Packets	Total count of broadcast packets sent via the STA's Ethernet interface.
Ethernet RX, Total RX	Total count of bytes received by the STA's Ethernet interface.
Ethernet RX, Total RX packets	Total count of packets received by the STA's Ethernet interface.
Ethernet RX, Total RX packet errors	Total count of packets received by the STA's Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Ethernet RX, Total RX packet drops	Total count of packets dropped prior to sending out of the STA's wireless interface due to Ethernet setup or filtering issues.
Ethernet RX, RX – Multicast Packets	Total count of multicast packets received via the STA's Ethernet interface.
Ethernet RX, RX – Broadcast Packets	Total count of broadcast packets received via the STA's Ethernet interface.
Wireless Uplink, Total Kbit Counter	Total count of packets transmitted out of the STA's wireless interface in Kbits.
Wireless Uplink, Total Packet Counter	Total count of packets transmitted out of the STA's wireless interface.
Wireless Uplink, Error Drop Packet Counter	Total count of packets dropped after transmitting out of the STA's wireless interface due to RF errors (No acknowledgement and other RF related packet error).
Wireless Uplink, Capacity Drop Packet Counter	Total count of packets dropped after transmitting out of the STA's wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).

Attribute	Meaning
Wireless Uplink, MultiBroadcast Kbit Counter	Total count of multicast and broadcast packets transmitted out of the STA's wireless interface in Kbits.
Wireless Uplink, Retransmission Packet Counter	Total count of packets retransmitted after transmitting out of the STA's Wireless interface due to RF errors (No acknowledgement and other RF related packet error).
Wireless Downlink, Total Kbit Counter	Total Kbits received via the STA's wireless interface.
Wireless Downlink, Total Packet Counter	Total count of packets received via the STA's wireless interface.
Wireless Downlink, Error Drop Packet Counter	Total count of packets dropped prior to sending out of the STA's Ethernet interface due to RF errors (packet integrity error and other RF related packet error).
Wireless Downlink, MultiBroadcast Kbit Counter	Total count of multicast and broadcast packets received on the STA's wireless interface in Kbits.
Device Reboot Counter	Count of the number of reboots on the device since it has been powered up.
Session Dropped Counter	Count of the number of times the STA deregistered with the AP since the first registration.
DFS Detection Counter	Count of the number of times the STA triggered a DFS event.

STA System Status page

Use the System Status page to reference key system information.

Figure 45 STA System Status page

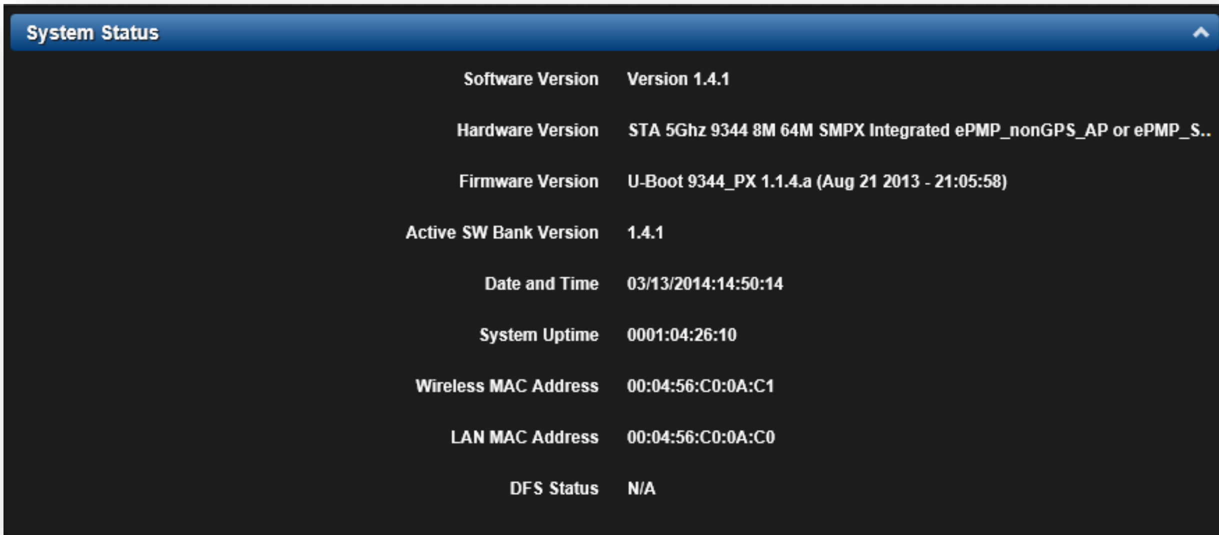


Table 70 STA System Status page attributes

Attribute	Meaning
Software Version	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).
Hardware Version	Board hardware version information.
Firmware Version	U-Boot version information.
Active SW Bank Version	Current operating version of software on the device in the active partition. This must be the same as the Software Version field above when the device is under normal operation.
Date and Time	Current date and time, subject to time zone offsets 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 wireless interface.
LAN MAC Address	The hardware address of the device LAN (Ethernet) interface.

Attribute	Meaning
DFS Status	**N/A:** DFS operation is not required for the region configured in parameter **Country Code** **Channel Availability Check**: Prior to 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** **In-Service Monitoring**: Radio is transmitting and receiving normally while monitoring for radar pulses which require a channel move **Radar Signal Detected**: The receiver has detected a valid radar pulse and is carrying out detect-and-avoid mechanisms (moving to an alternate channel). **In-Service Monitoring at Alternative Channel**: The radio has detected a radar pulse and has moved operation to a frequency configured in **DFS Alternative Frequency Carrier 1** or **DFS Alternative Frequency Carrier 2** **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

STA Wireless Status page

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

Figure 46 STA Wireless Status page

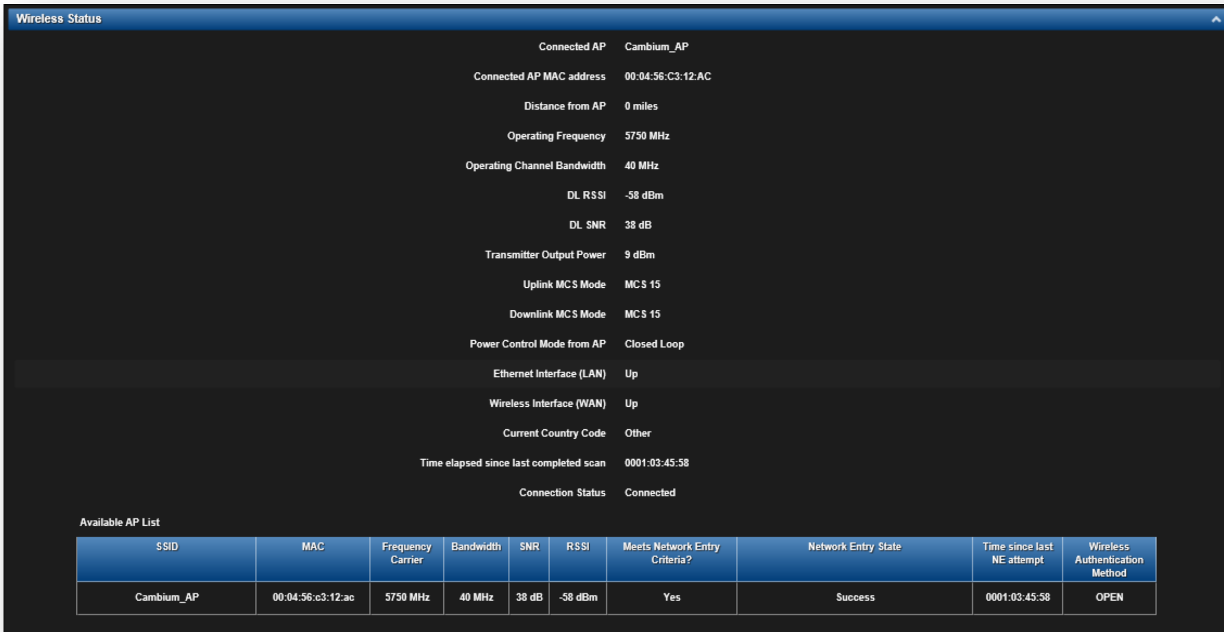


Table 71 STA Wireless Status page attributes

Attribute	Meaning
Connected AP	SSID of the AP to which the STA is registered.
Connected AP MAC address	Wireless MAC address of the AP to which the STA is registered.
Distance from AP	The distance from the AP, determined by radio signal propagation delay.
Operating Frequency	The current frequency at which the STA is transmitting and receiving.
Operating Channel Bandwidth	The current channel size at which the STA is transmitting and receiving.
DL RSSI	The Received Signal Strength Indicator, which is a measurement of the power level being received by the STA's antenna.
DL SNR	The Signal to Noise Ratio, which is an expression of the carrier signal quality with respect to signal noise.
Transmitter Output Power	The current power level at which the STA is transmitting.

Attribute	Meaning
Uplink MCS Mode	Modulation and Coding Scheme – indicates the modulation mode used for the radio uplink, based on radio conditions (MCS 1-7, 9-15).
Downlink MCS Mode	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 the AP	**Open Loop**: In this mode, the STA will not receive any power change information in the Group Poll Frame. STA calculates the UL transmit power based on path loss calculations only. **Closed Loop**: In closed loop UL power control, station will get the AP actual transmit power of beacon frame and **STA Target Received Power Level** in the beacon. Based on these two values, STA will calculate the path loss. Based on path loss and TRL values it will calculate it's transmit power such that the signal from STA arrives at AP at the configured target level. Path loss calculation will be updated by STA every time there is a change in values of AP actual TX power or TRL in the Beacon.
Ethernet Interface (LAN)	**Up**: The radio (LAN) interface is functioning properly. **Down**: The radio (LAN) interface has encountered an error and is not servicing traffic.
Wireless Interface (WAN)	**Up**: The radio (WAN) interface is functioning properly. **Down**: The radio (WAN) interface has encountered an error and is not servicing traffic.
Current Country Code	The current code the STA is operating under.
Time elapsed since last completed scan	Amount of time elapsed since the last scan was completed by the STA for available APs.
Connection Status	The current registration status of the STA.
Available AP List	The **Available AP List** may be referenced to view which APs are available for STA network entry, and also to view the status of the current AP to STA radio link.
SSID	The SSID of the visible AP.
MAC	The MAC address of the visible AP.
Frequency Carrier	The current operating frequency of the visible AP.
Bandwidth	The current operating channel bandwidth of the visible AP.
SNR	The current measured Signal-to-Noise Ratio of the STA to AP link.

Attribute	Meaning
RSSI	The current measured Received Signal Strength Indicator at the AP.
Meets Network Entry Attempt Criteria	**Yes**: The scanned AP meets the Network Entry criteria defined by the internal Network Algorithm. **No:** The scanned AP does not meet the Network Entry criteria defined by the internal Network Algorithm.
Network Entry State	The indication of the result of the STA's network entry attempt: **Successful**: STA registration is successful **Failed**: **Out of Range**: The STA is out of the AP's configured maximum range (**Max Range** parameter) **Failed**: **Capacity limit reached at AP**: The AP is no longer allowing STA network entry due to capacity reached **Failed: No Allocation on AP**: The STA to AP handshaking failed due to a misconfigured pre-shared key between the STA and AP **Failed: SW Version Incompatibility:** The version of software resident on the AP is older than the software version on the STA **Failed: PTP Mode: ACL Policy**: The AP is configured with **PTP Access** set to **MAC Limited** and the STA's MAC address is not configured in the AP's **PTP MAC Address** field **Failed: Other**: The AP does not have the required available memory to allow network entry
Time since last NE attempt	This timer indicates the last time that the STA attempted network entry to the AP.
Security Mode	This field indicates the security state of the AP to STA link.

STA Network Status page

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

Figure 47 STA Network Status page

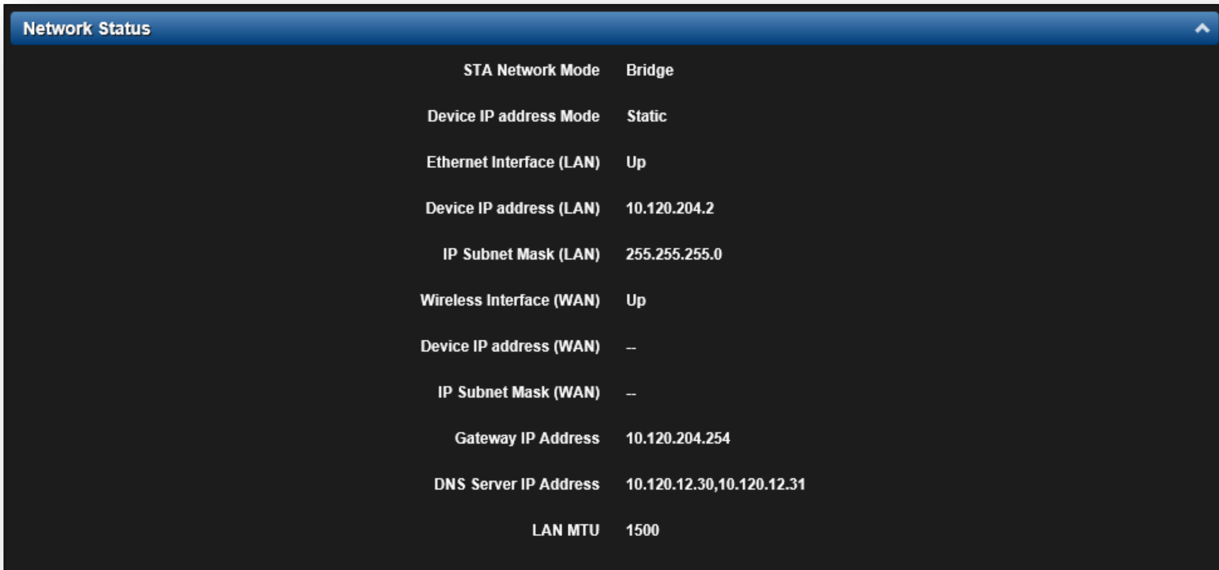


Table 72 STA Network Status page attributes

Attribute	Meaning
STA Network Mode	**Bridge:** The STA will act as a switch, and packets are forwarded or filtered based on their MAC destination address. **NAT:** The STA will act 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.
Device IP Address Mode	The current IP Address mode of the device (Static or DHCP)
Ethernet Interface (LAN)	**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.
Device IP address (LAN)	The currently configured Ethernet IP address, used for device management.
IP Subnet Mask (LAN)	The currently configured device IP subnet mask.

Attribute	Meaning
Wireless Interface (WAN)	**Up**: The device wireless interface is functioning and passing data **Down**: The device wireless interface has encountered an error disallowing full operation. Reset the device to reinitiate the wireless interface.
Device IP address (WAN)	The IP address for the wireless interface is displayed only when the STA is in NAT Mode.
IP Subnet Mask (WAN)	The subnet for the wireless interface is displayed only when the STA is in NAT Mode.
Gateway IP Address	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.
DNS Server IP Address	The IP addresses of the primary and secondary (if configured) servers used for DNS resolution.
LAN MTU	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.

STA System Log page

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

Figure 48 STA System Log page

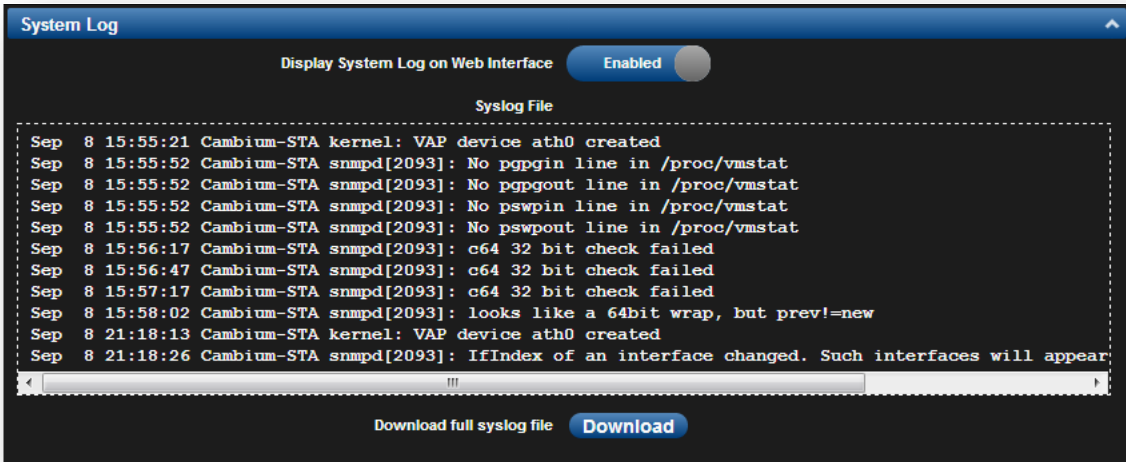


Table 73 STA System Log attributes

Attribute	Meaning
Display System Log on Web Interface	**Enabled**: The system log file is displayed on the management GUI **Disabled**: The system log file is hidden on the management GUI
Download full syslog file	Use this button to download the full system log file to a connected PC/device

STA TOOLS MENU

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

- STA Software Upgrade page on page 178
- STA Factory Default page on page 180
- STA Spectrum Analyzer page on page 181
- STA Throughput Test page on page 184
- STA Ping page on page 185
- STA Traceroute page on page 186

STA Software Upgrade page

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

Caution

Read the Release Notes associated with each software release.

Figure 49 STA Software Upgrade page

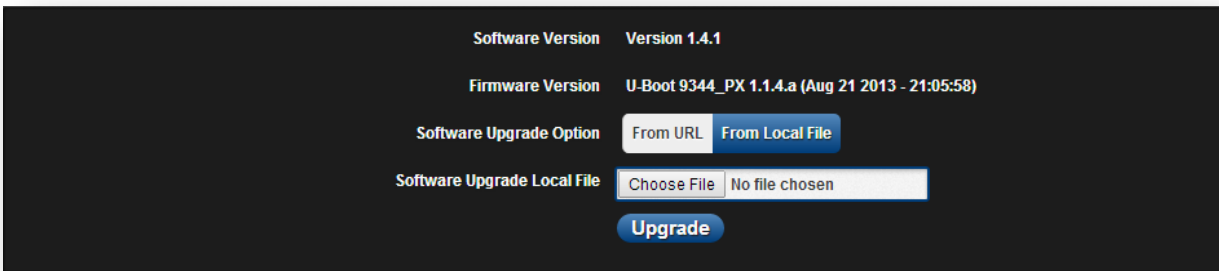


Table 74 STA Software Upgrade attributes

Attribute	Meaning
Software Version	The current operating software version.
Firmware Version	The current operating U-Boot version.
SW Upgrade Option	**From URL**: A webserver may be used to retrieve software upgrade packages (downloaded to the device via the webserver). For example, if a webserver is running at IP address 192.168.2.1 and the software upgrade packages are located in the home directory, an operator may select option **From URL** and configure the **Software Upgrade Source Info** field to **http://192.168.2.1/<software_upgrade_package>** **From Local File**: Click Browse to select the local file containing the software upgrade package
Software Upgrade Local 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:

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

STA Factory Default page

Use the STA Backup/Restore page to reset the device to its factory default configuration.

Figure 50 STA Factory Default page

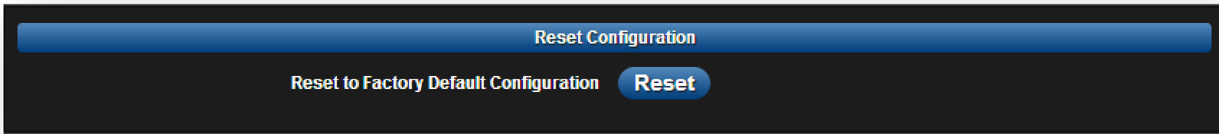


Table 75 STA Software Upgrade attributes

Attribute	Meaning
Reset to Factory Default Configuration	Use this button to reset the device to its factory default configuration Caution A reset to factory default configuration resets all device parameters. The STA ceases to transmit and any registered STAs lose their session.

STA Spectrum Analyzer page

Use the STA Spectrum Analyzer page to configure STA 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 STA to enter scan mode and the STA 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 throughout the week.

To conduct a spectrum analysis, follow these steps:

Required Software:

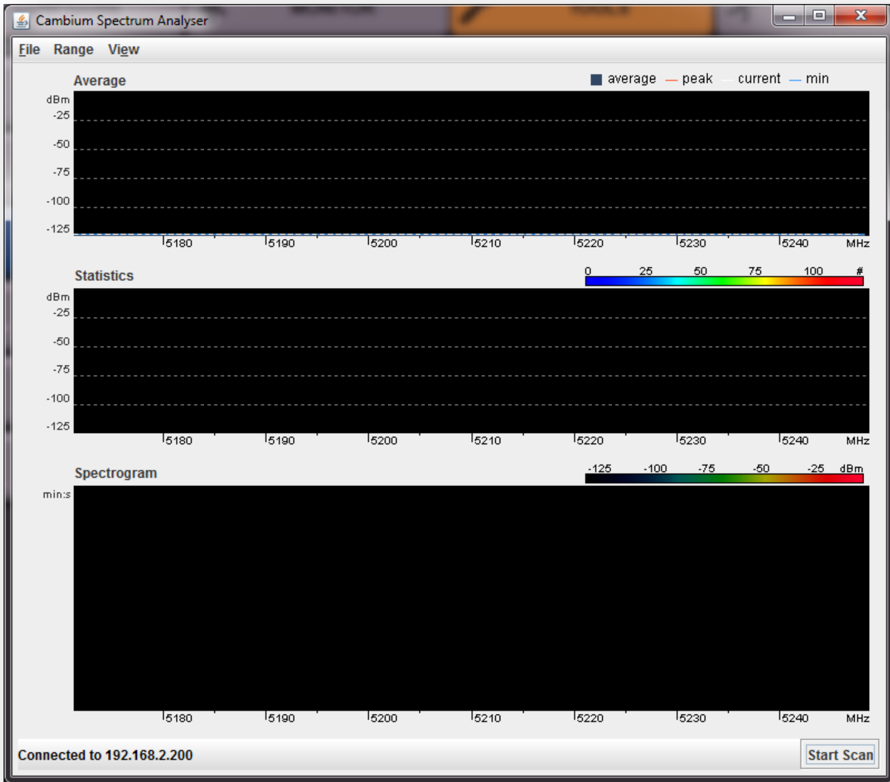
- Java Run-time Environment (JRE)

Procedure:

1. On the STA 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 STA GUI, then 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*"

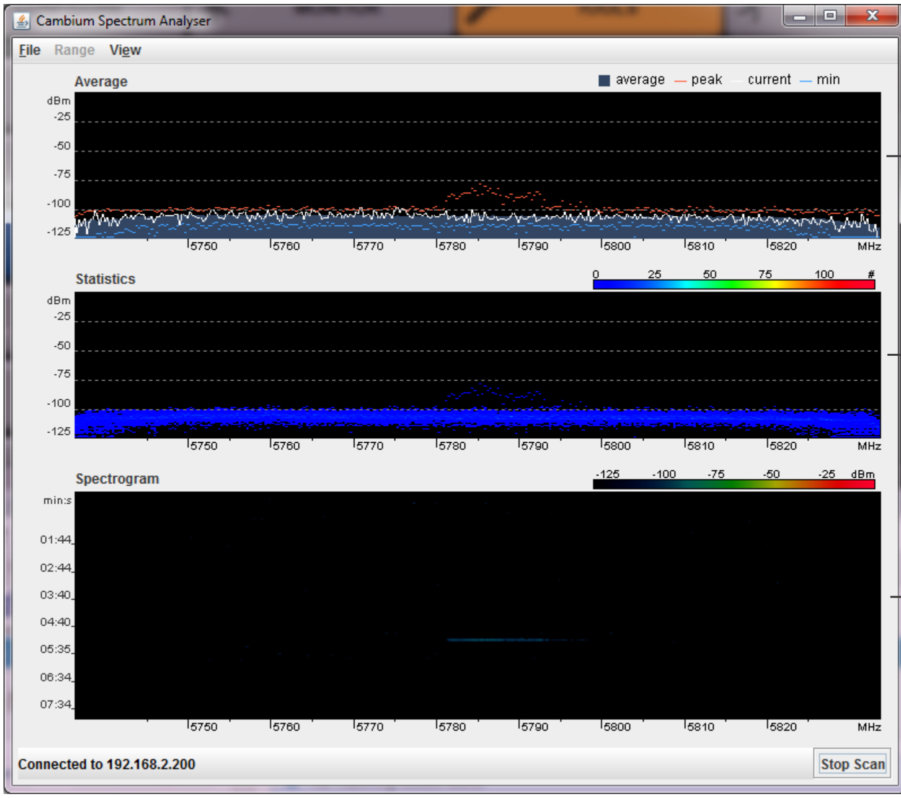
9 In the security warning window, click **Run**

The spectrum analyzer interface is displayed



10 Click **Range** to configure the range of frequencies to scan.

11 Click **Start Scan** to begin scanning



When scanning is complete, 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 STA GUI, navigate to **Configure** => **System**

4 Configure **Device Mode** to **STA**

5 Click the **Save** button

6 Click the **Reset** button

STA Throughput Test page

Use the STA Throughput Test page to conduct a simple test of STA 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 51 STA Throughput Test page

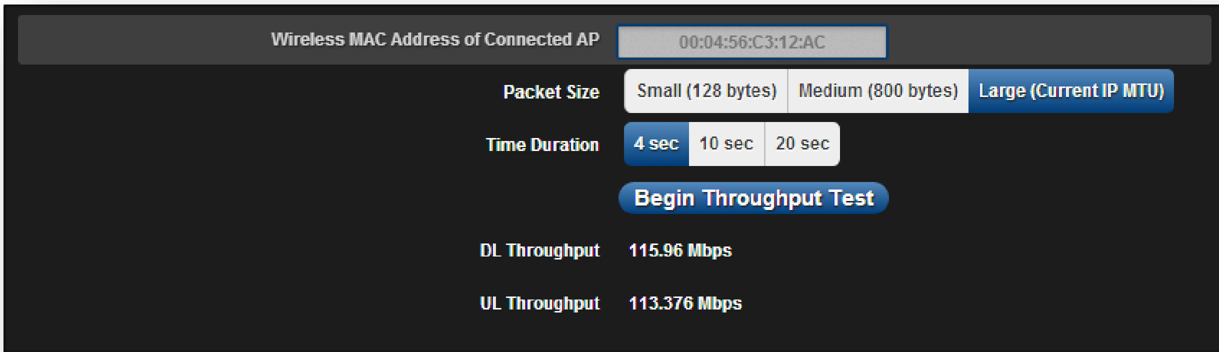


Table 76 STA Throughput Test attributes

Attribute	Meaning
Wireless MAC Address of Connected AP	This is not an editable field. It is automatically populated with the wireless MAC address of the AP to which the STA is registered.
Packet Size	Choose the Packet Size to use for the throughput test.
Time Duration	Choose the Time Duration in seconds to use for the throughput test.
DL Throughput	This field indicates the result of the throughput test on the downlink, in Mbps.
UL Throughput	This field indicates the result of the throughput test on the uplink, in Mbps.

STA Ping page

Use the STA Ping page to conduct a simple test of STA 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 STA, or there may be a failure in the network hardware (i.e. DNS server failure).

Figure 52 STA Ping page

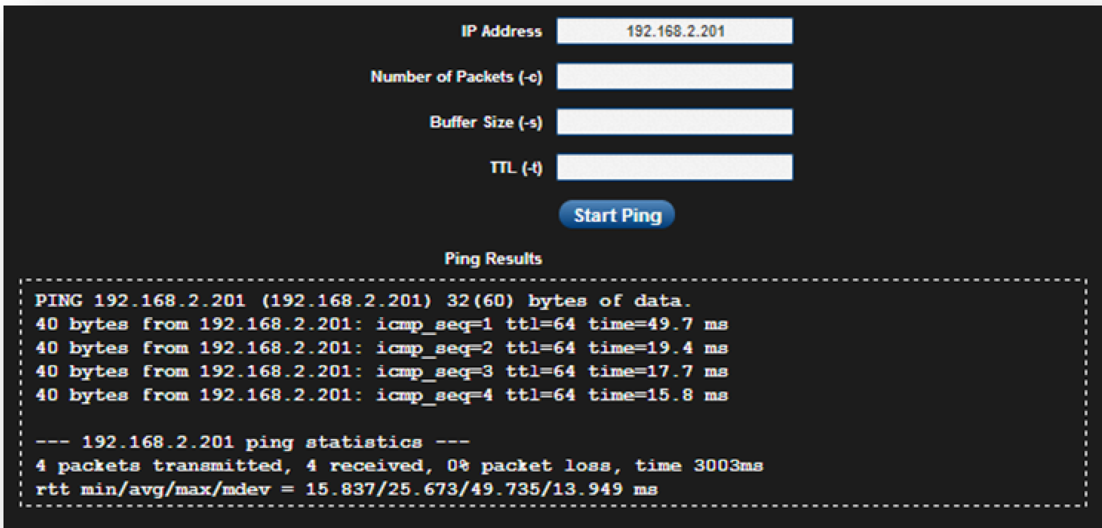


Table 77 STA Ping attributes

Attribute	Meaning
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

STA Traceroute page

Use the STA Traceroute page to display the route (path) and associated diagnostics for IP connectivity between the STA and the destination specified.

Figure 53 STA Traceroute page

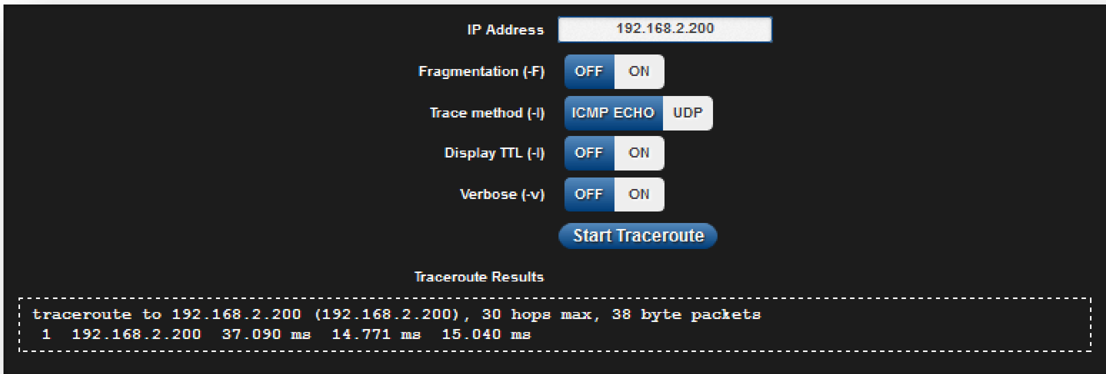


Table 78 STA Traceroute attributes

Attribute	Meaning
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 source or target)
Trace method (-I)	**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

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 3.0.0), 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

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.

To configure Free-Radius server, follow these steps:

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-station Cleartext-Password := "cambium",`

   where *cambium-station* - 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:

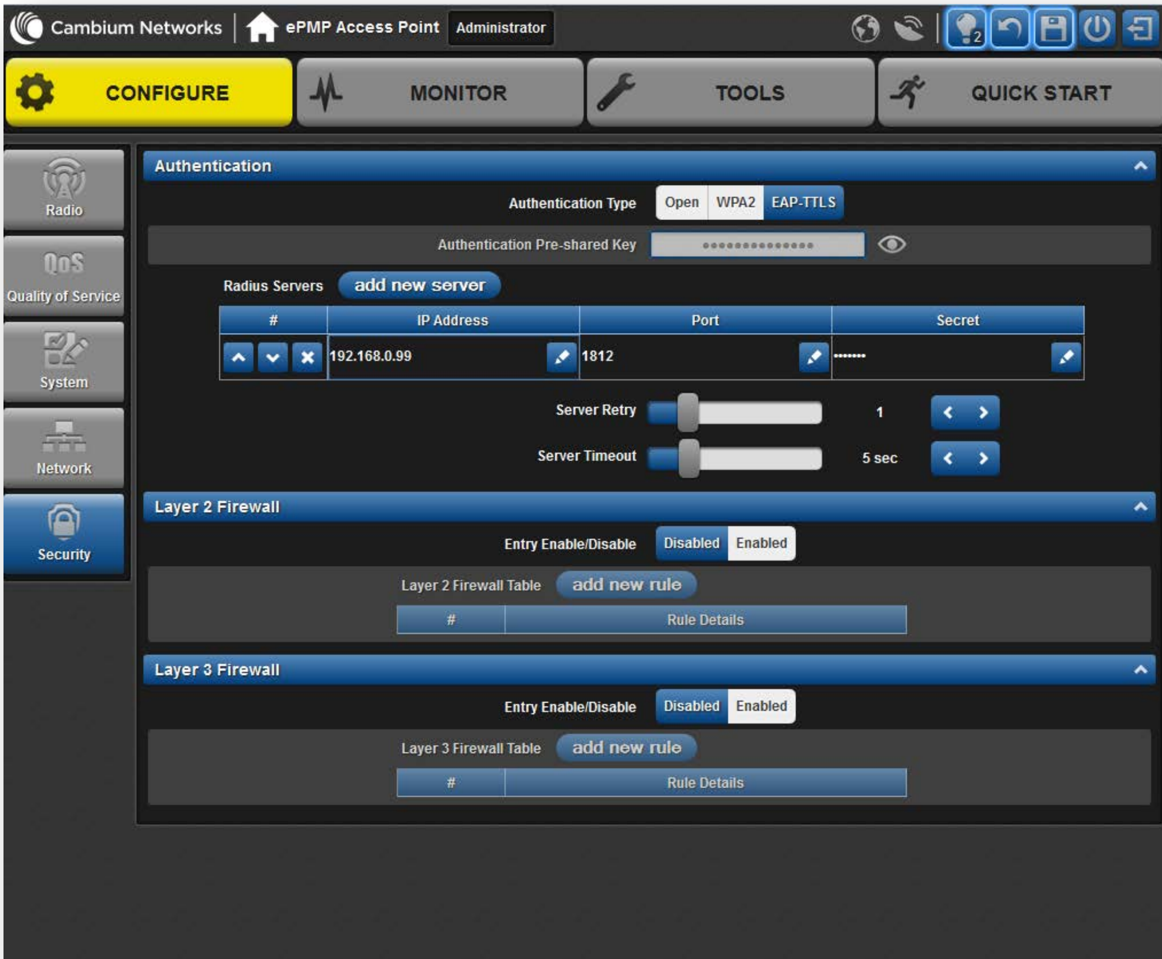
   ```
         copy_request_to_tunnel=yes
         use_tunnel_reply=yes
   ```

Note

Once these steps are performed, free-radius in debug mode can be initiated: *$ radiusd –X*.

CONFIGURING RADIUS PARAMETERS ON AP

Figure 54 AP Radius configuration

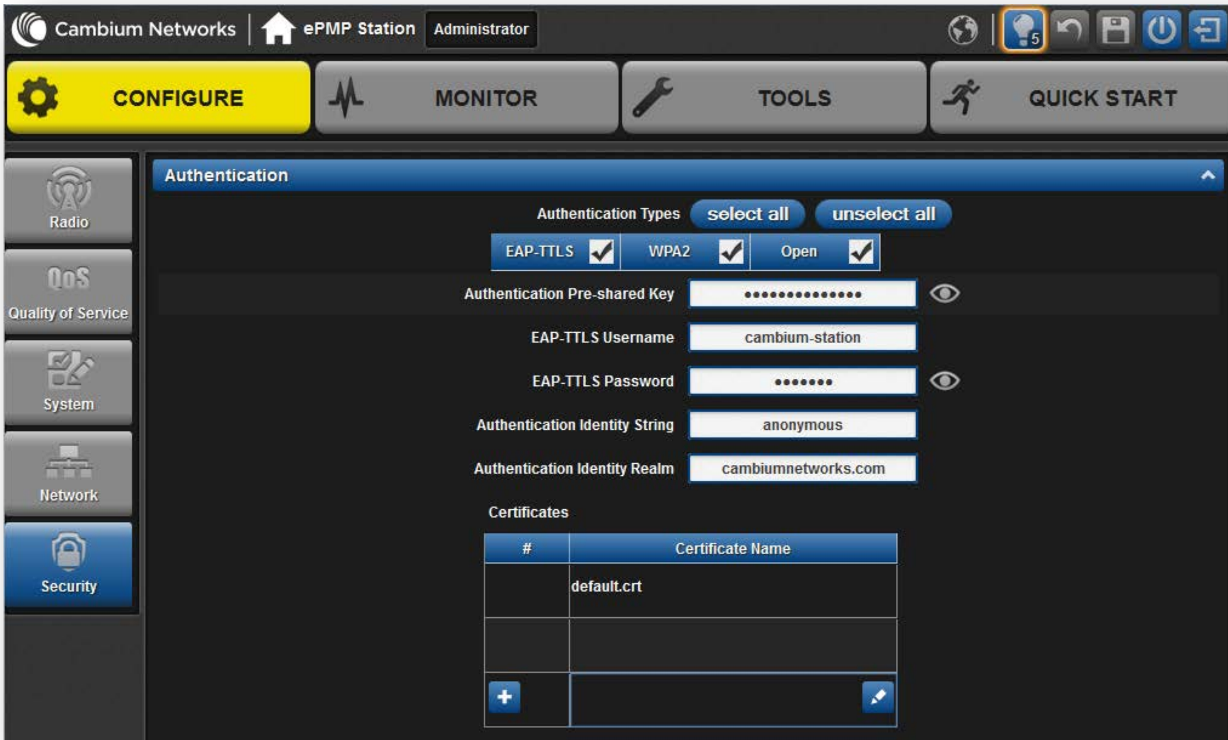


To configure Radius parameters on AP, follow these steps:

1. Open the GUI and login as *admin.*
2. Navigate to ***Configure*** -> ***Security*** -> ***Authentication.***
3. Change ***Authentication Type*** value to *EAP-TTLS.*
4. Add 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 STA

Figure 55 STA Radius configuration



To configure Radius parameters on STA, follow these steps:

1. Select ***EAP-TTLS*** Authentication Type.
2. Configure *EAP-TTLS Username* and *EAP-TTLS Password,* as configured in file **users***.*
3. Add *Certificates to* the **Certificates** table.
4. Click ***Save***, to keep the changes.

CONFIGURING MIR PROFILES

To configure the MIR profiles, follow these steps:

- Create a dictionary file with the MIR Profiles:

  # touch dictionary.cambium

- Edit *dictionary.cambium* according to the instructions that you can find under */usr/local/etc/raddb* directory in file ***dictionary***.

  For example:

```
 ATTRIBUTE   Cambium-Canopy-ULMB 110 integer    #Max Burst Uplink Rate
ATTRIBUTE   Cambium-Canopy-DLMB 110  integer    #Max Burst Downlink Rate

VENDOR                               Cambium                     17713

#
# Cambium vendor-specific attributes.
#

BEGIN-VENDOR                         Cambium

ATTRIBUTE   Cambium-Canopy-VLIGVID 21 integer    #VLAN Ingress VLAN ID
ATTRIBUTE   Cambium-Canopy-VLMGVID 22 integer    #VLAN Management VLAN ID
ATTRIBUTE   Cambium-Canopy-ULMB    26 integer    #Max Burst Uplink Rate
ATTRIBUTE   Cambium-Canopy-DLMB    27 integer    #Max Burst Downlink Rate
```

- Create link on your dictionary:

  #ln -s dictionary.cambium dictionary.local

- To configure MIR profiles, edit *usr/local/etc/raddb/users* and add profiles for each client below users configuration :

```
station33 Cleartext-Password := "cambium33"
Cambium-Canopy-ULMB = 100,
Cambium-Canopy-DLMB = 100

station34 Cleartext-Password := "cambium34"
        Cambium-Canopy-ULMB = 110,
        Cambium-Canopy-DLMB = 110

station35 Cleartext-Password := "cambium35"
        Cambium-Canopy-ULMB = 120,
        Cambium-Canopy-DLMB = 120
```

A few example scenarios of MIR and RADIUS configurations are described in Table 79.

Table 79 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 STAs. Configure the MIR profiles in the **Configure** => **Quality of Service** menu option on the AP GUI and apply the corresponding profile # in the STA under the same menu option on STA.
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 STA being managed by the Radius Server. In this case, create the MIR profile with Station usernames and password on the Radius server. At the time of registration, the AP will use the radius information and apply the corresponding profile to the STA. 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 STAs across multiple APs can then be managed via Radius.
Hybrid control using both Radius and MIR profile on the AP GUI	The system will also support a hybrid mode where Radius and the GUI QOS profiles can be used simultaneously as long as the same STA does not have a profile # associated from the AP & Radius. In case where it is redundant, Radius server setting will override the MIR profile settings from the GUI.

CREATING CERTIFICATE FOR RADIUS SERVER AND STA 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. File name 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). Content key, can 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

Generate a self-signed certificate CA:

```
openssl req-new-x509-days 3650 -key cambium-ca.key-out cambium-ca.crt
```

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 '.', 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)

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: 0D: 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: 0D: 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
```

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 in it:

```
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)

Create a server certificate (option cerver_cert), file name (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.
```

Then you must specify the fields you want, like for the root certificate. Default values have already crammed in square brackets. To use them simply click ENTER.

1. Your Country Name (2 letter country code):
2. State or Province Name (full name):
3. Locality Name (Ex.- city)
4. Organization Name (Ex.- Cambium Networks):
5. Organizational Unit Name (Ex.- Cambium):
6. Common Name (Ex.- radius.cambium.com):
7. 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
```

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.

Operation and Troubleshooting

This chapter provides instructions for operators of ePMP networks. The following topics are described in this chapter:

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 STA
    - 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. What is the history of the problem?
   - Have we changed something recently?
   - Have we seen other symptoms before this?
2. How wide-spread is the symptom?
   - Is the problem on only a single STA? (If so, focus on that STA.)
   - Is the problem on multiple STAs? If so
     - is the problem on one AP in the cluster? (If so, focus on that AP)
     - is the problem on multiple, but not all, APs in the cluster? (If so, focus on those APs)
     - is the problem on all APs in the cluster? (If so, focus on the CMM and the GPS signal.)
3. Based on data in the System Log
   - 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).
   - 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

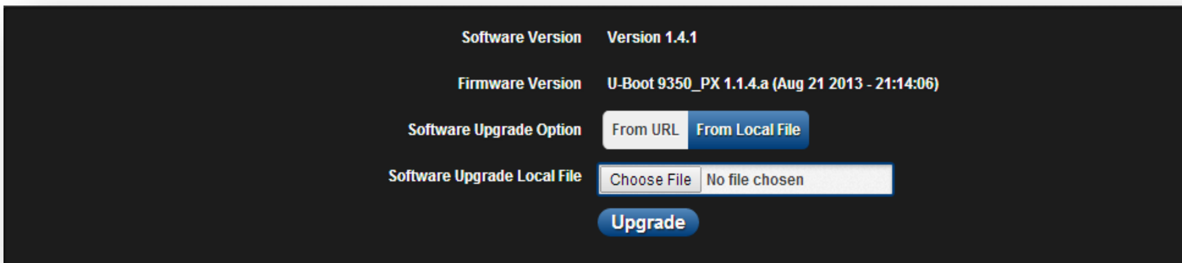
To upgrade the device software (AP or STA), follow this:

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 Set **SW Upgrade Option** to **From URL** to pull the software file from a network software server, or select **From Local File** to upload a file from the accessing device.

5 If **From URL** is selected, enter the server IP address, server port, and file path. If **From 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.

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 STA to equipment inside the building, are of the supported type, as defined in Ethernet cabling on page 57

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 on page 201
- Ethernet LED is off on page 201

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/STA 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/STA and power supply.

Action: The fault may be in the LAN or AP/STA 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/STA 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/STA

Log into the AP or STA 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 on page 202.

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/STA 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/STA. 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 STA under test:

Procedure:

1 Ensure that the IP address of the computer is configured appropriately for connection to the AP or STA 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 will need to be disconnected from the network in order 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 STA 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/STA under test.

6 Record how many Ping packets have been 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 STA.

MODULE HAS LOST OR DOES NOT ESTABLISH RADIO CONNECTIVITY

If there is no wireless activity, follow this:

Procedure:

1. Check that the AP and STAs are configured with the same **Frequency Carrier**. Also, if operating in a region where DFS is required, ensure that the STA'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 at the STA
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 STA 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 STA. if **Authentication Type** is set to **WPA2**, verify that the **Pre-shared Key** matches between the AP and the STA **Preferred AP List**
6. Check that the software at each end of the link is the same version.
7. Check that the desired AP's SSID is configured in the STA **Preferred AP List**.
8. On the STA, check the **DL RSSI** and **DL CINR** values. Verify that for the STA installed distance, that the values are consistent with Table 80 5 GHz threshold, power and link loss on page 260 and Table 81 2.4 GHz threshold, power and link loss on page 260.
9. Check Tx Power on the AP and STA
10. Check that the link is not obstructed or the AP/STA 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/STA 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 an STA are proper based on the distance of the link – see **Table 80 5 GHz threshold, power and link loss** on page **260** and **Table 81 2.4 GHz threshold, power and link loss** on page **260.**
3. Check that the path loss is low enough for the communication rates required.
4. Check that the AP or STA 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 STAs feature an external button which serves two purposes:

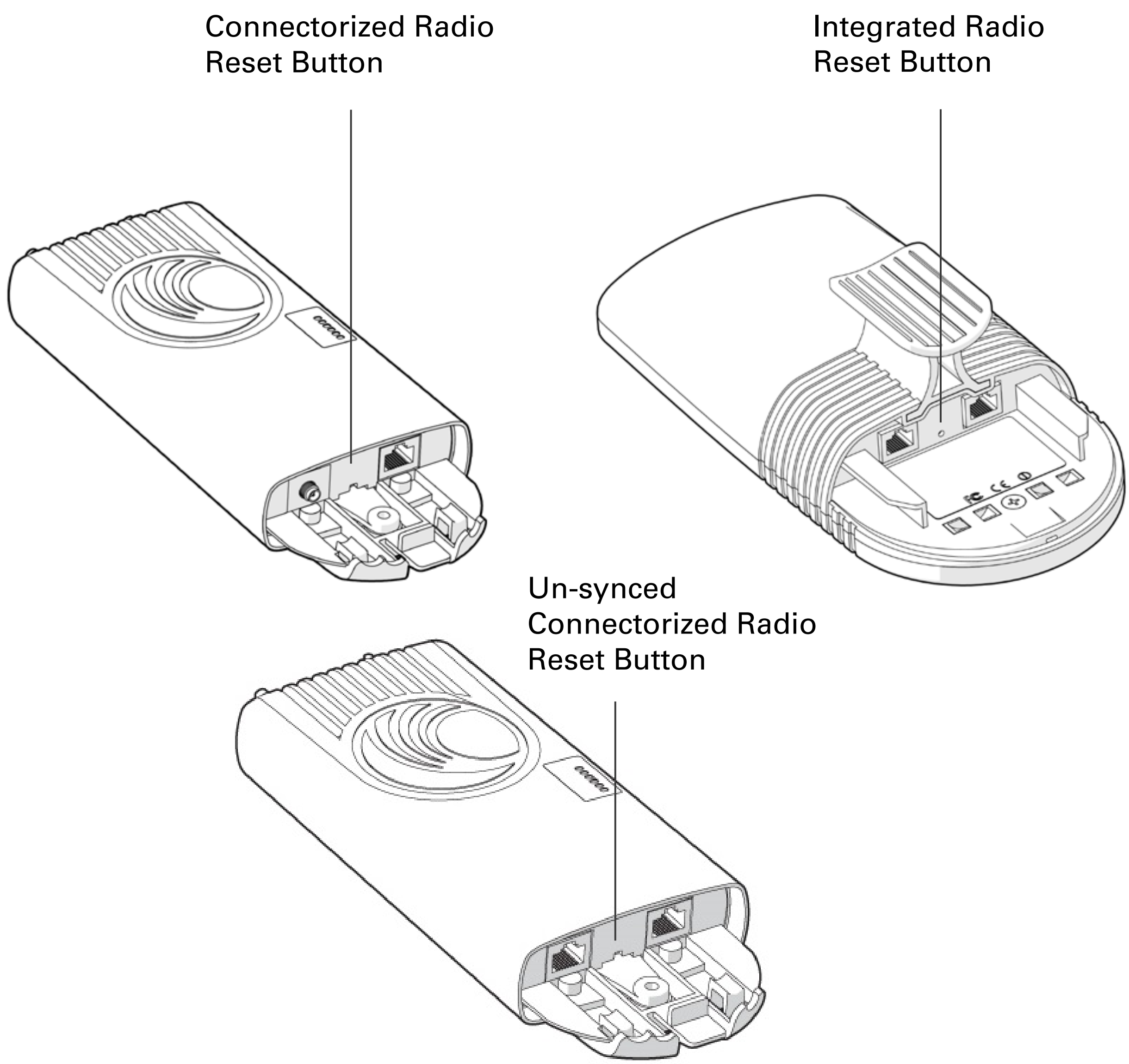
- To reset the device (briefly depress the button for more than two seconds but less than ten seconds then release)

⚠ 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)



Resetting the AP or STA to factory defaults by power cycling

Operators may reset an AP or STA to default factory configuration by a sequence of power cycling (removing power to the device. This procedure allows operators to perform a factory default reset without a tower climb or additional tools.

Procedure:

1. Remove the AP or STA's Ethernet cable from the power supply, then reconnect the Ethernet cable to re-supply power to the AP or STA device (1st power cycle)
2. Remove the AP or STA's Ethernet cable from the power supply, then reconnect the Ethernet cable to re-supply power to the AP or STA device (2nd power cycle)
3. Remove the AP or STA's Ethernet cable from the power supply, then reconnect the Ethernet cable to re-supply power to the AP or STA device (3rd power cycle)
4. Remove the AP or STA's Ethernet cable from the power supply, then reconnect the Ethernet cable to re-supply power to the AP or STA device (4th power cycle)
5. Remove the AP or STA's Ethernet cable from the power supply, then reconnect the Ethernet cable to re-supply power to the AP or STA device (5th power cycle) to bring it all the way up. The AP or STA will now come up with the factory default settings.

Note

Steps 1 through 4 above will have to be done within 10 seconds to reset the radio to its factory default settings. This is to reduce the risk of the radio resetting to factory default settings during normal, repeated power outages.

Legal and reference information

This chapter provides legal notices including software license agreements.

Caution

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

The following topics are described in this chapter:

- Cambium Networks end user license agreement on page 209
- Hardware warranty on page 258
- Limit of liability on page 259
- Compliance with safety standards on page 261 lists the safety specifications against which the ePMP has been tested and certified. It also describes how to keep RF exposure within safe limits.
- Compliance with radio regulations on page 264 describes how the ePMP complies with the radio regulations that are enforced in various countries.
- Notifications on page 278 contain notes made to regulatory bodies for the ePMP.
- Data throughput tables on page 287 contain tables and graphs to support calculation of the data rate capacity that can be provided by ePMP configurations.

Cambium Networks end user license agreement

ACCEPTANCE OF THIS AGREEMENT

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

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

DEFINITIONS

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

GRANT OF LICENSE

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

CONDITIONS OF USE

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

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

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

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

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

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

TITLE AND RESTRICTIONS

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

CONFIDENTIALITY

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

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

RIGHT TO USE CAMBIUM'S NAME

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

TRANSFER

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

UPDATES

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

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

MAINTENANCE

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

DISCLAIMER

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

LIMITATION OF LIABILITY

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

U.S. GOVERNMENT

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

TERM OF LICENSE

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

GOVERNING LAW

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

ASSIGNMENT

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

SURVIVAL OF PROVISIONS

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

ENTIRE AGREEMENT

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

THIRD PARTY SOFTWARE

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

Aquila	Copyright (c) 2002-2010, Atheros Communications Inc. Copyright (c) 2002-2005 Sam Leffler, Errno Consulting Copyright (C) 2011 Denali Software Inc. All rights reserved Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES

WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

===

Redistribution and use in source and binary forms are permitted
provided that the following conditions are met:
1. The materials contained herein are unmodified and are used unmodified.
2. Redistributions of source code must retain the above copyright notice, this list of conditions and the following NO ''WARRANTY'' disclaimer below (''Disclaimer''), without modification.
3. Redistributions in binary form must reproduce at minimum a disclaimer similar to the Disclaimer below and any redistribution must be conditioned upon including a substantially similar Disclaimer requirement for further binary redistribution.
4. Neither the names of the above-listed copyright holders nor the names of any contributors may be used to endorse or promote product derived from this software without specific prior written permission.

NO WARRANTY
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NONINFRINGEMENT,MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY

	OF SUCH DAMAGES.
Linux Kernel	Copyright (c) 1989, 1991 Free Software Foundation NOTE! This copyright does *not* cover user programs that use kernel services by normal system calls - this is merely considered normal use of the kernel, and does *not* fall under the heading of "derived work". Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the Linux kernel) is copyrighted by me and others who actually wrote it. Also note that the only valid version of the GPL as far as the kernel is concerned is _this_ particular version of the license (ie v2, not v2.2 or v3.x or whatever), unless explicitly otherwise stated. Linus Torvalds -- GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
gpio_keys	/* * Driver for keys on GPIO lines capable of generating interrupts. * * Copyright 2005 Phil Blundell * * This program is free software; you can redistribute it and/or modify * it under the terms of the GNU General Public License version 2 as * published by the Free Software Foundation. */
OpenWrt	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

	Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
uboot	Copyright (c) 2007 Wolfgan Denk, DENIX Software Engeneering, wd@denix.de # (C) Copyright 2000 - 2005 # Wolfgang Denk, DENX Software Engineering, wd@denx.de. # # See file CREDITS for list of people who contributed to this # project. # # This program is free software; you can redistribute it and/or # modify it under the terms of the GNU General Public License as # published by the Free Software Foundation; either version 2 of # the License, or (at your option) any later version. # # This program is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # # You should have received a copy of the GNU General Public License # along with this program; if not, write to the Free Software # Foundation, Inc., 59 Temple Place, Suite 330, Boston, # MA 02111-1307 USA See full license text on page 223.
jQuery	The MIT License (MIT) Copyright (c) 2013 The jQuery Foundation. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES

	OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
Data-Driven Document	Copyright (c) 2012, Michael Bostock Copyright (c) 2013, Michael Bostock All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. * The name Michael Bostock may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MICHAEL BOSTOCK BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

AjaxFileUpload	The MIT License (MIT) Copyright 2013-2014 powered by PHPLETTER Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jquery.caret	The MIT License (MIT) Copyright (c) 2010 C. F., Wong Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
jquery.cookie	Copyright 2013 Klaus Hartl Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

json2.js	http://www.JSON.org/json2.js 2010-08-25 Public Domain. NO WARRANTY EXPRESSED OR IMPLIED. USE AT YOUR OWN RISK. See http://www.JSON.org/js.html This code must be minified before deployment. See http://javascript.crockford.com/jsmin.html USE YOUR OWN COPY. IT IS EXTREMELY UNWISE TO LOAD CODE FROM SERVERS YOU DO NOT CONTROL.
jquery.noty	Copyright (c) 2012 Nedim Arabacı Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SlickGrid	Copyright (c) 2009-2012 Michael Leibman Copyright (c) 2010 Michael Leibman http://github.com/mleibman/slickgrid Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

jquery.event.drag	The MIT License (MIT) Copyright (c) 2010 Three Dub Media Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
IE9.js	The MIT License (MIT) Copyright (c) 2004-2010, Dean Edwards Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

busybox

--- A note on GPL versions

BusyBox is distributed under version 2 of the General Public License (included in its entirety, below). Version 2 is the only version of this license which this version of BusyBox (or modified versions derived from this one) may be distributed under.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> **b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> **c)** Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software

	Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally. **NO WARRANTY** **11.** BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. **12.** IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS
dnsmasq	# This program is free software; you can redistribute it and/or modify # it under the terms of the GNU General Public License as published by # the Free Software Foundation; version 2 dated June, 1991, or # (at your option) version 3 dated 29 June, 2007. See full license text on page 223.
dropbear	Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved
"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c
loginrec.h
atomicio.h
atomicio.c
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

ebtables	Copyright (C) 1999 Paul `Rusty' Russell & Michael J. Neuling Copyright (C) 2001-2002 Bart De Schuymer All code in this package, including the code from the extensions, is released under the GPL license, which you find hereafter. GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
eventlog	Copyright (c) 2003 BalaBit IT Ltd. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of BalaBit nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY BALABIT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

firewall	# Copyright (C) 2009-2010 OpenWrt.org
glib2	Copyright (C) 2007-2011 OpenWrt.org Copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Free Software Foundation, Inc. Copyright © 2004 Scott James Remnant <scott@netsplit.com>. Copyright (c) 1997-2006 University of Cambridge. Copyright © 2009 Codethink Limited Copyright (C) 2008-2010 Red Hat, Inc. Copyright (C) 2008 Hans Breuer Copyright (C) 2008, 2010 Collabora, Ltd. GNU LIBRARY GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.] See full license text on page 223.
hostapd	Copyright (c) 2002-2011, Jouni Malinen <j@w1.fi> and contributors All Rights Reserved. These programs are dual-licensed under both the GPL version 2 and BSD license (the one with advertisement clause removed). Either license may be used at your option. This package may include either wpa_supplicant, hostapd, or both. See README file respective subdirectories (wpa_supplicant/README or hostapd/README) for more details. See full license text on page 223.
hotplug	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 See full license text on page 223.
iperf	Copyright 1999, 2000, 2001, 2002, 2003, 2004 The Board of Trustees of the University of Illinois All rights reserved

	Permission is hereby granted, free of charge, to any person obtaining a copy of this software (Iperf) and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimers. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution. Neither the names of the University of Illinois, NCSA, nor the names of its contributors may be used to endorse or promote products derived from this Software without specific prior written permission. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE CONTIBUTORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
iproute2	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
iptables	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
iputils	/* * Copyright (c) 1989 The Regents of the University of California.

	* All rights reserved. * * This code is derived from software contributed to Berkeley by * Mike Muuss. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in the * documentation and/or other materials provided with the distribution. * 3. All advertising materials mentioning features or use of this software * must display the following acknowledgement: * This product includes software developed by the University of * California, Berkeley and its contributors. * 4. Neither the name of the University nor the names of its contributors * may be used to endorse or promote products derived from this software * without specific prior written permission. * * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. */
Button-hotplug	Copyright (C) 2008 Gabor Juhos <juhosg@openwrt.org> Based on the diag.c - GPIO interface driver for Broadcom boards Copyright (C) 2006 Mike Baker <mbm@openwrt.org>, Copyright (C) 2006-2007 Felix Fietkau <nbd@openwrt.org> Copyright (C) 2008 Andy Boyett <agb@openwrt.org> GPL v2 See full license text on page 223.

libdbi	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.] See full license text on page **223**.
libiconv	# Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, # 2005 Free Software Foundation, Inc. /* Copyright (C) 1992,1995-1999,2000-2002,2005-2006 Free Software Foundation, Inc. This file is part of the GNU C Library. /* Copyright (C) 1999-2001, 2003 Bruno Haible. This file is not part of the GNU LIBICONV Library. This file is put into the public domain. */ /* * Copyright (C) 1999-2001, 2005 Free Software Foundation, Inc. * This file is part of the GNU LIBICONV Library. * * The GNU LIBICONV Library is free software; you can redistribute it * and/or modify it under the terms of the GNU Library General Public * License as published by the Free Software Foundation; either version 2 * of the License, or (at your option) any later version. * * The GNU LIBICONV Library is distributed in the hope that it will be * useful, but WITHOUT ANY WARRANTY; without even the implied warranty of * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU * Library General Public License for more details. */ /* Copyright (C) 1999-2004, 2006 Free Software Foundation, Inc. This file is part of the GNU LIBICONV Tools. This program is free software; you can redistribute it and/or modify

```
SOFTWARE.
#
# Except as contained in this notice, the name of the X Consortium shall not
# be used in advertising or otherwise to promote the sale, use or other deal-
# ings in this Software without prior written authorization from the X Consor-
# tium.
#
#
# FSF changes to this file are in the public domain.
#
# Calling this script install-sh is preferred over install.sh, to prevent
# `make' implicit rules from creating a file called install from it
# when there is no Makefile.
#
# This script is compatible with the BSD install script, but was written
# from scratch.  It can only install one file at a time, a restriction
# shared with many OS's install programs.
```

See full license text on page 223.

libiwinfo


```
/*
 * iwinfo - Wireless Information Library - Command line frontend
 *
 *   Copyright (C) 2011 Jo-Philipp Wich <xm@subsignal.org>
 *
 * The iwinfo library is free software: you can redistribute it and/or
 * modify it under the terms of the GNU General Public License version 2
 * as published by the Free Software Foundation.
 *
 * The iwinfo library is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

	* See the GNU General Public License for more details. * * You should have received a copy of the GNU General Public License along * with the iwinfo library. If not, see http://www.gnu.org/licenses/. */ See full license text on page 223.
Libnl-tiny	LGPLv2.1 /* * lib/attr.c Netlink Attributes * * This library is free software; you can redistribute it and/or * modify it under the terms of the GNU Lesser General Public * License as published by the Free Software Foundation version 2.1 * of the License. * * Copyright (c) 2003-2008 Thomas Graf <tgraf@suug.ch> */ See full license text on page 223.
libpcap	Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy) Copyright (c) 2005 - 2008 CACE Technologies, Davis (California) Copyright (c) 1997 Yen Yen Lim and North Dakota State University Copyright (c) 1995-1999 Kungliga Tekniska Högskolan Copyright (c) 1982, 1986, 1988 - 1998, 2000 The Regents of the University of California Copyright (c) 2000 Torsten Landschoff <torsten@debian.org>, Sebastian Krahmer <krahmer@cs.uni-potsdam.de> Copyright (c) 2006 Paolo Abeni (Italy) Copyright (c) 2007 Fulko Hew, SITA INC Canada, Inc <fulko.hew@sita.aero> Copyright (c) 2001 Atsushi Onoe Copyright (c) 2002-2005 Sam Leffler, Errno Consulting Copyright 1989 by Carnegie Mellon Copyright (c) 1996 Juniper Networks, Inc. Copyright (c) 1993,1994 Texas A&M University. Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project. Portions Copyright (c) 1993 by Digital Equipment Corporation. Copyright (C) 1999 WIDE Project. Copyright (c) 2005 - 2006 CACE Technologies, Davis (California) (Ref: libpcap-1.0.0/LICENSE) License: BSD

	Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
libtool	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page **223**.

lua	Lua License ----------- Lua is licensed under the terms of the MIT license reproduced below. This means that Lua is free software and can be used for both academic and commercial purposes at absolutely no cost. For details and rationale, see http://www.lua.org/license.html . == ================= Copyright (C) 1994-2008 Lua.org, PUC-Rio. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LuCi

mtd

See full license text on page 223.

ncurses	Copyright (c) 1998-2004,2006 Free Software Foundation, Inc. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.
Net-snmp	Copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California Networks Associates Technology, Inc copyright notice (BSD) Copyright (c) 2001-2003, Networks Associates Technology, Inc Cambridge Broadband Ltd. copyright notice (BSD) Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. Copyright (c) 2003-2008, Sparta, Inc Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003 oss@fabasoft.com Author: Bernhard Penz <bernhard.penz@fabasoft.com> BSD like: Permission to use, copy, modify and distribute this software and its

	EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
openssh	# # Copyright (C) 2006, 2008-2011 OpenWrt.org # # This is free software, licensed under the GNU General Public License v2. # # See full license text on page 223.
openssl	LICENSE ISSUES ============== The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org. OpenSSL License --------------- /* == ====== * Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that the following conditions * are met: * * 1. Redistributions of source code must retain the above copyright * notice, this list of conditions and the following disclaimer. * * 2. Redistributions in binary form must reproduce the above copyright * notice, this list of conditions and the following disclaimer in * the documentation and/or other materials provided with the * distribution. * * 3. All advertising materials mentioning features or use of this * software must display the following acknowledgment: * "This product includes software developed by the OpenSSL Project * for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*   endorse or promote products derived from this software without
*   prior written permission. For written permission, please contact
*   openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
*
==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
----

*
* This package is an SSL implementation written

```
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an
acknowledgement:
 *    "This product includes software written by Tim Hudson
(tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
```

	WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. * * The licence and distribution terms for any publically available version or * derivative of this code cannot be changed. i.e. this code cannot simply be * copied and put under another distribution licence * [including the GNU Public Licence.] */
opkg	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
pcre	Copyright (c) 1997-2010 University of Cambridge Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself. THE MAIN PCRE LIBRARY --------------------- Written by: Philip Hazel Email local part: ph10 Email domain: cam.ac.uk University of Cambridge Computing Service, Cambridge, England. Copyright (c) 1997-2010 University of Cambridge All rights reserved THE C++ WRAPPER LIBRARY ----------------------- Written by: Google Inc. Copyright (c) 2007-2010 Google Inc All rights reserved

procps	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.
px5g	Copyright (C) 2009 Steven Barth <steven@midlink.org> Copyright (C) 2009 Paul Bakker <polarssl_maintainer at polarssl dot org> Copyright (C) 2006-2007 Pascal Vizeli <pvizeli@yahoo.de> This library is free software; you can redistribute it and/or Modify it under the terms of the GNU Lesser General Public License, version 2.1 as published by the Free Software Foundation. This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details. See full license text on page 223.
swconfig	Copyright (C) 2008-2009 Felix Fietkau <nbd@openwrt.org> Copyright (C) 2010 Martin Mares <mj@ucw.cz> # # Copyright (C) 2008-2010 OpenWrt.org # # This is free software, licensed under the GNU General Public License v2. # See /LICENSE for more information. # See full license text on page 223.
Syslog-ng	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 See full license text on page 223.
tcp_wrappers	Copyright 1995 by Wietse Venema. All rights reserved. Some individual files may be covered by other copyrights. Copyright (c) 1987 Regents of the University of California. All rights reserved. /** *******

	* Copyright 1995 by Wietse Venema. All rights reserved. Some individual * files may be covered by other copyrights. * * This material was originally written and compiled by Wietse Venema at * Eindhoven University of Technology, The Netherlands, in 1990, 1991, * 1992, 1993, 1994 and 1995. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that this entire copyright notice * is duplicated in all such copies. * * This software is provided "as is" and without any expressed or implied * warranties, including, without limitation, the implied warranties of * merchantibility and fitness for any particular purpose. *** ******/
tcpdump	Copyright (c) 2001 Seth Webster <swebster@sst.ll.mit.edu> Copyright (C) Andrew Tridgell 1995-1999 Copyright (c) 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 2000 The Regents of the University of California. All rights reserved. License: BSD Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

uClibc++	LGPL v2.1 GPL v2 See full license text on page 223.
Uboot-envtools	# # (C) Copyright 2002-2006 # Wolfgang Denk, DENX Software Engineering, wd@denx.de. # # See file CREDITS for list of people who contributed to this # project. # # This program is free software; you can redistribute it and/or # modify it under the terms of the GNU General Public License as # published by the Free Software Foundation; either version 2 of # the License, or (at your option) any later version. # # This program is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # # You should have received a copy of the GNU General Public License # along with this program; if not, write to the Free Software # Foundation, Inc., 59 Temple Place, Suite 330, Boston, # MA 02111-1307 USA # See full license text on page 223.

PPPd and PPPoE	Copyright to Michal Ostrowski for PPPoE and Paul Mackerras paulus@samba.org PPPoE The PPPoE plugin included in this package is a component of the Roaring Penguin PPPoE package, included in this package courtesy of Roaring Penguin Software. (http://www.roaringpenguin.com). PPPd Copyrights: *********** All of the code can be freely used and redistributed. The individual source files each have their own copyright and permission notice. Pppd, pppstats and pppdump are under BSD-style notices. Some of the pppd plugins are GPL'd. Chat is public domain. Distribution: ************* The primary site for releases of this software is: ftp://ftp.samba.org/pub/ppp/ ($Id: README,v 1.37 2006/05/29 23:51:29 paulus Exp $) James Carlson <carlson@workingcode.com> for PPPd See full license text on page **223.**

uci	Copyright (C) 2008-2010 OpenWrt.org Copyright (C) 2008 Felix Fietkau nbd@openwrt.org Copyright (C) 2006 Fokus Fraunhofer <carsten.tittel@fokus.fraunhofer.de /* * libuci - Library for the Unified Configuration Interface * Copyright (C) 2008 Felix Fietkau <nbd@openwrt.org> * * This program is free software; you can redistribute it and/or modify * it under the terms of the GNU Lesser General Public License version 2.1 * as published by the Free Software Foundation * * This program is distributed in the hope that it will be useful, * but WITHOUT ANY WARRANTY; without even the implied warranty of * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the * GNU General Public License for more details. */ /* * ucimap-example - sample code for the ucimap library * Copyright (C) 2008-2009 Felix Fietkau <nbd@openwrt.org> * * This program is free software; you can redistribute it and/or modify * it under the terms of the GNU General Public License version 2 * as published by the Free Software Foundation * * This program is distributed in the hope that it will be useful, * but WITHOUT ANY WARRANTY; without even the implied warranty of * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the * GNU General Public License for more details. */ See full license text on page **223**.

udevtigger

Copyright (C) 2003 Greg Kroah-Hartman <greg@kroah.com>
Copyright (C) 2005-2006 Kay Sievers <kay.sievers@vrfy.org>
Copyright (C) 2004 Daniel Walsh
Copyright (C) 2004 Ling, Xiaofeng <xiaofeng.ling@intel.com>
Copyright (C) 2006 Hannes Reinecke hare@suse.de

```
/*
 * Copyright (C) 2005-2006 Kay Sievers <kay.sievers@vrfy.org>
 *
 *      This program is free software; you can redistribute it and/or modify it
 *      under the terms of the GNU General Public License as published by the
 *      Free Software Foundation version 2 of the License.
 *
 *      This program is distributed in the hope that it will be useful, but
 *      WITHOUT ANY WARRANTY; without even the implied warranty of
 *      MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See
the GNU
 *      General Public License for more details.
 *
 *      You should have received a copy of the GNU General Public License
along
 *      with this program; if not, write to the Free Software Foundation, Inc.,
 *      51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA.
 *
 */
```

See full license text on page 223.

uhttpd	Apache License, Version 2.0 /* * uhttpd - Tiny single-threaded httpd - Main component * * Copyright (C) 2010 Jo-Philipp Wich <xm@subsignal.org> * * Licensed under the Apache License, Version 2.0 (the "License"); * you may not use this file except in compliance with the License. * You may obtain a copy of the License at * * http://www.apache.org/licenses/LICENSE-2.0 * * Unless required by applicable law or agreed to in writing, software * distributed under the License is distributed on an "AS IS" BASIS, * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. * See the License for the specific language governing permissions and * limitations under the License. */
Wireless-tools	Copyright (c) 1997-2007 Jean Tourrilhes <jt@hpl.hp.com> (Ref: wireless_tools.29/COPYING) GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See full license text on page 223.

zlib	(C) 1995-2004 Jean-loup Gailly and Mark Adler jloup@gzip.org madler@alumni.caltech.edu This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly Mark Adler jloup@gzip.org madler@alumni.caltech.edu
lighttpd	# # Copyright (C) 2006-2012 OpenWrt.org # # This is free software, licensed under the GNU General Public License v2. # See /LICENSE for more information. # See full license text on page **223**. Copyright (c) 2004, Jan Kneschke, incremental All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. - Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium Point-To-Multipoint Distributor. Cambium Networks 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 Networks shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

Limit of liability

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

System threshold, output power and link loss

The following table specifies the system threshold (dBm), output power (dBm) and maximum link loss (dB) per channel bandwidth and modulation mode:

- Table 80 - 5 GHz
- Table 81 – 2.4 GHz

Table 80 5 GHz threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth		Output power (dBm)	Maximum link loss (dB) per channel bandwidth	
	20 MHz	40 MHz	All bands	20 MHz	40 MHz
MCS15	-68	-65	23	115	112
MCS14	-70	-67	23	117	114
MCS13	-73	-70	23	120	117
MCS12	-77	-74	23	124	121
MCS11	-81	-79	23	128	126
MCS10	-83	-80	23	130	127
MCS9	-86	-84	23	133	131
MCS1	-89	-87	23	136	134

Table 81 2.4 GHz threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth		Output power (dBm)	Maximum link loss (dB) per channel bandwidth	
	20 MHz	40 MHz	All bands	20 MHz	40 MHz
MCS15	-68	-65	23	115	112
MCS14	-70	-67	23	117	114
MCS13	-73	-70	23	120	117
MCS12	-77	-74	23	124	121
MCS11	-81	-79	23	128	126
MCS10	-83	-80	23	130	127
MCS9	-86	-84	23	133	131
MCS1	-89	-87	23	136	134

Compliance with safety standards

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

ELECTRICAL SAFETY COMPLIANCE

The ePMP hardware has been tested for compliance to the electrical safety specifications listed in Table 82.

Table 82 ePMP safety compliance specifications

Region	Standard
USA	UL 60950-1, 2nd Edition
Canada	CSA C22.2 No.60950 2nd Edition
International	International CB certified and certified to IEC 60950-1:2005 (modified) plus EN60950-1:2006 + A1:2010

ELECTROMAGNETIC COMPATIBILITY (EMC) COMPLIANCE

The ePMP complies with European EMC Specification EN301 489-1 with testing carried out to the detailed requirements of EN301 489-4.

Table 83 lists the EMC specification type approvals that have been granted for ePMP.

Table 83 EMC emissions compliance

Region	Specification (Type Approvals)
USA	FCC CFR 47 Part 15 class B
Canada	RSS210, Issue 8
Europe	ETSI EN301 489-4

HUMAN EXPOSURE TO RADIO FREQUENCY ENERGY

Standards

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

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

Power density exposure limit

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

The applicable power density exposure limit from the standards (see **Human exposure to radio frequency energy** on page **262**) is:

- **10 W/m^2** for RF energy in the 5 GHz and 2.4 GHz frequency bands.

Calculation of power density

Note

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

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

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

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

Rearranging terms to solve for distance yields:

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

Calculated distances and power compliance margins

Table 84 shows calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination. These are conservative distances that include compliance margins. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

Explanation of terms used in Table 84:

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

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

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

S – power density (W/m^2)

d – minimum distance from point source (meters)

R – recommended distances (meters)

C – compliance factor

Table 84 Power compliance margins, 5 GHz

Band	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	C
5 GHz	Integrated, 13 dBi	0.199	20	10	0.18	.4	51
5 GHz	Connectorized, 15 dBi	0.199	31.6	10	0.22	.4	32

Table 85 Power compliance margins, 2.4 GHz, AP

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	C
PMP	20 MHz	Connectorized, 8 dBi Omni	0.631	6.3	10	0.18	0.4	50.5
PMP	40 MHz	Connectorized, 8 dBi Omni	0.631	6.3	10	0.18	0.4	50.5
PMP	20 MHz	Connectorized, 17 dBi Sector	0.079	50.1	10	0.18	0.4	50.5
PMP	40 MHz	Connectorized, 17 dBi Sector	0.032	50.1	10	0.11	0.3	71.3
PTP	20 MHz	Connectorized, 25 dBi Dish	0.003	316.2	10	0.08	0.2	63.2
PTP	40 MHz	Connectorized, 25 dBi Dish	0.003	316.2	10	0.08	0.2	63.2

Table 86 Power compliance margins, 2.4 GHz, STA

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	C
PMP	20 MHz	Connectorized, 8 dBi Omni	0.631	6.3	10	0.18	0.4	50.5
PMP	40 MHz	Integrated, 12 dBi Patch	0.251	15.8	10	0.18	0.4	50.5
PMP	20 MHz	Connectorized, 17 dBi Sector	0.079	50.1	10	0.18	0.4	50.5
PMP	40 MHz	Connectorized, 19 dBi Panel	0.050	79.4	10	0.18	0.4	50.5
PMP	20 MHz	Connectorized, 25 dBi Dish	0.010	316.2	10	0.16	0.4	63.5
PMP	40 MHz	Connectorized, 8 dBi Omni	0.100	6.3	10	0.07	0.2	79.6
PMP	20 MHz	Integrated, 12 dBi Patch	0.050	15.8	10	0.08	0.2	63.2
PMP	40 MHz	Connectorized, 17 dBi Sector	0.025	50.1	10	0.10	0.2	39.9
PMP	20 MHz	Connectorized, 19 dBi Panel	0.020	79.4	10	0.11	0.3	71.3
PMP	40 MHz	Connectorized, 25 dBi Dish	0.006	316.2	10	0.13	0.3	56.7
PTP	20 MHz	Integrated, 12 dBi Patch	0.398	15.8	10	0.22	0.4	31.9

PTP	40 MHz	Connectorized, 17 dBi Sector	0.158	50.1	10	0.25	0.5	39.5
PTP	20 MHz	Connectorized, 19 dBi Panel	0.050	79.4	10	0.18	0.4	50.5
PTP	40 MHz	Connectorized, 25 dBi Dish	0.010	316.2	10	0.16	0.4	63.5
PTP	20 MHz	Integrated, 12 dBi Patch	0.050	15.8	10	0.08	0.2	63.2
PTP	40 MHz	Connectorized, 17 dBi Sector	0.025	50.1	10	0.10	0.2	39.9
PTP	20 MHz	Connectorized, 19 dBi Panel	0.020	79.4	10	0.11	0.3	71.3
PTP	40 MHz	Connectorized, 25 dBi Dish	0.006	316.2	10	0.13	0.3	56.7

Note

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

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

At 2.4 GHz, 5.4 GHz and EU 5.8 GHz, the products are generally limited to a fixed EIRP which can be achieved with the Integrated Antenna. The calculations above assume that the maximum EIRP allowed by the regulations is being transmitted.

Note

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

Compliance with radio regulations

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

Caution

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

TYPE APPROVALS

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

Table 83 lists the radio specification type approvals that have been granted for ePMP frequency variants.

Table 87 Radio certifications

Frequency band	Region	Regulatory approvals
2.4 GHz, 5 GHz	USA	FCC Part 15 Class B
	Canada	IC RSS-210 Issue 8, Annex 8 (or latest)
	Europe	ETSI EN302 502 v1.2.1 ETSI EN301 893 v1.7.1

FCC AND ETSI COMPLIANCE TESTING

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

Note

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

Note

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

EXAMPLES OF REGULATORY LIMITS

Examples of the regulatory limits that apply in typical regions of operation are in the following tables:

- Table 88 – 5.1 GHz
- Table 89 – 5.2 GHz
- Table 90 – 5.4 GHz
- Table 91 – 5.8 GHz
- Table 92 – 2.4 GHz

Table 88 Regulatory Limits - 5.1 GHz

Country	Frequency range	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power
Argentina	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	13
Ecuador	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	13
Malaysia	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	13
Peru	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	13
Philippines	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	13
Venezuela	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	13
Other	5150-5250	5160-5240 every 5 MHz	5170-5230 every 5 MHz	18

Table 89 Regulatory limits - 5.2 GHz

Country	Frequency range	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Argentina	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Brazil	5250-5350					
Canada	5250-5350	5280 to 5320 every 5MHz	5290 to 5310 every 5MHz	DIFF between 20MHz/40MHz -> 12 for 20MHz, 13 for 40MHz	30	Yes
Chile	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Colombia	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Ecuador	5250-5350	5260 to 5340 every 5MHz	5270 to 5330 every 5MHz	13		No
Ghana	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Guam	5250-5350	5280 to 5320 every 5MHz	5290 to 5310 every 5MHz	DIFF between 20MHz/40MHz -> 12 for 20MHz, 13 for 40MHz	30	Yes
Hong Kong	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Kenya	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Malaysia	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Peru	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Philippines	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
Puerto Rico	5250-5350	5280 to 5320 every 5MHz	5290 to 5310 every 5MHz	DIFF between 20MHz/40MHz -> 12 for	30	Yes

Country	Frequency range	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
				20MHz, 13 for 40MHz		
Taiwan	5250-5350	5280 to 5320 every 5MHz	5290 to 5310 every 5MHz	13		Yes
Thailand	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	13		Yes
U.S. Virgin Islands	5250-5350	5280 to 5320 every 5MHz	5290 to 5310 every 5MHz	DIFF between 20MHz/40MHz -> 12 for 20MHz, 13 for 40MHz	30	Yes
Uganda	5250-5350	5270 to 5330 every 5MHz	5280 to 5320 every 5MHz	18		Yes
United States	5250-5350	5280 to 5320 every 5MHz	5290 to 5310 every 5MHz	DIFF between 20MHz/40MHz -> 12 for 20MHz, 13 for 40MHz	30	Yes
Venezuela	5250-5350	5260 to 5340 every 5MHz	5270 to 5330 every 5MHz	13		No
Other	5250-5350	5260 to 5340 every 5MHz	5270 to 5330 every 5MHz	18		No

Table 90 Regulatory limits - 5.4 GHz

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Argentina	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16		None
Australia	5470-5600,5650-5725	5485 to 5590 every 5MHz, 5660 to 5710 every 5 MHz	5495 to 5580 every 5MHz, 5670 to 5700 every 5 MHz	15	30	ETSI
Austria	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Belgium	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Bosnia and Herzegovina	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Brazil	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	FCC
Bulgaria	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Canada	5470-5600,5650-5725 (*1)	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	13	30	FCC
Chile	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	FCC
Colombia	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	FCC
Croatia	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Cyprus	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Czech Republic	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Denmark	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Ecuador	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	None
Finland	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
France	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Germany	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Ghana	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	FCC
Greece	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Guam	5470-5600,5650-5725	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	(5.47GHz to 5.55 GHz is 10) (5.55GHz to 5.725 GHz is 13)	30	FCC
Hong Kong	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	15	30	FCC
Hungary	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Ireland	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Italy	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Kenya	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	FCC

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Latvia	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Liechtenstein	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Lithuania	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Luxembourg	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Macedonia	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Malaysia	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16		
Malta	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Mauritius	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	15	30	ETSI
Mexico	5470-5600,5650-5725	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	16	30	FCC
Netherlands	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Netherlands Antilles	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Nigeria	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	15	36	
Norway	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Oman	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	15	30	ETSI
Peru	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	ETSI
Philippines	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	26	
Poland	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Portugal	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Puerto Rico	5470-5600,5650-5725	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	(5.47GHz to 5.55 GHz is 10) (5.55GHz to 5.725 GHz is 13)	30	FCC
Romania	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Serbia	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Slovakia	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Slovenia	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
South Africa	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	15	30	FCC
South Korea	5470-5650	5480 to 5640 every 5MHz	5490 to 5630 every 5MHz	16	30	ETSI
Spain	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Sweden	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Switzerland	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
Taiwan	5470-5600,5650-5725	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	13	30	FCC
Thailand	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	FCC
Turkey	5470-5725	5485 to 5710 every 5MHz	5495 to 5700 every 5MHz	15	30	ETSI
U.S. Virgin Islands	5470-5600,5650-5725	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	(5.47GHz to 5.55 GHz is 10) (5.55GHz to 5.725 GHz is 13)	30	FCC
Uganda	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	19	30	FCC
United Kingdom	5470-5600,5650-5725 (*1)	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI
United States	5470-5600,5650-5725	5495 to 5590 every 5MHz, 5660 to 5705 every 5 MHz	5510 to 5580 every 5MHz, 5670 to 5695 every 5 MHz	(5.47GHz to 5.55 GHz is 10) (5.55GHz to 5.725 GHz is 13)	30	FCC
Venezuela	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16	30	None
Vietnam						
Other	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	19		None
Follow AP CC	5470-5725	5480 to 5715 every 5MHz	5490 to 5705 every 5MHz	16		None
Generic ETSI	5470-5600,5650-5725	5480 to 5590 every 5MHz, 5660 to 5715 every 5 MHz	5490 to 5580 every 5MHz, 5670 to 5705 every 5 MHz	15	30	ETSI

(*1) The band 5600 MHz to 5650 MHz is reserved for the use of weather radars.

Table 91 Regulatory limits - 5.8 GHz

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Argentina	5725-5825	5735 to 5815 every 5 MHz	5745 to 5805 every 5 MHz	23		None
Australia	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	36	None
Bahrain	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	33	ETSI
Botswana	5725-5875	5735 to 5865 every 5 MHz	5745 to 5855 every 5 MHz	23	40	
Brazil	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Canada	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Chile	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	36	None
China	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	33	None
Colombia	5725-5825	5735 to 5815 every 5 MHz	5745 to 5805 every 5 MHz	23	53	None
Denmark (*1)	5725-5795,5815-5875	5735 to 5785 every 5 MHz, 5825 to 5865 every 5 MHz	5745 to 5775 every 5 MHz, 5835 to 5855 every 5 MHz	23	36	ETSI
Ecuador	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	53	None
Finland	5725-5795,5815-5850	5735 to 5785 every 5 MHz, 5825 to 5840 every 5 MHz	5745 to 5775 every 5 MHz,	23	36	ETSI
Germany	5755-5875	5765 to 5865 every 5 MHz	5775 to 5855 every 5 MHz	23	36	ETSI
Ghana	5725-5825	5740 to 5810 every 5 MHz	5750 to 5800 every 5 MHz	23	36	FCC
Greece	5725-5795	5735 to 5785 every 5 MHz	5745 to 5775 every 5 MHz	23	36	ETSI
Guam	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Hong Kong	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	36	None

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Iceland	5725-5875	5735 to 5865 every 5 MHz	5745 to 5855 every 5 MHz	23	36	ETSI
India	5825-5875	5840 to 5860 every 5 MHz	5850 to 5850 every 5 MHz	23	36	None
Indonesia	5725-5825	5735 to 5815 every 5 MHz	5745 to 5805 every 5 MHz	23	36	None
Ireland	5725-5875	5740 to 5860 every 5 MHz	5750 to 5850 every 5 MHz	23	33	None
Kenya	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	36	None
Liechtenstein	5725-5795,5815-5875	5735 to 5785 every 5 MHz, 5825 to 5865 every 5 MHz	5745 to 5775 every 5 MHz, 5835 to 5855 every 5 MHz	23	36	ETSI
Malaysia	5725-5875	5740 to 5860 every 5 MHz	5750 to 5850 every 5 MHz	23	30	None
Mauritius	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	36	ETSI
Mexico	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	36	None
New Zealand	5725-5825	5740 to 5810 every 5 MHz	5750 to 5800 every 5 MHz	23	53	
Nigeria	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23		ETSI
Norway (*1)	5725-5795,5815-5850	5735 to 5785 every 5 MHz, 5825 to 5840 every 5 MHz	5745 to 5775 every 5 MHz,	23	53	ETSI
Oman	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	33	ETSI
Peru	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	36	None
Philippines	5725-5825	5740 to 5810 every 5 MHz	5750 to 5800 every 5 MHz	23	30	
Portugal	5725-5875	5735 to 5865 every 5 MHz	5745 to 5855 every 5 MHz	23	36	ETSI
Puerto Rico	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Serbia	5725-5875	5735 to 5865 every 5 MHz	5745 to 5855 every 5 MHz	23	36	ETSI
Seychelles	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	53	ETSI

Country	Frequency ranges	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power	EIRP Power	DFS
Singapore	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	30	ETSI
South Africa	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	53	
South Korea	5725-5825	5740 to 5810 every 5 MHz	5750 to 5800 every 5 MHz	23	30	
Spain (*1)	5725-5795,5815-5855	5735 to 5785 every 5 MHz, 5825 to 5845 every 5 MHz	5745 to 5775 every 5 MHz, 5835 to 5835 every 5 MHz	23	36	ETSI
Switzerland	5725-5795,5815-5875	5735 to 5785 every 5 MHz, 5825 to 5865 every 5 MHz	5745 to 5775 every 5 MHz, 5835 to 5855 every 5 MHz	23	36	ETSI
Taiwan	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Thailand	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	30	None
U.S. Virgin Islands	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Uganda	5725-5825	5735 to 5815 every 5 MHz	5745 to 5805 every 5 MHz	23	32+2*Ag/3	
United Kingdom (*1)	5725-5795,5815-5850	5735 to 5785 every 5 MHz, 5825 to 5840 every 5 MHz	5745 to 5775 every 5 MHz,	23	36	ETSI
United States	5725-5850	5740 to 5835 every 5 MHz	5750 to 5825 every 5 MHz	23	PMP AP is 36. Other device/mode has no limit	None
Venezuela	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	36	None
Vietnam	5725-5850	5735 to 5840 every 5 MHz	5745 to 5830 every 5 MHz	23	30	None
Other	5725-5875	5735 to 5865 every 5 MHz	5745 to 5855 every 5 MHz	23		None
Follow AP CC	5725-5875	5735 to 5865 every 5 MHz	5745 to 5855 every 5 MHz	23		None

(*1) 5795 MHz to 5815 MHz band is assigned for Road Transport and Traffic Telematics (RTTT).

Table 92 Regulatory limits - 2.4 GHz

Country	Frequency range	Valid Center Frequency for 20 MHz Band	Valid Center Frequency for 40 MHz Band	Conducted Power
Argentina	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27
Canada	2400-2500	2412-2462 every 5MHz	2427-2452 every 5MHz	27
Ecuador	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27
Malaysia	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27
Peru	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27
Philippines	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27
United States	2400-2500	2412-2462 every 5MHz	2427-2452 every 5MHz	27
Venezuela	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27
Other	2400-2500	2412-2462 every 5MHz	2422-2452 every 5MHz	27

Notifications

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

2.4 GHZ, 5.4 GHZ REGULATORY COMPLIANCE

The ePMP complies with the regulations that are enforced in the USA, Canada and Europe. The relevant notifications are specified in this section.

2.4 GHz, 5.4 GHz FCC and IC notification

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

This device complies with part 15.407 of the US FCC Rules and Regulations and with RSS-210 Issue 8 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. In Canada, users must be cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5470 – 5725 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

For the connectorized version of the product and in order to reduce potential radio interference to other users, the antenna type and its gain must be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted by the regulations. The transmitted power must be reduced to achieve this requirement.

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

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

FCC IDs and Industry Canada Certification Numbers are reproduced on the product label (Figure 56 and Figure 57).

Figure 56 FCC and IC certifications on 5 GHz product labels

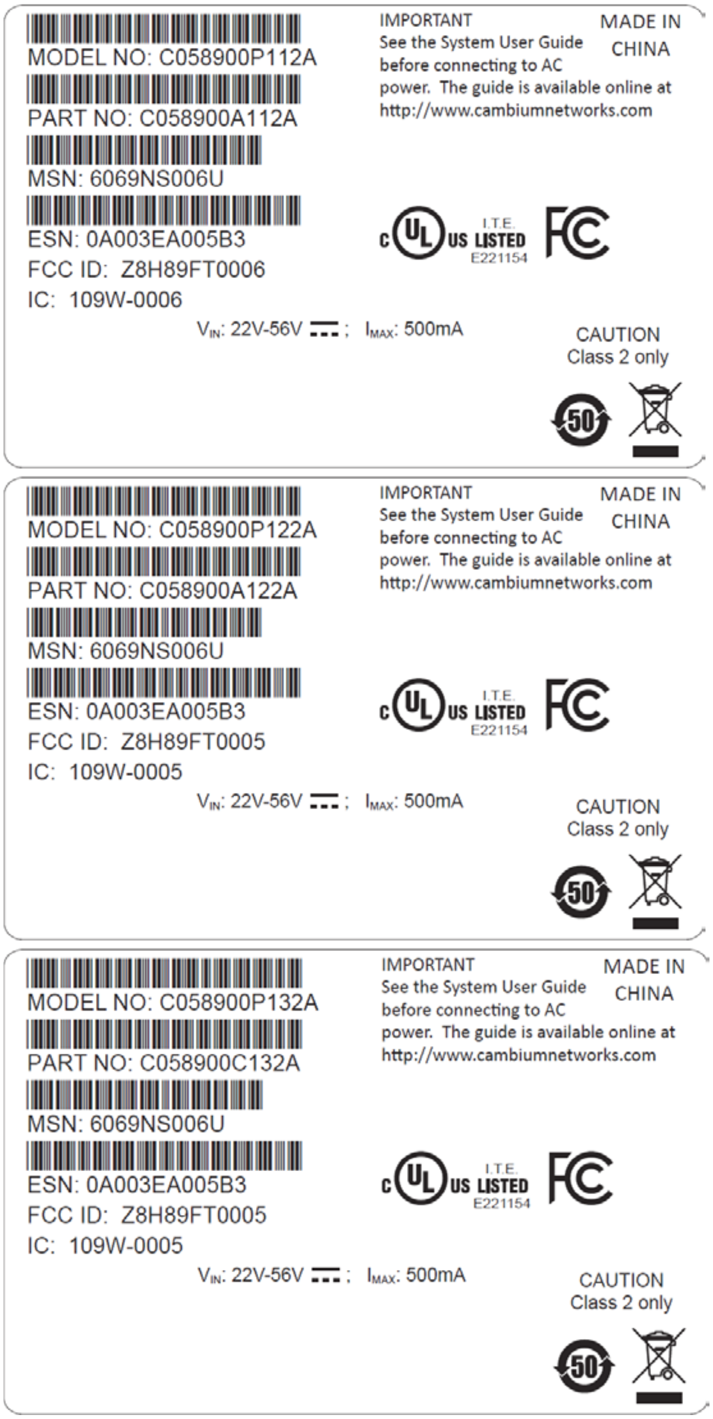


Figure 57 FCC and IC certifications on 2.4 GHz product labels

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

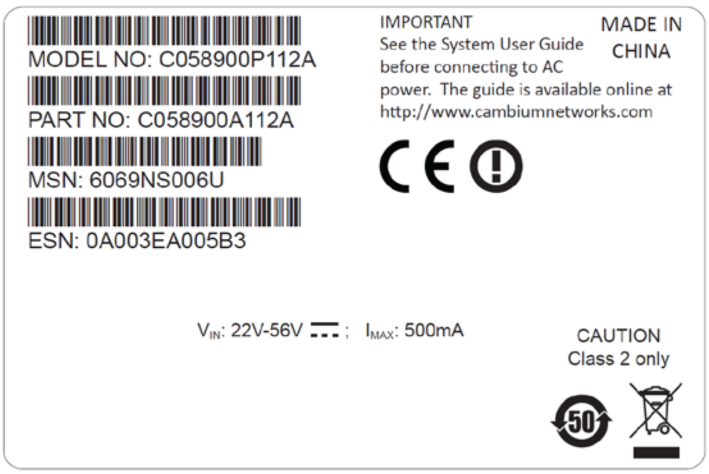
5.4 GHz European Union notification

The ePMP product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 1 device and uses operating frequencies that are harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

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

The European R&TTE directive 1999/5/EC Certification Number is reproduced on the product label (Figure 58).

Figure 58 European Union certification on 5.4 GHz product label



5.8 GHZ REGULATORY COMPLIANCE

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

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

U.S. Federal Communication Commission (FCC)

This device complies with part 15 of the US FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

Industry Canada (IC)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme á la norme NMB-003 du Canada.

RSS-GEN issue 3 (7.1.3) Licence-Exempt Radio Apparatus:

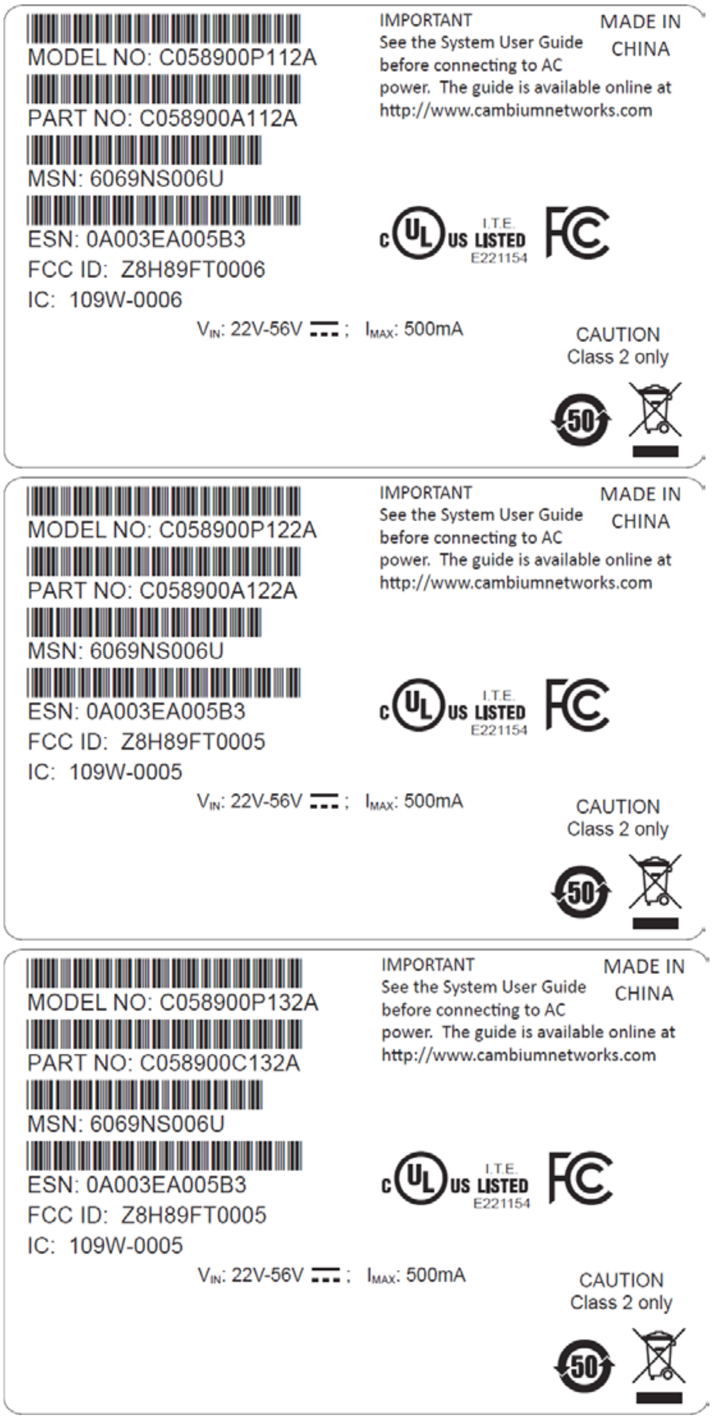
> This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
>
> *Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

In Canada, high power radars are allocated as primary users (meaning they have priority) of the 5650 – 5850 MHz spectrum. These radars could cause interference or damage to license-exempt local area network (LE-LAN) devices.

Product labels

FCC IDs and Industry Canada Certification Numbers are reproduced on the product label (**Figure 59**).

Figure 59 FCC and IC certifications on 5.8 GHz product label



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

5.8 GHz European Union notification

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

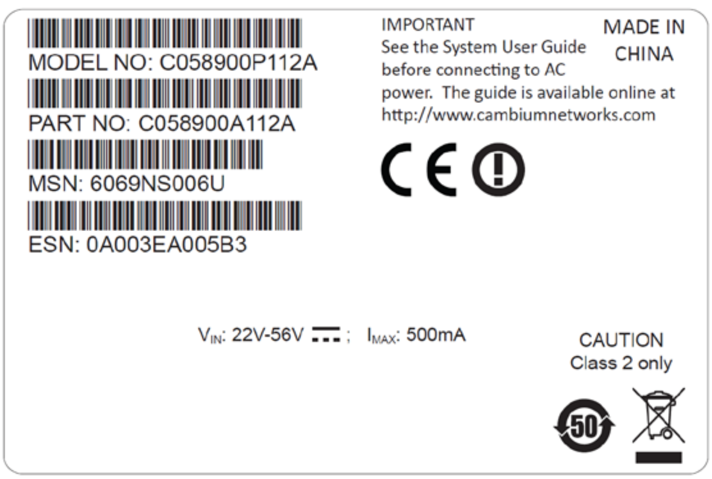
Caution

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

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

The European R&TTE directive 1999/5/EC Certification Number is reproduced on the product label (**Figure 60**).

Figure 60 European Union certification on 5.8 GHz product label



5.8 GHz operation in the UK

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

THAILAND NOTIFICATION

เครื่องโทรคมนาคมและอุปกรณ์นี
มีความสอดคล้องตามข้อกำหนดของ กทช.

This telecommunication equipment conforms to the requirements of the National Telecommunications Commission.

Data throughput tables

This section contains tables to support calculation of the data rate capacity that can be provided by ePMP configurations, as follows:

- Data throughput capacity on page 287

DATA THROUGHPUT CAPACITY

Table 93 shows the data throughput rates (Mbits/s) achieved with an AP/STA pair and the link distance (range), is 0 km.

Table 93 Throughput for ePMP

MCS	Spatial Streams	Mod. Type	Coding Rate	20 MHz			40 MHz		
				DL	UL	Both	DL	UL	Both
MCS15	2	64-QAM	5/6	90.64	28.33	118.97	187.83	55.23	243.06
MCS14	2	64-QAM	3/4	72.93	22.02	94.95	174.46	50.23	224.69
MCS13	2	64-QAM	2/3	53.15	13.52	66.67	151.41	46.54	197.95
MCS12	2	16-QAM	3/4	36.46	10.91	47.37	107.07	29.88	136.95
MCS11	2	16-QAM	1/2	27.57	8.6	37.17	56.66	15.48	72.14
MCS10	2	QPSK	3/4	21.96	7.57	29.53	38	11.67	49.67
MCS9	2	QPSK	1/2	9.31	3.18	12.49	19.06	5.93	24.99
MCS1	1	QPSK	1/2	8.39	2.42	10.81	18.63	5.72	24.35

At zero range. All rates are in Mbit/s. UDP 1518-byte packets, 75%DL/25%UL duty cycle

Radio Specifications

CONNECTORIZED RADIO SPECIFICATIONS

Table 94 Connectorized Radio specifications, 5 GHz

Product	
SALES MODEL NUMBERS	C058900A112A (US/FCC), C050900A013A (EU), C050900A011A (ROW)
Spectrum	
CHANNEL SPACING	Configurable on 5 MHz increments
FREQUENCY RANGE	5150 - 5875 MHz
CHANNEL WIDTH	20 MHz or 40 MHz
Interface	
MAC (MEDIA ACCESS CONTROL) LAYER	Cambium Proprietary
PHYSICAL LAYER	2x2 MIMO/OFDM
ETHERNET INTERFACE	100/1000BaseT, rate auto negotiated (802.3af compliant)
POWERING METHODS SUPPORTED	30V PoE Supply (included), CMM3 & CMM4, 802.3af PoE Supply
PROTOCOLS USED	IPv4, UDP, TCP, IP, ICMP, SSH, SNMPv2c, HTTP, HTTPs, FTP
NETWORK MANAGEMENT	HTTP, HTTPs, SSH, FTP, SNMPv2c
VLAN	802.1Q with 802.1p priority
Performance	
SUBSCRIBERS PER SECTOR	Up to 120
ARQ	Yes
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 20MHZ CHANNEL	MCS1 = -89 dBm to MCS15 = -68 dBm (per branch)
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 40MHZ CHANNEL	MCS1 = -87 dBm to MCS15 = -65 dBm (per branch)
MAXIMUM DEPLOYMENT RANGE @ 20 MHz CHANNEL	Up to 13 miles
MAXIMUM DEPLOYMENT RANGE @ 40 MHz CHANNEL	Up to 9 miles
MODULATION LEVELS (ADAPTIVE)	MCS1 (QPSK 1/2) to MCS15 (64QAM 5/6)

LATENCY (nominal, roundtrip)	17 ms
GPS SYNCHRONIZATION	Yes, via Internal GPS, CMM3, or CMM4
QUALITY OF SERVICE	Three level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Addr,
Link Budget	
ANTENNA Options	Antennas for 90° or 120° sectors are available
TRANSMIT POWER RANGE	-20 to +30 dBm (combined, to regional EIRP limit) (1 dB interval)
ANTENNA GAIN	15 dBi (90° sector)
MAXIMUM TRANSMIT POWER	30 dBm combined (5.8 GHz Band)
Physical	
ANTENNA CONNECTION	50 Ω, RP (Rev
SURGE SUPPRESSION	1 Joule Integrated
ENVIRONMENTAL	IP55
TEMPERATURE	-30°C to +55°C (-22°F to +131°F)
WEIGHT	4.5 kg (10 lbs) with antenna 0.52 kg (1.1 lbs) without antenna
WIND SURVIVAL	190 km/hour (118 mi/hour) with antenna
DIMENSIONS (H x W x D)	Radio: 26.9 x 11 x 7.7 cm (10.6 x 4.3 x 3.0 in) Antenna (excl brackets): 80.4 x 16 x 6.3 cm (31.7 x 6.3 x 2.5 in)
Security	
ENCRYPTION	128-bit AES (CCMP mode)
Certifications	
FCCID	Z8H89FT0006
INDUSTRY CANADA CERT	109W-0006
CE	EN 302 502 v1.2.1 EN 301 893 v1.7.1

Table 95 Connectorized Radio specifications, 2.4 GHz

Product	
SALES MODEL NUMBERS	C024900A011A
Spectrum	
CHANNEL SPACING	Configurable on 5 MHz increments
FREQUENCY RANGE	2402 - 2472 MHz (20 MHz) 2407 - 2472 MHz (40 MHz)
CHANNEL WIDTH	20 MHz or 40 MHz
Interface	
MAC (MEDIA ACCESS CONTROL) LAYER	Cambium Proprietary
PHYSICAL LAYER	2x2 MIMO/OFDM
ETHERNET INTERFACE	100/1000BaseT, rate auto negotiated (802.3af compliant)
POWERING METHODS SUPPORTED	30V PoE Supply (included), CMM3 & CMM4, 802.3af PoE Supply
PROTOCOLS USED	IPv4, UDP, TCP, IP, ICMP, SSH, SNMPv2c, HTTP, HTTPs, FTP
NETWORK MANAGEMENT	HTTP, HTTPs, SSH, FTP, SNMPv2c
VLAN	802.1Q with 802.1p priority
Performance	
SUBSCRIBERS PER SECTOR	Up to 120
ARQ	Yes
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 20MHZ CHANNEL	MCS1 = -89 dBm to MCS15 = -68 dBm (per branch)
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 40MHZ CHANNEL	MCS1 = -87 dBm to MCS15 = -65 dBm (per branch)
MAXIMUM DEPLOYMENT RANGE @ 20 MHz CHANNEL	Up to 13 miles
MAXIMUM DEPLOYMENT RANGE @ 40 MHz CHANNEL	Up to 9 miles
MODULATION LEVELS (ADAPTIVE)	MCS1 (QPSK 1/2) to MCS15 (64QAM 5/6)
LATENCY (nominal, roundtrip)	17 ms
GPS SYNCHRONIZATION	Yes, via Internal GPS, CMM3, or CMM4

QUALITY OF SERVICE	Three level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Addr,
Link Budget	
ANTENNA Options	Antennas for 90° or 120° sectors are available
TRANSMIT POWER RANGE	-20 to +30 dBm (combined, to regional EIRP limit) (1 dB interval)
ANTENNA GAIN	15 dBi (90° / 120° sector)
MAXIMUM TRANSMIT POWER	30 dBm combined
Physical	
ANTENNA CONNECTION	50 Ω, RP (Reve
SURGE SUPPRESSION	1 Joule Integrated
ENVIRONMENTAL	IP55
TEMPERATURE	-30°C to +55°C (-22°F to +131°F)
WEIGHT	4.5 kg (10 lbs) with antenna 0.52 kg (1.1 lbs) without antenna
WIND SURVIVAL	190 km/hour (118 mi/hour) with antenna
DIMENSIONS (H x W x D)	Radio: 26.9 x 11 x 7.7 cm (10.6 x 4.3 x 3.0 in) Antenna (excl brackets): 80.4 x 16 x 6.3 cm (31.7 x 6.3 x 2.5 in)
Security	
ENCRYPTION	128-bit AES (CCMP mode)
Certifications	
FCCID	Z8H89FT0006
INDUSTRY CANADA CERT	109W-0006
CE	EN 302 502 v1.2.1 EN 301 893 v1.7.1

INTEGRATED RADIO SPECIFICATIONS

Table 96 Integrated Radio specifications, 5 GHz

Product	
MODEL NUMBER	C058900C132A (US/FCC), C050900C033A (EU), C050900C031A (ROW)
Spectrum	
CHANNEL SPACING	Configurable on 5 MHz increments
FREQUENCY RANGE	5150 - 5875 MHz
CHANNEL WIDTH	20 MHz or 40 MHz
Interface	
MAC (MEDIA ACCESS CONTROL) LAYER	Cambium Proprietary
PHYSICAL LAYER	2x2 MIMO/OFDM
ETHERNET INTERFACE	100BaseT, Cambium PoE (V+ = pins 7 & 8, Return = pins 4 & 5)
PROTOCOLS USED	IPv4, UDP, TCP, IP, ICMP, SSH, SNMPv2c, HTTPs, FTP
NETWORK MANAGEMENT	HTTPs, SSH, FTP, SNMPv2c
VLAN	802.1Q with 802.1p priority
Performance	
ARQ	Yes
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 20MHZ CHANNEL	MCS1 = -89 dBm to MCS15 = -70 dBm (per branch)
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 40MHZ CHANNEL	MCS1 = -87 dBm to MCS15 = -65 dBm (per branch)
MAXIMUM DEPLOYMENT RANGE @ 20 MHz CHANNEL	Up to 13 miles
MODULATION LEVELS (ADAPTIVE)	MCS1 (QPSK 1/2) to MCS15 (64QAM 5/6)
LATENCY (nominal, roundtrip)	17 ms
QUALITY OF SERVICE	Three level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Addr, Broadcast, Multicast and Station Priority
Link Budget	
ANTENNA BEAM WIDTH	24° azimuth, 12° elevation

TRANSMIT POWER RANGE	-20 to +30 dBm (combined, to regional EIRP limit) (1 dB interval)
ANTENNA GAIN	13 dBi, integrated patch
MAXIMUM TRANSMIT POWER	30 dBm combined (5.8 GHz Band)
Physical	
ANTENNA CONNECTION	Integrated patch antenna
SURGE SUPPRESSION	1 Joule Integrated
ENVIRONMENTAL	IP55
TEMPERATURE	-30°C to +55°C (-22°F to +131°F)
WEIGHT	0.49 kg (1.1 lb.)
WIND SURVIVAL	145 km/hour (90 mi/hour) with antenna
DIMENSIONS (H x W x D)	29.1 x 14.5 x 8.3 cm (11.4 x 5.7 x 3.3 in)
POWER CONSUMPTION	7 W Maximum, 5 W Typical
INPUT VOLTAGE	24 to 30 V
Security	
ENCRYPTION	128-bit AES (CCMP mode)
Certifications	
FCCID	Z8H89FT0006
INDUSTRY CANADA CERT	109W-0006
CE	EN 302 502 v1.2.1 EN 301 893 v1.7.1

Table 97 Integrated Radio specifications, 2.4 GHz

Product	
MODEL NUMBER	C024900A031A
Spectrum	
CHANNEL SPACING	Configurable on 5 MHz increments
FREQUENCY RANGE	2402 - 2472 MHz (20 MHz) 2407 - 2472 MHz (40 MHz)
CHANNEL WIDTH	20 MHz or 40 MHz
Interface	
MAC (MEDIA ACCESS CONTROL) LAYER	Cambium Proprietary
PHYSICAL LAYER	2x2 MIMO/OFDM
ETHERNET INTERFACE	100BaseT, Cambium PoE (V+ = pins 7 & 8, Return = pins 4 & 5)
PROTOCOLS USED	IPv4, UDP, TCP, IP, ICMP, SSH, SNMPv2c, HTTPs, FTP
NETWORK MANAGEMENT	HTTPs, SSH, FTP, SNMPv2c
VLAN	802.1Q with 802.1p priority
Performance	
ARQ	Yes
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 20MHZ CHANNEL	MCS1 = -89 dBm to MCS15 = -70 dBm (per branch)
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 40MHZ CHANNEL	MCS1 = -87 dBm to MCS15 = -65 dBm (per branch)
MAXIMUM DEPLOYMENT RANGE @ 20 MHz CHANNEL	Up to 13 miles
MODULATION LEVELS (ADAPTIVE)	MCS1 (QPSK 1/2) to MCS15 (64QAM 5/6)
LATENCY (nominal, roundtrip)	17 ms
QUALITY OF SERVICE	Three level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Addr, Broadcast, Multicast and Station Priority
Link Budget	
ANTENNA BEAM WIDTH	24° azimuth, 12° elevation
TRANSMIT POWER RANGE	-20 to +30 dBm (combined, to regional EIRP limit) (1 dB interval)

ANTENNA GAIN	12 dBi, integrated patch
MAXIMUM TRANSMIT POWER	30 dBm combined
Physical	
ANTENNA CONNECTION	Integrated patch antenna
SURGE SUPPRESSION	1 Joule Integrated
ENVIRONMENTAL	IP55
TEMPERATURE	-30°C to +55°C (-22°F to +131°F)
WEIGHT	0.49 kg (1.1 lb.)
WIND SURVIVAL	145 km/hour (90 mi/hour) with antenna
DIMENSIONS (H x W x D)	29.1 x 14.5 x 8.3 cm (11.4 x 5.7 x 3.3 in)
POWER CONSUMPTION	7 W Maximum, 5 W Typical
INPUT VOLTAGE	24 to 30 V
Security	
ENCRYPTION	128-bit AES (CCMP mode)
Certifications	
FCCID	Z8H89FT0006
INDUSTRY CANADA CERT	109W-0006
CE	EN 302 502 v1.2.1 EN 301 893 v1.7.1

UN-SYNCED CONNECTORIZED RADIO SPECIFICATIONS

Table 98 Un-synced Connectorized Radio specifications, 5 GHz

Product	
SALES MODEL NUMBERS	C058900A122A (US/FCC), C050900A023A (EU), C050900A021A (ROW)
Spectrum	
CHANNEL SPACING	Configurable on 5 MHz increments
FREQUENCY RANGE	5150 - 5875 MHz
CHANNEL WIDTH	20 MHz or 40 MHz
Interface	
MAC (MEDIA ACCESS CONTROL) LAYER	Cambium Proprietary
PHYSICAL LAYER	2x2 MIMO/OFDM
ETHERNET INTERFACE	100BaseT, Cambium PoE (V+ = pins 7 & 8, Return = pins 4 & 5)
PROTOCOLS USED	IPv4, UDP, TCP, IP, ICMP, SSH, SNMPv2c, HTTPs, FTP
NETWORK MANAGEMENT	HTTPs, SSH, FTP, SNMPv2c
VLAN	802.1Q with 802.1p priority
Performance	
ARQ	Yes
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 20MHZ CHANNEL	MCS1 = -89 dBm to MCS15 = -70 dBm (per branch)
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 40MHZ CHANNEL	MCS1 = -87 dBm to MCS15 = -65 dBm (per branch)
MAXIMUM DEPLOYMENT RANGE @ 20 MHz CHANNEL	Up to 13 miles
MAXIMUM DEPLOYMENT RANGE @ 40 MHz CHANNEL	Up to 9 miles
MODULATION LEVELS (ADAPTIVE)	MCS1 (QPSK 1/2) to MCS15 (64QAM 5/6)
LATENCY (nominal, roundtrip)	17 ms
QUALITY OF SERVICE	Three level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Addr, Broadcast, Multicast and Station Priority

Link Budget	
ANTENNA Options	Antennas for 90° or 120° sectors are available
TRANSMIT POWER RANGE	-20 to +30 dBm (combined, to regional EIRP limit) (1 dB interval)
ANTENNA GAIN	15 dBi (90° sector)
MAXIMUM TRANSMIT POWER	30 dBm combined (5.8 GHz Band)
Physical	
ANTENNA CONNECTION	50 Ω, RP (Rev
SURGE SUPPRESSION	1 Joule Integrated
ENVIRONMENTAL	IP55
TEMPERATURE	-30°C to +55°C (-22°F to +131°F)
WEIGHT	4.5 kg (10 lbs) with antenna 0.52 kg (1.1 lbs) without antenna
WIND SURVIVAL	190 km/hour (118 mi/hour) with antenna
DIMENSIONS (H x W x D)	Radio: 26.9 x 11 x 7.7 cm (10.6 x 4.3 x 3.0 in) Antenna (excl brackets): 80.4 x 16 x 6.3 cm (31.7 x 6.3 x 2.5 in)
Security	
ENCRYPTION	128-bit AES (CCMP mode)
Certifications	
FCCID	Z8H89FT0006
INDUSTRY CANADA CERT	109W-0006
CE	EN 302 502 v1.2.1 EN 301 893 v1.7.1

Table 99 Un-synced Connectorized Radio specifications, 2.4 GHz

Product	
SALES MODEL NUMBERS	C024900A021A
Spectrum	
CHANNEL SPACING	Configurable on 5 MHz increments
FREQUENCY RANGE	2402 - 2472 MHz (20 MHz) 2407 - 2472 MHz (40 MHz)
CHANNEL WIDTH	20 MHz or 40 MHz
Interface	
MAC (MEDIA ACCESS CONTROL) LAYER	Cambium Proprietary
PHYSICAL LAYER	2x2 MIMO/OFDM
ETHERNET INTERFACE	100BaseT, Cambium PoE (V+ = pins 7 & 8, Return = pins 4 & 5)
PROTOCOLS USED	IPv4, UDP, TCP, IP, ICMP, SSH, SNMPv2c, HTTPs, FTP
NETWORK MANAGEMENT	HTTPs, SSH, FTP, SNMPv2c
VLAN	802.1Q with 802.1p priority
Performance	
ARQ	Yes
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 20MHZ CHANNEL	MCS1 = -89 dBm to MCS15 = -70 dBm (per branch)
NOMINAL RECEIVE SENSITIVITY (W/ FEC) @ 40MHZ CHANNEL	MCS1 = -87 dBm to MCS15 = -65 dBm (per branch)
MAXIMUM DEPLOYMENT RANGE @ 20 MHz CHANNEL	Up to 13 miles
MAXIMUM DEPLOYMENT RANGE @ 40 MHz CHANNEL	Up to 9 miles
MODULATION LEVELS (ADAPTIVE)	MCS1 (QPSK 1/2) to MCS15 (64QAM 5/6)
LATENCY (nominal, roundtrip)	17 ms
QUALITY OF SERVICE	Three level priority (Voice, High, Low) with packet classification by DSCP, COS, VLAN ID, IP & MAC Addr, Broadcast, Multicast and Station Priority
Link Budget	
ANTENNA Options	Antennas for 90° or 120° sectors are available

TRANSMIT POWER RANGE	-20 to +30 dBm (combined, to regional EIRP limit) (1 dB interval)
ANTENNA GAIN	15 dBi (90° / 120° sector)
MAXIMUM TRANSMIT POWER	30 dBm combined
Physical	
ANTENNA CONNECTION	50 female, RP (Reverse Pol
SURGE SUPPRESSION	1 Joule Integrated
ENVIRONMENTAL	IP55
TEMPERATURE	-30°C to +55°C (-22°F to +131°F)
WEIGHT	4.5 kg (10 lbs) with antenna 0.52 kg (1.1 lbs) without antenna
WIND SURVIVAL	190 km/hour (118 mi/hour) with antenna
DIMENSIONS (H x W x D)	Radio: 26.9 x 11 x 7.7 cm (10.6 x 4.3 x 3.0 in) Antenna (excl brackets): 80.4 x 16 x 6.3 cm (31.7 x 6.3 x 2.5 in)
Security	
ENCRYPTION	128-bit AES (CCMP mode)
Certifications	
FCCID	Z8H89FT0006
INDUSTRY CANADA CERT	109W-0006
CE	EN 302 502 v1.2.1 EN 301 893 v1.7.1

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
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
STA	Station
SW	Software
TDD	Time Division Duplex

TDWR	Terminal Doppler Weather Radar
TX	Transmit
UNII	Unlicensed National Information Infrastructure
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network