Cambium Networks™

USER GUIDE

ePMP

Forcs 425

Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

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

© 2020 Cambium Networks Limited. All rights reserved

Contents

Contents ... 3

Safety and regulatory information ... 12

Important safety information ... 12

- Power lines ... 12
- Working at heights ... 12
- Grounding and protective earth ... 12
- Powering down before servicing ... 12
- Primary disconnect device ... 12
- External cables ... 12
- RF exposure near the antenna ... 12
- Minimum separation distances ... 12
- Important Regulatory Information ... 13
- Radar avoidance ... 13
- Specific expertise and training required for professional installers ... 13
- Ethernet networking skills ... 13
- Lightning protection ... 13
- Training ... 13

About this User Guide ... 14

General information ... 14

- Version information ... 14
- Contacting Cambium Networks ... 14
- Purpose ... 14
- Cross-references ... 14

Problems and warranty ... 15

- Reporting problems ... 15

Security advice ... 16

Precautionary statements ... 16

- Warning ... 16
- Attention ... 16

Note 16
Caring for the environment 16
In EU countries 17
In non-EU countries 17
Chapter 1: Product description 18
Overview of ePMP 18
Purpose – ePMP portfolio 18
ePMP Force 400C key features 19
Typical installation Equipment 27
Wireless operation 27
MU-MIMO 27
MIMO 28
Smart Beamforming (ePMP Force series) 28
Time-division duplexing 30
OFDM and channel bandwidth 30
Adaptive modulation 30
Radar avoidance 30
Encryption 31
Country codes 31
Further reading on the wireless operation 31
System management 32
Management agent 32
Webserver 32
SNMP 33
Network Time Protocol (NTP) 33
Software upgrade 33
Further reading on system management 33
Chapter 2: System hardware 34
Site planning 34
Site installation 34

Grounding and lightning protection 35
Lightning protection zones 36
ePMP Force 425 Access Point 37
ePMP Force 425 Access Point description 38
ePMP Force 425 Access Point part numbers 38
ePMP Force 425 Access Point mounting bracket 39
ePMP Force 425 Access Point Interfaces 40
ePMP Force 425 Access Point specifications 40
ePMP Force 425 Access Point heater 41
ePMP Force 425 Access Point wind loading 41
ePMP Force 425 Access Point software packages 42
ePMP Force 400C Access Point 42
ePMP Force 400C Access Point description 43
ePMP Force 400C Access Point part numbers 43
ePMP Force 400C Access Point mounting bracket 44
ePMP Force 400C Access Point Interfaces 45
ePMP Force 400C Access Point specifications 45
ePMP Force 400C Access Point heater 46
ePMP Force 400C Access Point wind loading 46
ePMP Force 400C Access Point software packages 47
Force 300-25 47
Force 300-25 Integrated description 48
Force 300-25 part numbers 48
Force 300-25 mounting bracket 49
Force 300-25 Interfaces 50
Force 300-25 specifications 50
Force 300-25 heater 51
Force 300-25 wind loading 51
Force 300-25 software packages 52
Force 300-19 52

Force 300-19 Integrated description 52
Force 300-19 part numbers 53
Force 300-19 mounting bracket 53
Force 300-19 Interfaces 54
Force 300-19 specifications 54
Force 300-19 heater 54
Force 300-19 wind loading 55
Force 300-19 software packages 55
Force 300-19R 56
Force 300-19R Integrated description 56
Force 300-19R part numbers 56
Force 300-19R mounting bracket 57
Force 300-19R Interfaces 58
Force 300-19R specifications 58
Force 300-19R heater 58
Force 300-19R wind loading 59
Force 300-19R software packages 59
Force 300-16 59
Force 300-16 Integrated description 60
Force 300-16 part numbers 60
Force 300-16 Interfaces 61
Force 300-16 specifications 61
Force 300-16 heater 61
Force 300-16 wind loading 62
Force 300-16 software packages 63
Force 300-13 63
Force 300-13 Integrated description 63
Force 300-13 Interfaces 63
Force 300-13 specifications 63
Force 300-13 heater 64

64
Force 300-13 wind loading 64
65
Force 300-13 software packages 65
Force 300-CSM 65
Force 300-CSM Integrated description 66
Force 300-CSM part numbers 66
Force 300-CSM Interfaces 67
Force 300-CSM specifications 67
Force 300-CSM heater 67
68
Force 300-CSM wind loading 68
Force 300-CSM software packages 68
Power Supply 69
Power supply description 69
Power supply part numbers 69
Power supply interfaces 70
Power supply specifications 71
Power supply location 71
Ethernet cabling 71
Ethernet standards and cable lengths 72
Outdoor Cat5e cable 72
Surge suppression unit 73
Gigabit Ethernet Surge Suppressor 73
cnPulse sync generator 75
Chapter 3: System planning 76
Radio spectrum planning 76
General wireless specifications 76
Regulatory limits 77
Available spectrum 78

Conforming to the limits 78
Channel bandwidth 78
Link planning 78
Range and obstacles 78
Path loss 78
Adaptive modulation 79
Data network planning 79
Ethernet interfaces 79
Management VLAN 80
Quality of service for bridged Ethernet traffic 80
Chapter 4: Using the Device Management Interface 81
Preparing for configuration 81
Safety precautions 81
Regulatory compliance 81
Connecting to the unit 81
Configuring the management PC 82
Connecting to the PC and powering up 82
Using the web interface 82
Logging into the web interface 83
Using the installation wizard – Access Point 83
Installation wizard step 1 – Main system parameters 84
Installation wizard step 4 – Security parameters 85
Using the installation wizard – Subscriber Module 86
Installation wizard step 1 – Main system parameters 86
Installation wizard step 2 – Radio parameters 87
Installation wizard step 4 – Security parameters 88
Using the menu options 88
Status page 90
Installation page 93
Configuration menu 93

Configuration > Radio page 93
Configuration > System page 100
Configuration > Network page 105
Configuration > Security page 121
Monitor menu 126
Monitor > Performance page 127
Monitor > System page 132
Monitor > Wireless Page 134
Monitor > Throughput Chart page 140
Monitor > GPS page (Access Point Mode) 140
Monitor > Network page 142
Monitor > System Log Page 145
Tools menu 145
Tools > Software Upgrade page 145
Tools > Backup/Restore page 147
Tools > License Management page (Access Point Mode) 149
Tools > Spectrum Analyzer page 151
Tools > eAlign page 153
Tools > Wireless Link Test page 154
Tools > Watchdog page 155
Tools > Ping page 156
Tools > Traceroute page 157
Chapter 5: Operation and Troubleshooting 159
General Planning for Troubleshooting 159
Upgrading device software 160
Testing hardware 160
Checking the power supply LED 160
Power LED is off 161
Ethernet LED is off 161
Troubleshooting the radio link 162

The module has lost or does not establish radio connectivity 162
Module exhibiting frequent boots or disconnects 163
Link is unreliable or does not achieve data rates required 163
Resetting ePMP to factory defaults by power cycling 163
Chapter 6: Legal and reference information 165
Cambium Networks end user license agreement 165
Acceptance of this agreement 165
Definitions 165
Grant of license 166
Conditions of use 166
Title and restrictions 166
Confidentiality 167
Right to use Cambium's name 167
Transfer 167
Updates 167
Maintenance 167
Disclaimer 168
Limitation of liability 168
U.S. government 168
Term of license 168
Governing law 169
Assignment 169
Survival of provisions 169
Entire agreement 169
Third party software 169
Source Code Requests 169
Hardware warranty 231
Limit of liability 231
System threshold, output power and link loss 231
Compliance with safety standards 231

Electrical safety compliance 231
Electromagnetic compatibility (EMC) compliance 232
Human exposure to radio frequency energy 232
Compliance with radio regulations 241
Type approvals 242
FCC and ETSI compliance testing 242
Notifications 243
5.1 GHz regulatory compliance 243
Radio Specifications 248
Product Specifications 248

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

ePMP devices and mounting structures 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 "Calculated distances and power compliance margins" on page 234.

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).

This device complies with part 15 of the 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.

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 the 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.

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 GHz band (5150 – 5250 MHz – FCC only, 5250 – 5350 MHz, 5470 – 5725 MHz and 5725 – 5850 MHz).

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 Site planning on page "Site planning" on page 34.

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 setups at a base workshop before live installations.

About this User Guide

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

For radio network design, see:

- Chapter 1: Product description
- Chapter 2: System hardware
- Chapter 5: Site planning

For system configuration, monitoring and fault finding, see:

- Chapter 4: Using the Device Management Interface

General information

Version information

The following shows the issue status of this document:

Issue	Date of issue	Remarks
pmp-2461_000v012	Jan 2019	System Release 4.3.0
pmp-2461_001v002	June 2019	System Release 4.3.2

Contacting Cambium Networks

Support website: http://www.cambiumnetworks.com/support
Main website: http://www.cambiumnetworks.com
Sales enquiries: solutions@cambiumnetworks.com
Address: Cambium Networks Limited
Unit B2, Linhay Business Park, Eastern Road
Ashburton, United Kingdom, TQ13 7UP

Purpose

Cambium Networks 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 blue text in electronic versions, are active links to the references.

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

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@cambiumnetworks.com.

Problems and warranty

Reporting problems

At Cambium Networks, we know what it takes to keep a growing network running optimally. We provide multiple layers of support including training, online documentation, technical support, information-sharing with an experienced community of users, software downloads, warranty services, and repair.

Through the Cambium Support Center portal at https://support.cambiumnetworks.com/ you can:

- Submit support requests
- Submit RMA request
- View support global contact numbers

Addition information including field service bulletins, license key information, warranty details, security advisories, Cambium Care program descriptions, regional codes for PTP solutions, and compliance requirements can be viewed at https://www.cambiumnetworks.com/support/.

Repair and service

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

Warranty

For products shipped after October 1st, 2018 Cambium's standard hardware warranty is for three (3) years 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 ePMP products or activate warranties, visit the support website.

For warranty assistance, contact the reseller or distributor.

Attention

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

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

Security advice

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

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

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

Precautionary statements

The following describes how precautionary statements are used in this document.

Warning

Precautionary statements with the Warning tag 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

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

Attention

Precautionary statements with the Attention tag precede instructions that 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. An attention statement has the following format:

Attention

Text and consequence for not following the instructions.

Note

Precautionary statements with the Note tag indicate the possibility of an undesirable situation or provide additional information to help the reader understand a topic or concept. A note has the following format:

Note

Note text.

Caring for the environment

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

In EU countries

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

Disposal of Cambium equipment

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

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

Disposal of surplus packaging

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

In non-EU countries

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

Chapter 1: Product description

This chapter provides a high-level description of the ePMP product. It describes the function of the product, the main product variants, and the typical installation. It also describes the main hardware components.

The following topics are described in this chapter:

- The key features, typical uses, product variants and components of the ePMP are explained in Overview of ePMP on page "Overview of ePMP" below.
- How the ePMP wireless link is operated, including modulation modes, power control, and security is described under Wireless operation on page "Wireless operation" on page 27.
- The ePMP management system, including the web interface, installation, configuration, alerts, and upgrades is described in System management on page "System management " on page 32.

Overview of ePMP

This section introduces the key features, typical uses, product variants and components of the ePMP portfolio as a whole (802.11n and 802.11ac products).

Note

This product meets the UL/cUL 62368 / IEC 62368 edition 2 specification, and the radio housings are designed to be raintight.

Purpose – ePMP portfolio

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

ePMP devices support point-to-point microwave links in the unlicensed 5 GHz band.

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

ePMP Force 400C key features

ePMP Force 400C Access Point

The ePMP Force 400C is the third-generation access point (AP) that carries on the interference tolerance mechanisms with an emphasis on high-performance in low-density point to multipoint sectors. The ePMP Force 400C is a 2X2 MIMO connectorized access point that can support a wide variety of deployments including 90/120 degree sectors, narrow-sector horns or even 360-degree Omni coverage. In addition, the ePMP Force 400C continues interference mitigation techniques with support of TDD synchronization using GPS and the robust software from the ePMP product line. The ePMP Force 400C system consists of the ePMP Force 400C AP, an optional 2X2 sector antenna and a wide variety of subscriber modules with varying form factors and link budgets. ePMP Force 400C supports backward and forward compatibility with ePMP 802.11n devices to provide an immediate sector upgrade to 802.11ac Wave 2 performance, and also to support future upgrades of networks operating ePMP 1000/2000 Access Points.

The ePMP Force 400C system boasts a high packet per second performance, peak throughput of 600 Mbps and supports subscriber modules with up to 600 Mbps of peak throughput.

A summary of the main ePMP Force 400C characteristics is listed under Table 1 Main characteristics of the ePMP Force 400C Series.

Table 2 Main characteristics of the ePMP Force 400C Series

Characteristic	Value
Topology	PMP or PTP
Wireless link condition	LOS, near LOS
Scheduler	TDD
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	20 MHz, 40 MHz, 80 MHz
Data rate	Up to 1+ Gbps Sector Throughput

Force 300-25

Force 300-25 is a rugged high-capacity outdoor point-to-multipoint or point-to-point link wireless device in the unlicensed 5 GHz frequency bands with a maximum UDP throughput of 500+ Mbps (when operating with 80 MHz channel bandwidth). It is capable of operating in line-of-sight (LOS) and near-LOS conditions. Force 300-25 is available as an integrated unit with a dual-polarized 25 dBi narrow Beamwidth dish antenna.

Force 300-25 is based on highly-integrated wireless semiconductor components designed to meet the IEEE 802.11ac standard, however, the Force 300-25 device has a proprietary air interface for the main point-to-point link.

Force 300-25 is powered by standard power-over-Ethernet to a 1000Base-T port.

Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

A summary of the main Force 300-25 characteristics is listed under Table 3 Main characteristics of the Force 300-25 Series.

Table 3 Main characteristics of the Force 300-25 Series

Characteristic	Value
Topology	PMP, PTP
Wireless link condition	LOS, near LOS
Scheduler	TDD
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	20 MHz, 40 MHz, 80 MHz
Data rate	Up to 500+ Mbps

Force 300-19

Force 300-19 is rugged high-capacity outdoor point-to-multipoint or point-to-point link wireless devices in the unlicensed 5 GHz frequency bands with a maximum UDP throughput of 500+ Mbps (when operating with 80 MHz channel bandwidth). The Force 300-19 is IP55 rated capable of operating in line-of-sight (LOS) and near-LOS conditions.

Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

A summary of the main Force 300-19(R) characteristics is listed under Table 4 Main characteristics of the Force 300-16 Series.

Table 4 Main characteristics of the Force 300-19(R) Series

Characteristic	Value
Topology	PMP, PTP
Wireless link condition	LOS, near LOS
Scheduler	TDD
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	20 MHz, 40 MHz, 80 MHz
Data rate	Up to 500+ Mbps

Force 300-19(R)

Force 300-19R is a rugged high-capacity outdoor point-to-multipoint or point-to-point link wireless devices in the unlicensed 5 GHz frequency bands with a maximum UDP throughput of 600+ Mbps (when operating with 80 MHz channel bandwidth). The Force 300-19R is IP67 rated capable of operating in line-of-sight (LOS) and near-LOS conditions. Force 300-19(R) is available as an integrated unit with a dual-polarized 19dBi integrated flat-panel antenna.

Force 300-19(R) is based on highly-integrated wireless semiconductor components designed to meet the IEEE 802.11ac standard, however, the Force 300-19(R) device has a proprietary air interface for the main point-to-point link.

Force 300-19(R) is powered by standard power-over-Ethernet to a 1000Base-T port.

Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

A summary of the main Force 300-19(R) characteristics is listed under Table 4 Main characteristics of the Force 300-16 Series.

Table 5 Main characteristics of the Force 300-19(R) Series

Characteristic	Value
Topology	PMP, PTP
Wireless link condition	LOS, near LOS
Scheduler	TDD
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	5 /10/20/40/80 MHz
Data rate	Up to 500+ Mbps
Environmental	IP67
Temperature	-30°C to +60°C (-22°F to 140°F)

Force 300-16

Force 300-16 is a rugged high-capacity outdoor point-to-multipoint or point-to-point link wireless device in the unlicensed 5 GHz frequency bands with a maximum UDP throughput of 500+ Mbps (when operating with 80 MHz channel bandwidth). It is capable of operating in line-of-sight (LOS) and near-LOS conditions. Force 300-16 is available as an integrated unit with a dual-polarized 16 dBi integrated antenna.

Force 300-16 is based on highly-integrated wireless semiconductor components designed to meet the IEEE 802.11ac standard, however, the Force 300-16 device has a proprietary air interface for the main point-to-point link.

Force 300-16 is powered by standard power-over-Ethernet to a 1000Base-T port.

Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

A summary of the main Force 300-16 characteristics is listed under Table 4.

Table 4 Main characteristics of the Force 300-16 Series

Characteristic	Value
Topology	PMP, PTP
Wireless link condition	LOS, near LOS
Scheduler	TDD
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	20 MHz, 40 MHz, 80 MHz
Data rate	Up to 500+ Mbps

Force 300-13

Force 300-13 is a rugged high-capacity outdoor point-to-multipoint or point-to-point link wireless device in the unlicensed 5 GHz frequency bands with a maximum UDP throughput of 500+ Mbps (when operating with 80 MHz channel bandwidth). It is capable of operating in line-of-sight (LOS). Force 300-13 is available as an integrated unit with a dual-polarized 13dBi flat-panel antenna.

Force 300-13 is based on highly-integrated wireless semiconductor components designed to meet the IEEE 802.11ac standard, however, the Force 300-13 device has a proprietary air interface for the main point-to-point link.

Force 300-13 is powered by standard power-over-Ethernet to a 1000Base-T port.

Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

A summary of the main Force 300-13 characteristics is listed under Table 5.

Table 5 Main characteristics of the Force 300-13 Series

Characteristic	Value
Topology	PMP, PTP
Wireless link condition	LOS
Scheduler	TDD
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	20 MHz, 40 MHz, 80 MHz
Data rate	Up to 500+ Mbps

Force 300-CSM

Force 300-CSM is an IP67 rugged high-capacity outdoor point-to-multipoint or point-to-point link wireless device in the unlicensed 5 GHz frequency bands with a maximum UDP throughput of 600+ Mbps (when operating with 80 MHz channel bandwidth). It is capable of operating in line-of-sight (LOS). Force 300-CMS is a Connectorized device with support for RF Element Twistport™ adaptors.

Force 300-CSM is based on highly-integrated wireless semiconductor components designed to meet the IEEE 802.11ac standard.

Management of the unit is conducted via the same interface as the bridged traffic (in-band Management).

A summary of the main Force 300-13 characteristics is listed under Table 5.

Table 5 Main characteristics of the Force 300-13 Series

Characteristic	Value
Topology	PMP, PTP
Wireless link condition	LOS
Scheduler	TDD

Characteristic	Value
Connectivity	Ethernet
Operating frequencies	Unlicensed bands, 5 GHz
Channel bandwidth	20 MHz, 40 MHz, 80 MHz
Data rate	Up to 600+ Mbps

Typical installation Equipment

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

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

- ePMP Force 425 Access Point: A connectorized outdoor transceiver unit containing all the radio, networking, and surge suppression electronics.
- ePMP Force 400C Access Point: A connectorized IP67 outdoor transceiver unit containing all the radio, networking, and surge suppression electronics.
- ePMP Force 425/400C Access Point Power Supply: An indoor power supply module providing Power-over-Ethernet (PoE) supply and 1000 / 100 Base-TX to the Access Point.
- ePMP Force 425/400C Access Point Radio Cabling and Lightning Protection: Shielded Cat5e cables, grounding cables, surge suppressors, and connectors.
- ePMP Smart Antenna and cabling (optional): For Smart Beamforming, dynamically creates a narrow, targeted beam to each subscriber
- Force 300-25/Force 300-19/Force 300-19R/Force 300-16/Force 300-13/Force 300-CSM Integrated Radio: Integrated outdoor transceiver units containing all the radio, networking, and surge suppression electronics.
- Force 300-25/Force 300-19/Force 300-19R/Force 300-16/Force 300-13/Force 300-CSM Power Supply: An indoor power supply module providing Power-over-Ethernet (PoE) supply and 100/1000 Base-T to the Force 300-25 device.
- Force 300-25/Force 300-19/Force 300-19R/Force 300-16/Force 300-13/Force 300-CSM Radio Cabling and Lightning Protection: Shielded Cat5e cables, grounding cables, surge suppressors, and connectors.

For more information about these components, including interfaces, specifications, and Cambium part numbers, see System hardware on page " System hardware" on page 34.

Wireless operation

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

MU-MIMO

The ePMP Force 425 MU-MIMO access point features an array of antennas. When multiple subscriber modules wish to communicate, the array is divided such that some antennas are used to communicate with

one subscriber, while other antennas are used to communicate with another subscriber – simultaneously.

This is a contrast to a traditional wireless system, where two subscribers cannot communicate on the same channel to the same access point at the same time without causing significant self-interference and degrading the overall wireless network performance.

MIMO

Multiple-Input Multiple-Output (MIMO) technique provides protection against fading and increases the probability of a received decoded signal to be usable.

Smart Beamforming (ePMP Force series)

ePMP Force Smart Beamforming drastically reduces the effects of on-channel interference. The System learns the locations of each served Subscriber Module and forms a narrow beam towards the desired Subscriber Module while that radio is transmitting in the uplink. This reduces the gain on the uplink for on-channel interferers that are transmitting at an azimuth angle different than the Subscriber Module.

Smart Antenna key advantages:

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

Time-division duplexing

TDD cycle

ePMP links operate using Time Division Duplexing (TDD). The links employ a TDD cycle in which the Access Point determines which Subscriber Modules 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.

OFDM and channel bandwidth

ePMP Force 425 transmits using Orthogonal Frequency Division Multiplexing (OFDM). This wideband signal consists of many equally spaced sub-carriers. Although each subcarrier is modulated at a low rate using conventional modulation schemes, the resultant data rate from all the sub-carriers is high.

The channel bandwidth of the OFDM signal is 20 MHz, 40 MHz or 80 MHz, based on operator configuration.

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

Adaptive modulation

ePMP Force 425 can transport data over the wireless link using a number of different modulation modes ranging from 256-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 256-QAM will transport data at a much higher rate than the less complex modulation modes, the receiver requires a much higher signal to noise ratio.

ePMP Force 425 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.

Radar avoidance

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

To meet this requirement, 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 that requires DFS, ensure that the AP is configured with alternate frequencies and that the SM is configured to scan for these frequencies to avoid long outages.

Encryption

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

Country codes

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

Country codes affect the following aspects of wireless operation:

- Maximum transmit power
- Radar avoidance (future release)
- Frequency range

Attention

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

Further reading on the wireless operation

For information on planning wireless operation, see:

- The regulatory restrictions that affect radio spectrum usages, such as frequency range and radar avoidance are described under Radio spectrum planning on page "Radio spectrum planning" on page 76.
- The factors to be taken into account when planning links such as range, path loss, and data throughput are described under Link planning on page "Link planning" on page 78.
- The safety specifications against which the ePMP has been tested are listed under Compliance with safety standards on page "For up-to-date data, please refer to:" on page 231. It also describes how

to keep RF exposure within safe limits.

- How ePMP complies with the radio regulations that are enforced in various countries is explained in Compliance with radio regulations on page "Compliance with radio regulations" on page 241.

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

- The configuration parameters of the ePMP devices described under Using the menu options on page "Using the menu options" on page 88.
- Post- installation procedures and troubleshooting tips are explained under Operation and Troubleshooting on page " Operation and Troubleshooting" on page 159.

System management

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

Management agent

ePMP equipment is managed through an embedded management agent. Management workstations, network management systems or PCs can be connected to this agent using the module's Ethernet port, SFP port, over the air (Subscriber Module connection via Access Point) or by using the device WiFi management interface.

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)
- cnMaestro™ Cloud-based or On-premises Management System
- Dynamic Host Configuration Protocol (DHCP)

Webserver

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.

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 CMM module or an NTP server configured in the system’s management network.

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

Software upgrade

Software upgrades may be issued via the radio web interface (Tools > Software Upgrade) or via cnMaestro (cloud.cambiumnetworks.com). For software upgrades, see

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

Further reading on system management

For more information on system management, see Operation and Troubleshooting on page " Operation and Troubleshooting" on page 159

Chapter 2: System hardware

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

The following topics are described in this chapter:

- Factors to be considered when planning the proposed network is described under Site planning on page "Site planning" below.
- The ePMP Force 425 Access Point hardware, part numbers, mounting equipment, and specifications are described under ePMP Force 425 Access Point on page "ePMP Force 425 Access Point" on page 37.
- The Force 300-25 module hardware, part numbers, mounting equipment, and specifications are described under Force 300-25 on page "Force 300-25" on page 47.
- The Force 300-16 module hardware, part numbers, mounting equipment, and specifications are described under Force 300-19 on page "Force 300-19" on page 52.
- The power supply hardware, part numbers, and specifications are described under Power Supply on page "Power Supply" on page 69.
- Cable standards and lengths are described under Ethernet cabling on page "Ethernet cabling" on page 71.
- Surge suppression requirements and recommendations are described under Surge suppression unit on page "Surge suppression unit" on page 73.

Site planning

Conduct a site survey to ensure that the proposed 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 devices.

Find a location for the device 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 "Calculated distances and power compliance margins" on page 234.
- The equipment is lower than the top of the supporting structure (tower, mast or building) or its lightning air terminal.
- There is one Ethernet interface, a copper Cat5e connection from the device to the power supply and network terminating equipment.

Grounding and lightning protection

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

Warning

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

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

Note

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

Figure 1 Access Point installation diagram

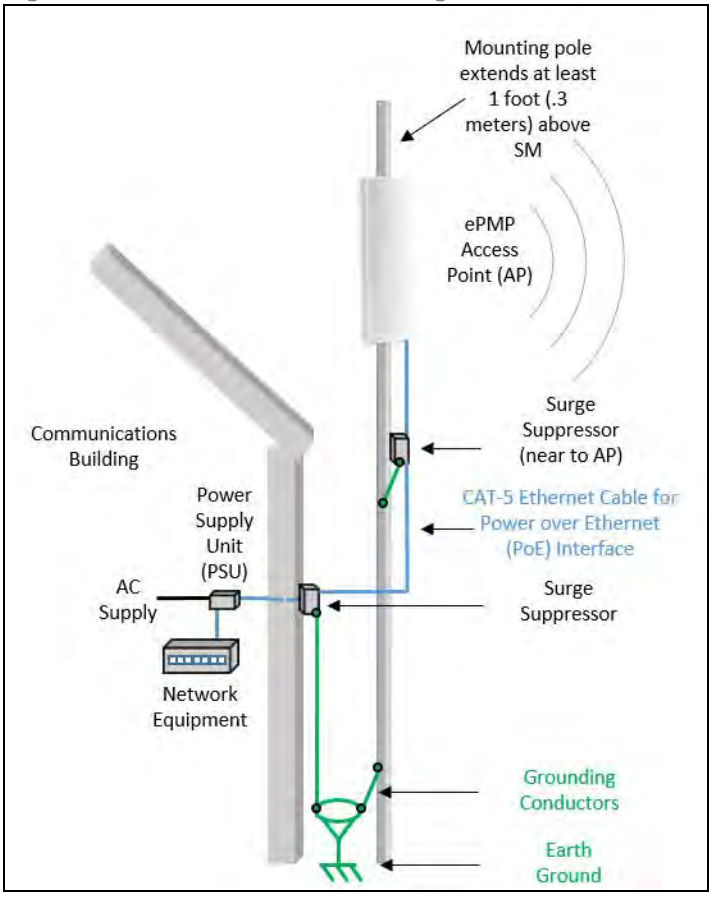
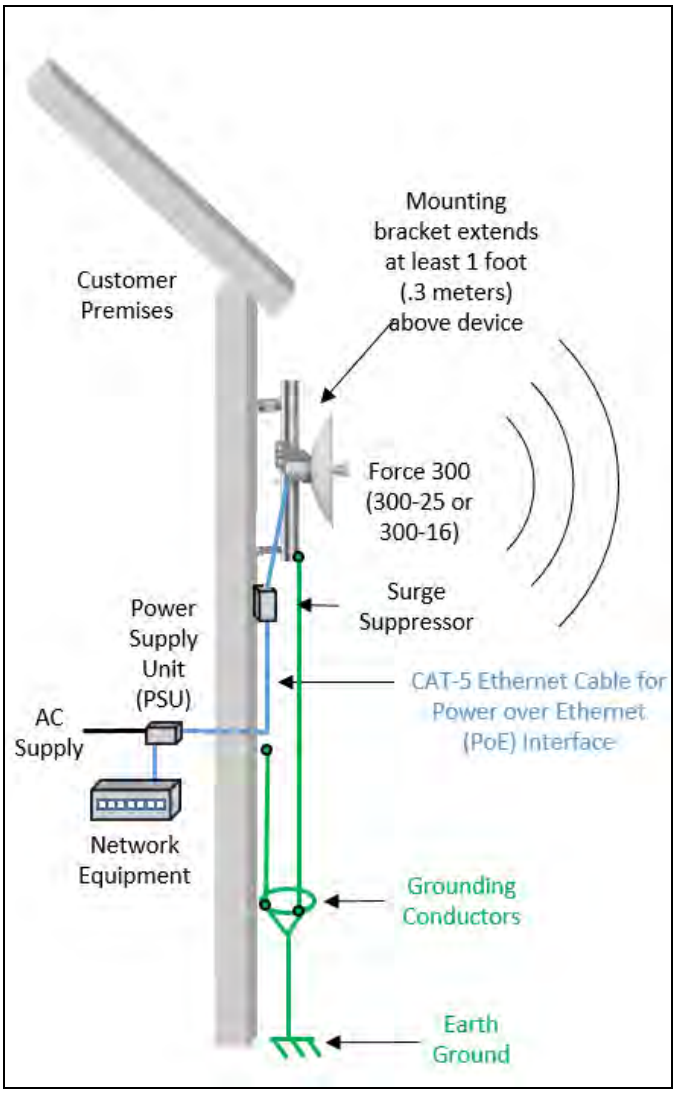


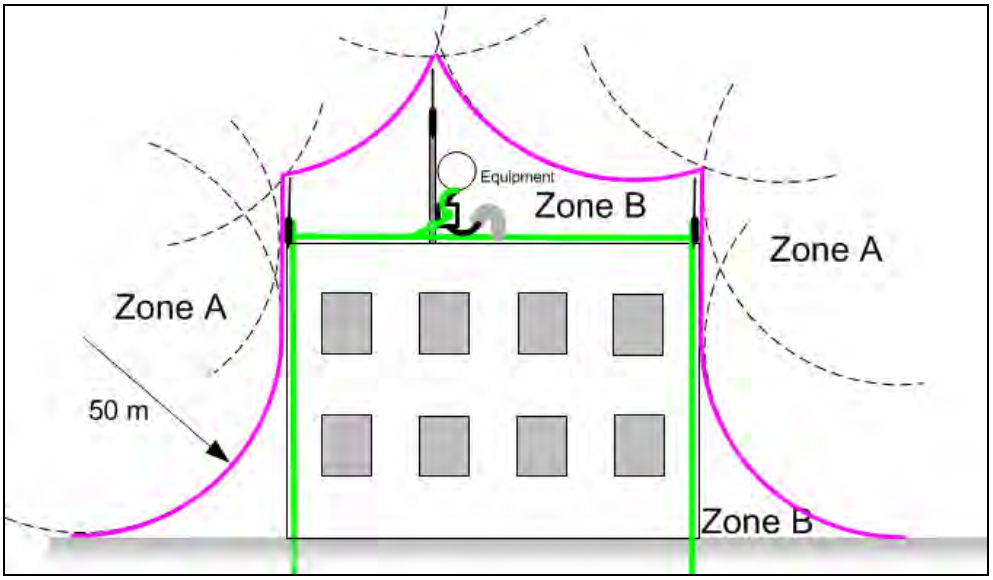
Figure 2 Subscriber / Point-to-Point installation diagram



Lightning protection zones

Use the rolling sphere method (Figure 3 Rolling sphere method to determine the lightning protection zones) 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 3 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

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

ePMP Force 425 Access Point

For details of the ePMP Force 425 Access Point hardware, see:

- ePMP Force 425 Access Point description on page "ePMP Force 425 Access Point description" on the next page
- ePMP Force 425 Access Point part numbers on page "ePMP Force 425 Access Point part numbers" on the next page
- ePMP Force 425 Access Point mounting bracket on page "ePMP Force 425 Access Point mounting bracket" on page 39
- ePMP Force 425 Access Point Interfaces on page "ePMP Force 425 Access Point Interfaces" on page 40
- ePMP Force 425 Access Point specifications on page "ePMP Force 425 Access Point specifications" on page 40

ePMP Force 425 Access Point description

The ePMP Force 425 device is a self-contained transceiver unit that houses both radio and networking electronics.	Figure 4 ePMP Force 425 Access Point

ePMP Force 425 Access Point part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed in Table 22 Force 300-25 part numbers includes the following items:

- One connectorized unit
- One power supply 1000/100 Base-TX LAN injector (excluding C050910AZ01A, C050910D301A)
- One line cord (excluding C050910A001A, C050910AZ01A, C050910D301A)

Table 6 ePMP Force 425 Access Point part numbers

Cambium description	Cambium part number
ePMP Force 425 5 GHz Access Point Radio (FCC) (US cord)	C058910A102A
ePMP Force 425 5 GHz Access Point Radio (IC) (Canada/US cord)	C050910A104A
ePMP Force 425 5 GHz Access Point Radio (EU) (EU cord)	C050910A203A
ePMP Force 425 5 GHz Access Point Radio (EU) (UK cord)	C050910A303A
ePMP Force 425 5 GHz Access Point Radio (ROW) (no cord)	C050910A001A
ePMP Force 425 5 GHz Access Point Radio (ROW) (US cord)	C050910A101A
ePMP Force 425 5 GHz Access Point Radio (ROW) (EU cord)	C050910A201A
ePMP Force 425 5 GHz Access Point Radio (ROW) (UK cord)	C050910A301A
ePMP Force 425 5 GHz Access Point Radio (ROW) (India cord)	C050910A401A

Cambium description	Cambium part number
ePMP Force 425 5GHz Access Point Radio (India) (India Cord)	C050910A402A
ePMP Force 425 5 GHz Access Point Radio (ROW) (China cord)	C050910A501A
ePMP Force 425 5 GHz Access Point Radio (ROW) (Brazil cord)	C050910A601A
ePMP Force 425 5 GHz Access Point Radio (ROW) (Argentina cord)	C050910A701A
ePMP Force 425 5 GHz Access Point Radio (ROW) (ANZ cord)	C050910A801A
ePMP Force 425 5 GHz Access Point Radio (ROW) (South Africa cord)	C050910A901A
ePMP Force 425 5 GHz Access Point Radio (ROW) (No PSU)	C050910AZ01A
ePMP 4x4 MU-MIMO Sector Antenna (for ePMPForce 425AP)	C050910D301A

Table 7 ePMP Force 425 accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

ePMP Force 425 Access Point mounting bracket

The ePMP 3000 Access Point module is designed to be mounted with a sector antenna or pole-mounted using the mounting bracket provided in the box with the radio.	Figure 5 ePMP Force 425 Access Point module mounting bracket

ePMP Force 425 Access Point Interfaces

The Ethernet port is located on the bottom of the unit. This interface is described in Table 8 ePMP Force 425 Series – rear interfaces.

Table 8 ePMP Force 425 Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE)
		100/1000BASE-T Ethernet	Data
SFP	SFP	Optical or Copper Gigabit Ethernet	Management and/or data

ePMP Force 425 Access Point specifications

The ePMP Force 425 connectorized module conforms to the specifications listed in Table 9 ePMP Force 425 Access Point physical specifications and Table 10 ePMP Force 425 Access Point environmental specifications.

The connectorized module meets the low- level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 9 ePMP Force 425 Access Point physical specifications

Category	Specification
Dimensions (Length x Width x Height)	22.2 cm x 12.4 cm x 4.5 cm (8.75 in x 4.9 in x 1.75 in) without brackets
Weight	0.7 kg (1.5 lbs) without brackets

Table 10 ePMP Force 425 Access Point environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)
Wind loading	124 mph (200 kph) maximum. See Table 12 ePMP Force 425 Access Point wind loading (Kg) on page "Table 12 ePMP Force 425 Access Point wind loading (Kg)" on the next page for a full description.
Humidity	95% condensing
Environmental	IP55

ePMP Force 425 Access Point heater

At startup, if the ePMP Force 425 Access Point 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 the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 27 Force 300-25 startup times based on ambient temperature.

Table 11 ePMP Force 425 Access Point startup times based on ambient temperature

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

ePMP Force 425 Access Point wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 200 kph (124 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	the surface area in square meters
V	wind speed in meters per second

Force (in pounds) = $0.0042_{AV}2$

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 12 ePMP Force 425 Access Point wind loading (Kg) and Table 13 ePMP Force 425 Access Point wind loading (lb).

Table 12 ePMP Force 425 Access Point wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)		
		40	50	60
ePMP Force 425 Access Point with Sector Antenna	0.13	21.74 Kg	33.96 Kg	48.91 Kg

Table 13 ePMP Force 425 Access Point wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
ePMP Force 425 Access Point with Sector Antenna	1.4	37.63 lb	58.80 lb	84.67 lb

ePMP Force 425 Access Point software packages

ePMP Force 425 Access Point devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4-2.GA.img (or higher version number)

ePMP Force 400C Access Point

For details of the ePMP Force 400C Access Point hardware, see:

- ePMP Force 425 Access Point description ePMP Force 400C Access Point description on page"ePMP Force 400C Access Point description" on the next page
- ePMP Force 400C Access Point part numbers on page "ePMP Force 400C Access Point part numbers" on the next page
- ePMP Force 400C Access Point mounting bracket on page "ePMP Force 400C Access Point mounting bracket" on page 44
- ePMP Force 400C Access Point Interfaceson page"ePMP Force 400C Access Point Interfaces" on page 45

- ePMP Force 400C Access Point specifications on page "ePMP Force 400C Access Point specifications" on page 45

ePMP Force 400C Access Point description

The ePMP Force 400C device is a self-contained transceiver unit that houses both radio and networking electronics.	Figure 6 ePMP Force 400C Access Point

ePMP Force 400C Access Point part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed in Table 22 Force 300-25 part numbers includes the following items:

- One connectorized unit
- One power supply 100/1000BaseT, rate auto negotiated, 802.3at compliant & Aux SFP port
- One line cord (excluding C050910A001A, C050910AZ01A, C050910D301A)

Table 14 ePMP Force 400C Access Point part numbers

Cambium description	Cambium part number
ePMP 3000L 5 GHz Access Point Radio (FCC) (US cord)	C058910A122A
ePMP 3000 5 GHz Access Point Radio (IC) (Canada/US cord)	C050910A124A
ePMP 3000 5 GHz Access Point Radio (EU) (EU cord)	C050910A223A
ePMP 3000 5 GHz Access Point Radio (EU) (UK cord)	C050910A323A
ePMP 3000 5 GHz Access Point Radio (ROW) (no cord)	C050910A021A
ePMP 3000 5 GHz Access Point Radio (ROW) (US cord)	C050910A121A
ePMP 3000 5 GHz Access Point Radio (ROW) (EU cord)	C050910A221A
ePMP 3000 5 GHz Access Point Radio (ROW) (UK cord)	C050910A321A
ePMP 3000 5 GHz Access Point Radio (ROW) (India cord)	C050910A421A

Cambium description	Cambium part number
ePMP 3000 5GHz Access Point Radio (India) (India Cord)	C050910A422A
ePMP 3000 5 GHz Access Point Radio (ROW) (China cord)	C050910A521A
ePMP 3000 5 GHz Access Point Radio (ROW) (Brazil cord)	C050910A621A
ePMP 3000 5 GHz Access Point Radio (ROW) (Argentina cord)	C050910A721A
ePMP 3000 5 GHz Access Point Radio (ROW) (ANZ cord)	C050910A821A
ePMP 3000 5 GHz Access Point Radio (ROW) (South Africa cord)	C050910A921A
ePMP 3000 5 GHz Access Point Radio (ROW) (No PSU)	C050910AZ21A
ePMP 4x4 MU-MIMO Sector Antenna (for ePMP3000AP)	C050910D321A

Table 15 ePMP 3000L accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

ePMP Force 400C Access Point mounting bracket

The ePMP Force 400C Access Point module is designed to be mounted with a sector antenna or pole-mounted using the mounting bracket provided in the box with the radio.	Figure 7 ePMP Force 425 Access Point module mounting bracket

ePMP Force 400C Access Point Interfaces

The Ethernet port is located on the bottom of the unit. This interface is described in Table 8 ePMP Force 425 Series – rear interfaces.

Table 16 ePMP Force 400C Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE)
		100/1000BASE-T Ethernet	Data
SFP	SFP	Optical or Copper Gigabit Ethernet	Management and/or data

ePMP Force 400C Access Point specifications

The ePMP 3000L connectorized module conforms to the specifications listed in Table 9 ePMP Force 425 Access Point physical specifications and Table 10 ePMP Force 425 Access Point environmental specifications.

The connectorized module meets the low- level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 17 ePMP Force 400C Access Point physical specifications

Category	Specification
Dimensions (Length x Width x	22.2 cm x 12.4 cm x 4.5 cm (8.75 in x 4.9 in x 1.75 in) without

Category	Specification
Height)	brackets
Weight	0.7 kg (1.5 lbs) without brackets

Table 18 ePMP Force 400C Access Point environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)
Wind loading	124 mph (200 kph) maximum. See Table 12 ePMP Force 425 Access Point wind loading (Kg) on page "Table 12 ePMP Force 425 Access Point wind loading (Kg)" on page 42 for a full description.
Humidity	95% condensing
Environmental	IP67

ePMP Force 400C Access Point heater

At startup, if the ePMP Force 400C Access Point 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 the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 27 Force 300-25 startup times based on ambient temperature.

Table 19 ePMP Force 400C Access Point startup times based on ambient temperature

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

ePMP Force 400C Access Point wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 200 kph (124 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	the surface area in square meters
V	wind speed in meters per second

Force (in pounds) = $0.0042_{Av}2$

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 12 ePMP Force 425 Access Point wind loading (Kg) and Table 13 ePMP Force 425 Access Point wind loading (lb).

Table 20 ePMP Force 400C Access Point wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)		
		40	50	60
ePMP Force 400C Access Point with Sector Antenna	0.13	21.74 Kg	33.96 Kg	48.91 Kg

Table 21 ePMP Force 400C Access Point wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
ePMP Force 400C Access Point with Sector Antenna	1.4	37.63 lb	58.80 lb	84.67 lb

ePMP Force 400C Access Point software packages

ePMP Force 400C Access Point devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4-2.GA.img (or higher version number)

Force 300-25

For details of the Force 300-25 hardware, see:

- Force 300-25 Integrated description on page "Force 300-25 Integrated description" on the next page
- Force 300-25 part numbers on page "Force 300-25 part numbers" on the next page

- Force 300-25 mounting bracket on page "Force 300-25 mounting bracket" on the next page
- Force 300-25 specifications on page "Force 300-25 specifications" on page 50
- Force 300-25 heater on page " Force 300-25 heater" on page 51
- Force 300-25 wind loading on page "Force 300-25 wind loading" on page 51
- Force 300-25 software packages on page "Force 300-25 software packages" on page 52

Force 300-25 Integrated description

The Force 300-25 device is a self-contained transceiver unit that houses both radio and networking electronics.

Figure 8 Force 300-25 Integrated

Force 300-25 part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed in Table 22 Force 300-25 part numbers includes the following items:

- One integrated unit
- One power supply 1000/100 Base-TX LAN injector (excluding C050910CZ01A)
- One line cord (excluding C050910CA01A, C050910CZ01A)

Table 22 Force 300-25 part numbers

Cambium description	Cambium part number
ePMP Force 300-25-25 5 GHz High Gain Radio (FCC) (US Cord)	C058910C102A
ePMP Force 300-25-25 5 GHz High Gain Radio (IC) (Canada/US Cord)	C050910C104A
ePMP Force 300-25-25 5 GHz High Gain Radio (EU) (EU Cord)	C050910C203A
ePMP Force 300-25-25 5 GHz High Gain Radio (EU) (UK Cord)	C050910C303A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (no Cord)	C050910C001A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (US Cord)	C050910C101A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (EU Cord)	C050910C201A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (UK Cord)	C050910C301A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (India Cord)	C050910C401A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (China Cord)	C050910C501A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (Brazil Cord)	C050910C601A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (Argentina Cord)	C050910C701A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (ANZ Cord)	C050910C801A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (South Africa Cord)	C050910C901A
ePMP Force 300-25-25 5 GHz High Gain Radio (RoW) (No PSU)	C050910CZ01A

Table 23 Force 300-25 accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

Force 300-25 mounting bracket

The Force 300-25 module is designed to be pole-mounted using the mounting bracket provided in the box with the radio. Figure 9

Force 300- 25 module mounting bracket

Force 300-25 Interfaces

The Ethernet port is located on the rear of the integrated unit. This interface is described in Table 24 Force 300-25 Series – rear interfaces.

Table 24 Force 300-25 Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE).
		100/1000BASE-T Ethernet	Data

Force 300-25 specifications

The Force 300-25 integrated module conforms to the specifications listed in Table 25 Force 300-25 physical specifications and Table 26 Force 300-25 environmental specifications.

The integrated module meets the low-level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 25 Force 300-25 physical specifications

Category	Specification
Dimensions (Diameter x Depth)	47 cm x 31 cm (18.5 in x 12.2 in)
Weight	2.4 kg (5.2 lbs)

Table 26 Force 300-25 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +55°C (131°F)
Wind loading	124 mph (200 kph) maximum. See Force 300-25 wind loading on page "Force 300-25 wind loading" on the next page for a full description.
Humidity	95% condensing
Environmental	IP55

Force 300-25 heater

At startup, if the Force 300-25 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 the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated, and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 27 Force 300-25 startup times based on ambient temperature.

Table 27 Force 300-25 startup times based on ambient temperature

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

Force 300-25 wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 200 kph (124 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	the surface area in square meters
V	wind speed in meters per second

Force (in pounds) = $0.0042_{Av}2$

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 28 Force 300-25 wind loading (Kg) and Table 29 Force 300-25 wind loading (lb).

Table 28 Force 300-25 wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second) 40	50	60
Force 300-25 Integrated	0.15	25.08 Kg	39.2 Kg	56.43 Kg

Table 29 Force 300-25 wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
Force 300-25 Integrated	1.61	43.28 lb	67.62 lb	97.37 lb

Force 300-25 software packages

Force 300-25 devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4.2-GA.img (or higher version number)

Force 300-19

For details of the Force 300-19(R) hardware, see:

- Force 300-25 Integrated descriptionForce 300-19 Integrated description on page "Force 300-19 Integrated description" below
- Force 300-19 part numbers on page "Force 300-19 part numbers" on the next page
- Force 300-19 mounting bracket on page "Force 300-19 mounting bracket" on the next page
- Force 300-19 specifications on page "Force 300-19 specifications" on page 54
- Force 300-19 heater on page " Force 300-19 heater" on page 54
- Force 300-19 wind loading on page "Force 300-19 wind loading" on page 55
- Force 300-19 software packages on page "Force 300-19 software packages" on page 55

Force 300-19 Integrated description

The Force 300-19 device is a self-contained transceiver unit that houses both radio and networking electronics.
(FCCID:Z8H89FT0048 | IC:109W-0048)

Force 300-19 part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed in Table 20 includes the following items:

- One integrated unit
- One power supply 1000/100 Base-TX LAN injector (excluding C050910CZ01A)
- One line cord (excluding C050910CA01A, C050910CZ01A)

Table 20 Force 300-19 part numbers

Cambium description	Cambium part number
ePMP 5GHz Force 300-19 SM (FCC) (US cord)	C058900C801A
ePMP 5GHz Force 300-19 SM (IC) (Canada/US cord)	C050900C801A
ePMP 5GHz Force 300-19 SM (EU) (EU cord)	C050900C802A
ePMP 5GHz Force 300-19 SM (EU) (UK cord)	C050900C803A
ePMP 5GHz Force 300-19 SM (ROW) (no cord)	C050900C804A
ePMP 5GHz Force 300-19 SM (ROW) (US cord)	C050900C805A
ePMP 5GHz Force 300-19 SM (ROW) (EU cord)	C050900C806A
ePMP 5GHz Force 300-19 SM (ROW) (UK cord)	C050900C807A
ePMP 5GHz Force 300-19 SM (ROW) (India cord)	C050900C808A
ePMP 5GHz Force 300-19 SM (India) (India cord)	C050900C809A
ePMP 5GHz Force 300-19 SM (ROW) (China cord)	C050900C810A
ePMP 5GHz Force 300-19 SM (ROW) (Brazil cord)	C050900C811A
ePMP 5GHz Force 300-19 SM (ROW) (Argentina cord)	C050900C812A
ePMP 5GHz Force 300-19 SM (ROW) (ANZ cord)	C050900C813A
ePMP 5GHz Force 300-19 SM (ROW) (South Africa cord)	C050900C814A
ePMP 5GHz Force 300-19 SM (ROW) (No PSU)	C050900C815A

Table 20 Force 300-19 accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

Force 300-19 mounting bracket

The Force 300-19 module is designed to be pole-mounted using the mounting bracket provided in the box with the radio.

Figure 10 Force 300-19 module mounting bracket

Force 300-19 Interfaces

The Ethernet port is located on the rear of the integrated unit. This interface is described in Table 21.

Table 21 Force 300-19 Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input 100/1000BASE-T Ethernet	Power over Ethernet (PoE). Data

Force 300-19 specifications

The Force 300-19 integrated module conforms to the specifications listed in Table 22 and Table 23.

The integrated module meets the low-level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 22 Force 300-19 physical specifications

Category	Specification
Dimensions	27.8 cm x 27.8 cm x 4.5cm (10.9 in x 10.9 in x 1.8 in)
Weight	1.45 kg (3.2 lbs) (Including mounting bracket)
Antenna Gain	19 dBi

Table 23 Force 300-19 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (140°F)
Wind loading	113 mph (180 kph) maximum. See Force 300-25 wind loading on page "Force 300-25 wind loading" on page 5120 for a full description.
Humidity	95% condensing
Environmental	IP55 for 300-19

Force 300-19 heater

At startup, if the Force 300-19 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 the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 24.

Table 24 Force 300-19 startup times based on ambient temperature

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

Force 300-19 wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 180 kph (113 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	the surface area in square meters
V	wind speed in meters per second

Force (in pounds) = $0.0042_{Av}2$

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 25 and Table 26.

Table 25 Force 300-19 wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)		
		40	50	60
Force 300-19 Integrated	0.08	13.4Kg	20.9Kg	30.1Kg

Table 26 Force 300-19 wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
Force 300-19 Integrated	0.8281	22.3 lb	34.8 lb	50.1 lb

Force 300-19 software packages

Force 300-19 devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4.2-GA.img (or higher version number)

Force 300-19R

For details of the Force 300-19(R) hardware, see:

- Force 300-19R Integrated descriptionon page "Force 300-19R Integrated description" below
- Force 300-19R part numbers on page "Force 300-19R part numbers" below
- Force 300-19R mounting bracket on page "Force 300-19R mounting bracket" on the next page
- Force 300-19R specifications on page "Force 300-19R specifications" on page 58
- Force 300-19R heater on page " Force 300-19R heater" on page 58
- Force 300-19R wind loading on page "Force 300-19R wind loading" on page 59
- Force 300-19R software packages on page "Force 300-19R software packages" on page 59

Force 300-19R Integrated description

The Force 300-19R device is a self-contained transceiver unit that houses both radio and networking electronics.
(FCCID: Z8H89FT0048 | IC:109W-0048)

Force 300-19R part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed in Table 20 includes the following items:

- One integrated unit
- One power supply 1000/100 Base-TX LAN injector (excluding C050910CZ01A)
- One line cord (excluding C050910CA01A, C050910CZ01A)

Table 20 Force 300-19(R) part numbers

Cambium description	Cambium part number
ePMP 5GHz Force 300-19R SM (FCC) (US cord)	C058900C901A
ePMP 5GHz Force 300-19R SM (IC) (Canada/US cord)	C050900C901A
ePMP 5GHz Force 300-19R SM (EU) (EU cord)	C050900C902A
ePMP 5GHz Force 300-19R SM (EU) (UK cord)	C050900C903A
ePMP 5GHz Force 300-19R SM (ROW) (no cord)	C050900C904A
ePMP 5GHz Force 300-19R SM (ROW) (US cord)	C050900C905A
ePMP 5GHz Force 300-19R SM (ROW) (EU cord)	C050900C906A
ePMP 5GHz Force 300-19R SM (ROW) (UK cord)	C050900C907A
ePMP 5GHz Force 300-19R SM (ROW) (India cord)	C050900C908A
ePMP 5GHz Force 300-19R SM (India) (India cord)	C050900C909A
ePMP 5GHz Force 300-19R SM (ROW) (China cord)	C050900C910A
ePMP 5GHz Force 300-19R SM (ROW) (Brazil cord)	C050900C911A
ePMP 5GHz Force 300-19R SM (ROW) (Argentina cord)	C050900C912A
ePMP 5GHz Force 300-19R SM (ROW) (ANZ cord)	C050900C913A
ePMP 5GHz Force 300-19R SM (ROW) (South Africa cord)	C050900C914A
ePMP 5GHz Force 300-19R SM (ROW) (No PSU)	C050900C915A

Table 20 Force 300-19R accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

Force 300-19R mounting bracket

The Force 300-19R module is designed to be pole-mounted using the mounting bracket provided in the box with the radio.

Figure 11 Force 300-19R module mounting bracket

Force 300-19R Interfaces

The Ethernet port is located on the rear of the integrated unit. This interface is described in Table 21.

Table 21 Force 300-19R Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE).
		100/1000BASE-T Ethernet	Data

Force 300-19R specifications

The Force 300-19R integrated module conforms to the specifications listed in Table 22 and Table 23.

The integrated module meets the low-level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 22 Force 300-19R physical specifications

Category	Specification
Dimensions	27.8 cm x 27.8 cm x 4.5cm (10.9 in x 10.9 in x 1.8 in)
Weight	1.45 kg (3.2 lbs) (Including mounting bracket)
Antenna Gain	19 dBi

Table 23 Force 300-19R environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (140°F)
Wind loading	113 mph (180 kph) maximum. See Force 300-25 wind loading on page "Force 300-25 wind loading" on page 5120 for a full description.
Humidity	95% condensing
Environmental	IP67

Force 300-19R heater

At startup, if the Force 300-19(R) module temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated, and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 24.

Table 24 Force 300-19(R) startup times based on ambient temperature

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

Force 300-19R wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 180 kph (113 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 the surface area in square meters
V wind speed in meters per second

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

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 25 and Table 26.

Table 25 Force 300-19R wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second) 40	50	60
Force 300-19 Integrated	0.08	13.4Kg	20.9Kg	30.1Kg

Table 26 Force 300-19R wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour) 80	100	120
Force 300-19 Integrated	0.8281	22.3 lb	34.8 lb	50.1 lb

Force 300-19R software packages

Force 300-19R devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4.2-GA.img (or higher version number)

Force 300-16

For details of the Force 300-16 hardware, see:

- Force 300-16 Integrated description
- Force 300-16 part numbers

- Force 300-16 Interfaces
- Force 300-16 specifications
- Force 300-16 heater
- Force 300-16 software packages

Force 300-16 Integrated description

The Force 300-16 device is a self-contained transceiver unit that houses both radio and networking electronics.

Figure 12 Force 300-16 Integrated

Force 300-16 part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed includes the following items:

- One integrated unit
- One power supply 1000/100 Base-TX LAN injector (excluding C050910CZ11A)
- One line cord (excluding C050910C011A, C050910CZ11A)

Table 27 Force 300-16 part numbers

Cambium description	Cambium part number
ePMP 5 GHz Force 300-16 Radio (FCC) (US cord)	C058910C112A
ePMP 5 GHz Force 300-16 Radio (IC) (Canada/US cord)	C050910C114A
ePMP 5 GHz Force 300-16 Radio (EU) (EU cord)	C050910C213A
ePMP 5 GHz Force 300-16 Radio (EU) (UK cord)	C050910C313A
ePMP 5 GHz Force 300-16 Radio (ROW) (no cord)	C050910C011A
ePMP 5 GHz Force 300-16 Radio (ROW) (US cord)	C050910C111A
ePMP 5 GHz Force 300-16 Radio (ROW) (EU cord)	C050910C211A
ePMP 5 GHz Force 300-16 Radio (ROW) (UK cord)	C050910C311A
ePMP 5 GHz Force 300-16 Radio (ROW) (India cord)	C050910C411A
ePMP 5 GHz Force 300-16 Radio (India) (India cord)	C050910C412A
ePMP 5 GHz Force 300-16 Radio (ROW) (China cord)	C050910C511A
ePMP 5 GHz Force 300-16 Radio (ROW) (Brazil cord)	C050910C611A
ePMP 5 GHz Force 300-16 Radio (ROW) (Argentina cord)	C050910C711A
ePMP 5 GHz Force 300-16 Radio (ROW) (ANZ cord)	C050910C811A

Cambium description	Cambium part number
ePMP 5 GHz Force 300-16 Radio (ROW) (South Africa cord)	C050910C911A
ePMP 5 GHz Force 300-16 Radio (ROW) (No PSU)	C050910CZ11A

Table 28 Force 300-16 accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

Force 300-16 Interfaces

The Ethernet port is located on the rear of the integrated unit.

Table 29 Force 300-16 Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE).
		100/1000BASE-T Ethernet	Data

Force 300-16 specifications

The Force 300-16 integrated module conforms to the specifications listed in Table 30 and Table 31.

The integrated module meets the low-level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 30 Force 300-16 physical specifications

Category	Specification
Dimensions (Diameter x Depth)	12.4 cm x 25.1 cm x 11.9 cm (4.9 in x 9.9 in x 4.7 in) – with mounting bracket
Weight	0.5 kg (1.1 lbs) – with mounting bracket

Table 31 Force 300-16 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (140°F)
Wind loading	112 mph (180 kph) maximum. See Force 300-16 wind loading for a full description.
Environmental	IP55

Force 300-16 heater

At startup, if the Force 300-16 module temperature is at or below 32° F (0° C), an internal heater is activated to ensure that the device can successfully begin operation. The unit's heater is only activated

when the unit is powered on and will not apply heat to the device once the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 32.

Table 32 Force 300-16 startup times based on ambient temperature

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

Force 300-16 wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 180 kph (124 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	the surface area in square meters
V	wind speed in meters per second

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

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 33 and Table 34.

Table 33 Force 300-16 wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)		
		30	40	50
Force 300-16 Integrated	0.03	2.8 Kg	5 Kg	7.8 Kg

Table 34 Force 300-16 wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
Force 300-16 Integrated	0.34	9.1 lb	14.3 lb	20.6 lb

Force 300-16 software packages

Force 300-16 devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4.2-GA.img (or higher version number)

Force 300-13

For details of the Force 300-13 hardware, see:

- Force 300-13 Integrated description
- Force 300-13 part numbers
- Force 300-13 Interfaces
- Force 300-13 specifications
- Force 300-13 heater
- Force 300-13 wind loading
- Force 300-13 software packages

Force 300-13 Integrated description

The Force 300-13 device is a self-contained transceiver unit that houses both radio and networking electronics.

(FCCID:Z8H89FT0048 | IC:109W-0048)

Figure 13 Force 300-13 Integrated

Force 300-13 Interfaces

The Ethernet port is located on the rear of the integrated unit.

Table 37 Force 300-13 Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input 100/1000BASE-T Ethernet	Power over Ethernet (PoE). Data

Force 300-13 specifications

The Force 300-13 integrated module conforms to the specifications listed in Table 38 and Table 39.

The integrated module meets the low-level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 38 Force 300-13 physical specifications

Category	Specification
Dimensions (Diameter x Depth)	12.4 cm x 25.1 cm x 11.9 cm (4.9 in x 9.9 in x 4.7 in) – with mounting bracket
Weight	0.5 kg (1.1 lbs) – with mounting bracket
Antenna Gain	13 dBi

Table 39 Force 300-13 environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60°C (140°F)
Wind loading	112 mph (180 kph) maximum. See Force 300-16 wind loading for a full description.
Environmental	IP55

Force 300-13 heater

At startup, if the Force 300-13 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 the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 40.

Table 40 Force 300-13 startup times based on ambient temperature

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

Force 300-13 wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 180 kph (124 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	the surface area in square meters
V	wind speed in meters per second

Force (in pounds) = $0.0042_{AV}2$

Where: Is:

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 41 and Table 42.

Table 41 Force 300-13 wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)		
		30	40	50
Force 300-16 Integrated	0.03	2.82 Kg	5.02 Kg	7.84 Kg

Table 42 Force 300-13 wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
Force 300-16 Integrated	0.28	7.53 lb	11.76 lb	16.93 lb

Force 300-13 software packages

Force 300-16 devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4.2-GA.img (or higher version number)

Force 300-CSM

For details of the Force 300-CSM hardware, see:

- Force 300-CSM Integrated description
- Force 300-CSM part numbers
- Force 300-CSM Interfaces
- Force 300-CSM specifications
- Force 300-CSM heater
- Force 300-CSM wind loading
- Force 300-CSM software packages

Force 300-CSM Integrated description

The Force 300-CSM device is a self-contained transceiver unit that houses both radio and networking electronics.

Figure 14 Force 300-CSM Integrated

Force 300-CSM part numbers

Choose the correct regional variant to adhere to local licensing restrictions.

Each of the parts listed includes the following items:

- One integrated unit
- One power supply 1000/100 Base-TX LAN injector (excluding C050910CZ11A)
- One line cord (excluding C050910C011A, C050910CZ11A)

Table 35 Force 300-CSM part numbers

Cambium description	Cambium part number
ePMP 5GHz Force 300-CSM SM (FCC) (US cord)	C058910C122A
ePMP 5GHz Force 300-CSM SM (IC) (Canada/US cord)	C050910C124A
ePMP 5GHz Force 300-CSM SM (EU) (EU cord)	C050910C223A
ePMP 5GHz Force 300-CSM SM (EU) (UK cord)	C050910C323A
ePMP 5GHz Force 300-CSM SM (ROW) (no cord)	C050910C021A
ePMP 5GHz Force 300-CSM SM (ROW) (US cord)	C050910C121A
ePMP 5GHz Force 300-CSM SM (ROW) (EU cord)	C050910C221A
ePMP 5GHz Force 300-CSM SM (ROW) (UK cord)	C050910C321A
ePMP 5GHz Force 300-CSM SM (ROW) (India cord)	C050910C421A
ePMP 5GHz Force 300-CSM SM (India) (India cord)	C050910C422A
ePMP 5GHz Force 300-CSM SM (ROW) (China cord)	C050910C521A
ePMP 5GHz Force 300-CSM SM (ROW) (Brazil cord)	C050910C621A
ePMP 5GHz Force 300-CSM SM (ROW) (Argentina cord)	C050910C721A
ePMP 5GHz Force 300-CSM SM (ROW) (ANZ cord)	C050910C821A
ePMP 5GHz Force 300-CSM SM (ROW) (South Africa cord)	C050910C921A
ePMP 5GHz Force 300-CSM SM (ROW) (No PSU)	C050910CZ21A

Table 36 Force 300-CSM accessory part numbers

Cambium description	Cambium part number
PoE Gigabit DC Injector, 15W Output at 30V, Energy Level 6 Supply	N000900L001
CABLE, UL POWER SUPPLY CORD SET, ARGENTINA	N000900L013
CABLE, UL POWER SUPPLY CORD SET, AUS/NZ	N000900L011
CABLE, UL POWER SUPPLY CORD SET, Brazil	N000900L010
CABLE, UL POWER SUPPLY CORD SET, CHINA	N000900L015
CABLE, UL POWER SUPPLY CORD SET, EU	N000900L008
CABLE, UL POWER SUPPLY CORD SET, INDIA	N000900L012
CABLE, UL POWER SUPPLY CORD SET, UK	N000900L009
CABLE, UL POWER SUPPLY CORD SET, US	N000900L007

Force 300-CSM Interfaces

The Ethernet port is located on the rear of the integrated unit.

Table 37 Force 300-CSM Series – rear interfaces

Port name	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE).
		100/1000BASE-T Ethernet	Data

Force 300-CSM specifications

The Force 300-CSM integrated module conforms to the specifications listed in Table 38 and Table 39.

The integrated module meets the low-level static discharge specifications identified in Electromagnetic compatibility (EMC) compliance on page "Electromagnetic compatibility (EMC) compliance" on page 232 and provides internal surge suppression but does not provide lightning suppression.

Table 38 Force 300-CSM physical specifications

Category	Specification
Dimensions (Diameter x Depth)	220mm x 80mm x 25mm (8.7in x 3.15in x 1.0in)
Weight	0.5 kg (1.1 lbs) – with mounting bracket

Table 39 Force 300-CSM environmental specifications

Category	Specification
Temperature	-30°C (-22°F) to +60C (140°F)
Wind loading	112 mph (180 kph) maximum. See Force 300-16 wind loading for a full description.
Environmental	IP67

Force 300-CSM heater

At startup, if the Force 300-13 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 the startup is complete. When the unit temperature is greater than 32° F (0° C), the heater is deactivated and the unit continues its startup sequence.

The effect on device startup time at various temperatures is defined in Table 40.

Table 40 Force 300-CSM startup times based on ambient temperature

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

Force 300-CSM wind loading

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

The device and its mounting bracket are capable of withstanding wind speeds of up to 180 kph (124 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	the surface area in square meters
V	wind speed in meters per second

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

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

Applying these formulae to the ePMP device at different wind speeds, the resulting wind loadings are shown in Table 41 and Table 42.

Table 41 Force 300-CSM wind loading (Kg)

Type of ePMP device	Largest surface area (square meters)	Wind speed (meters per second)		
		30	40	50
Force 300-CSM Integrated	0.03	2.82 Kg	5.02 Kg	7.84 Kg

Table 42 Force 300-CSM wind loading (lb)

Type of ePMP device	Largest surface area (square feet)	Wind speed (miles per hour)		
		80	100	120
Force 300-CSM Integrated	0.28	7.53 lb	11.76 lb	16.93 lb

Force 300-CSM software packages

Force 300-CSM devices may be upgraded by downloading new software packages from the Cambium Networks website or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AC-v4.4.2-GA.img (or higher version number)

Power Supply

For details of the ePMP power supply units, see:

- Power supply description on page "Power supply description" below
- Power supply part numbers on page "Power supply part numbers" below
- Power supply interfaces on page "Power supply interfaces" on the next page
- Power supply specifications on page "Power supply specifications" on page 71
- Power supply location on page "Power supply location" on page 71

Power supply description

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

Attention

All RJ45 Ethernet LAN cables used for providing power or are connected to power ports (PoE) must be UL certified with VW-1 markings.

Attention

Each cnRanger device must be powered by the corresponding power supply. This product is intended to be supplied by a UL Listed Power Supply Unit marked "LPS" or "PS2" and providing power over the Ethernet (PoE)" supply.

Power supply part numbers

Each module requires one power supply and one power supply line cord (line cord included with radio device, see Table 22 Force 300-25 part numbers).

Table 30 Power supply component part numbers

Cambium description	Cambium part number	Device Compatibility
ePMP Pwr Supply for GPS Radio - no cord (spare)	N000900L001	Force 300-25 Force 300-16
POWER SUPPLY, 30W, 56V – Gbps support	N000000L034	ePMP 3000 Access Point

Attention

Each ePMP device must be powered by the corresponding power supply listed in Table 30 Power supply component part numbers.

Power supply interfaces

The power supply interfaces are illustrated in Figure 15 Power supply interfaces and described in Table 31 Power supply interface functions - N000900L001 and Table 33 Power Supply LED functions.

Figure 15 Power supply interfaces

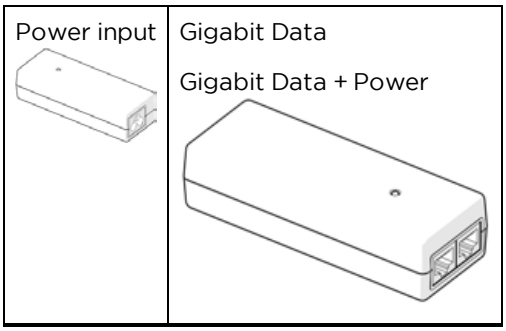


Table 31 Power supply interface functions - N000900L001

Interface	Function
Power input	Mains power input.
Power output	30V
Gigabit Data + Power	RJ45 socket for connecting Cat5e cable to the radio
Gigabit Data	RJ45 socket for connecting Cat5e cable to the network.

Table 32 Power supply interface functions - N000000L034

Interface	Function
Power input	Mains power input.
Power output	56V
Gigabit Data + Power	RJ45 socket for connecting Cat5e cable to the radio. **Note** All RJ45 Ethernet LAN cables used for providing power or are connected to power ports (PoE) must be UL certified with VW-1 markings.
Gigabit Data	RJ45 socket for connecting Cat5e cable to the network.

Table 33 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 34 Power supply physical specifications, Table 35 Power supply environmental specifications, and Table 36 Power supply electrical specifications.

Table 34 Power supply physical specifications

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

Table 35 Power supply environmental specifications

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

Table 36 Power supply electrical specifications

Category	Specification
AC Input	100 to 240 VAC
Efficiency	Meets Energy Level 6
Over Current Protection	Short circuit, with auto-recovery
Hold uptime	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 36 Power supply electrical specifications.

Ethernet cabling

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

- Ethernet standards and cable lengths on page "Ethernet standards and cable lengths" below
- Outdoor Cat5e cable on page "Outdoor Cat5e cable" below

Note

All RJ45 Ethernet LAN cables used for providing power or are connected to power ports (PoE) must be UL certified with VW-1 markings.

Attention

All cables used for outdoor installations must be suitable to be used for that environment and rated accordingly.

Attention

All RJ45 Ethernet LAN cables used for providing power or are connected to power ports (PoE) must be UL certified with VW-1 markings.

Ethernet standards and cable lengths

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

For each power supply, the maximum permitted drop cable length is specified in Table 37 Power supply drop cable length restrictions.

Table 37 Power supply drop cable length restrictions

Part number	Description	Maximum cable length (*1)
N000900L001 N000000L034	Power Supply for Radio with Gigabit Ethernet (no cord)	330 feet (100m)

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

Outdoor Cat5e cable

Cambium Industrial Cable

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

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

The connectors are fully shielded with integrated strain relief for greater pull strength, utilize a staggered contact design that minimizes crosstalk and maximizes electrical performance, and the contacts are

plated with 50 micro-inch thick 24-carat gold, exceeding TIA-1096 specifications and ensuring the best possible connection and oxidation resistance.

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

Table 38 Cambium Industrial Cable component part numbers

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

Surge suppression unit

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.

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

Note

Lightning-prone installations can be improved by:

- Installing a surge suppressor near the device (transient surge suppression)
- Grounding the device to the pole (ground bonding)
- Lowering the device/dish such that it is not the highest metallic object on the pole.

Gigabit Ethernet Surge Suppressor

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

Table 39 Surge suppressor component part numbers

Cambium description	Cambium part number	Device Compatibility
Gigabit Surge Suppressor (30V)	C000000L065A	Force 300-25 Force 300-19(R) Force 300-16 Force 300-13
Gigabit Surge Suppressor (56V)	C000000L033A	ePMP 3000 Access Point

Attention

Choose the 30V or 56V surge suppressor option based on your installed device power rating. Installing a 30V surge suppressor for a 56V device or a 56V surge suppressor for a 30V device may result in inadequate surge protection. Reference Table 39 Surge suppressor component part numbers.

cnPulse sync generator

cnPulse is the latest GPS synchronization generation device designed specifically for Cambium Networks PMP and PTP radios. The cnPulse module is IP67 (weatherproof and supports a wide temperature range for rugged environments. The GPS receiver is highly reliable and supports both GPS and GNSS signals.

cnPulse receives its power from the CAT-5 drop cable in mode 2 so no external power supply is required. There are no configuration or software settings required. For ePMP Force 425, cnPulse is deployed in-line with the radio's CAT-5 drop cable.

For more information, see http://community.cambiumnetworks.com/t5/cnPulse/bd-p/cnPulse

Chapter 3: System planning

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

The following topics are described in this chapter:

- How to plan ePMP links to conform to the regulatory restrictions that apply in the country of operation is explained under Radio spectrum planning on page "Radio spectrum planning" below.
- Factors to be considered when planning links such as range, path loss and throughput are described under Link planning on page "Link planning" on page 78.
- The grounding and lightning protection requirements of an ePMP installation are described under Grounding and lightning protection on page "There is one Ethernet interface, a copper Cat5e connection from the device to the power supply and network terminating equipment. " on page 34.
- Factors to be considered when planning ePMP data networks are described under Data network planning on page "Data network planning" on page 79.

Radio spectrum planning

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

Attention

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

Note

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

General wireless specifications

The wireless specifications that apply to ePMP 802.11ac variants are listed under Table 40 Wireless specifications (all variants). The wireless specifications that are specific to each frequency variant are listed in Table 41 Wireless specifications, 5 GHz band.

Table 40 Wireless specifications (all variants)

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

Item	Specification
Maximum transmit power	ePMP 3000 Access Point: 33 dBm Force 300-25: 29 dBm Force 300-19(R): 28dBm Force 300-16: 29 dBm Force 300-13: 28dBm
Integrated device antenna type	Force 300-25: Dish antenna Force 300-19(R): Integrated patch Force 300-16: Integrated patch Force 300-13: Integrated patch
Duplex scheme	Adaptive TDD
Over- the- air encryption	AES
Error Correction	FEC

Table 41 Wireless specifications, 5 GHz band

Item	5 GHz
RF band (GHz)	4.910 – 5.970 MHz
Channel bandwidth	20 MHz, 40 MHz, or 80 MHz
Typical antenna gain	Integrated dish antenna – 25 dBi Integrated patch antenna – 16 dBi Sector antenna – 17 dBi
Antenna 3dB beamwidth (Integrated dish)	Sector Antenna: 70° azimuth, 6° elevation Integrated Dish: 6-10° azimuth, 6-10° elevation Integrated Patch: 15° azimuth, 30° elevation

Regulatory limits

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

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

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

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

Available spectrum

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

Certain regulations have allocated certain channels as unavailable for use:

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

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 some European countries, the RTTT band 5795 MHz to 5815 MHz is barred. With the appropriate country code configured for this region, the ePMP will not operate on channels within this band.

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

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 operating in ETSI regions, it is required to enter a license key in the ePMP web management interface to unlock valid country- specific frequencies. This key may be obtained from https://support.cambiumnetworks.com/licensekeys/epmp.

Channel bandwidth

Select the required channel bandwidth for the link. The selection depends upon the ePMP frequency variant and country code, as specified on page 1.

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

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

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 the strength of the received signal and the strength that the receiver requires for maintaining a reliable link.

Adaptive modulation

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

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 42 Ethernet bridging specifications.

Table 42 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	10BASE-Te/100BASE-Tx/1000BASE-T IEEE 802.3 IEEE 802.3at (PoE) IEEE802.3u compliant Auto-negotiation

Ethernet Bridging	Specification
Interface	10/100/1000BaseT (RJ-45)
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 device management agent will be connected in a VLAN. If so, decide if this is a standard (IEEE 802.1Q) VLAN or provider bridged (IEEE 802.1ad) VLAN, and select the VLAN ID for this VLAN.

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

Quality of service for bridged Ethernet traffic

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

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

Chapter 4: Using the Device Management Interface

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 "Preparing for configuration" below
- Connecting to the unit on page "Connecting to the unit" below
- Using the web interface on page "Using the web interface" on the next page
- Using the installation wizard – Access Point on page "Using the installation wizard – Access Point" on page 83
- Using the installation wizard – Subscriber Module on page "Using the installation wizard – Subscriber Module" on page 86
- Using the menu options on page "Using the menu options" on page 88

Preparing for configuration

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

Safety precautions

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

Warning

Ensure that personnel is not exposed to unsafe levels of RF energy. The units start to radiate as soon as they are powered up. Respect the safety standards defined in Compliance with safety standards on page "For up-to-date data, please refer to:" on page 231, in particular, the minimum separation distances.

Observe the following guidelines:

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

Regulatory compliance

All applicable radio regulations must be followed while configuring the units and aligning the antennas. For more information, Compliance with safety standards on page "Compliance with safety standards" on page 231.

Connecting to the unit

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

- Configuring the management PC on page "Configuring the management PC" below
- Connecting to the PC and powering up on page "Connecting to the PC and powering up" below

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 169.254.1.x network, avoiding 169.254.1.1. A good example is 169.254.1.100:	
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 (“Gigabit Data+Power” or “10/100Mbit Data+Power”).
	2	Connect the PC Ethernet port to the LAN (“Gigabit Data” or “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 "Testing hardware" on page 160.

Using the web interface

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

- Logging into the web interface on page "Logging into the web interface" below

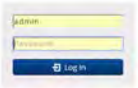
Logging into the web interface

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

Equipment and tools:

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

Procedure:

	1	Check that the device and power supply are correctly connected (the device Ethernet port is connected to the power supply Ethernet power port (“Gigabit Data+Power” or “10/100Mbit Data+Power”).
	2	Configure the host machine with an IP address in the 169.254.1.x subnet (excluding 169.254.1.1)
	3	Connect the PC Ethernet port to the LAN (“Gigabit Data” or “10/100Mbit Data”) port of the power supply using a standard (not crossed) Ethernet cable.
	4	Connect the power supply to power mains
	5	 In your browser, navigate to the device default IP address **169.254.1.1**.
	6	Log in with username **admin** and password **admin**

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 192.168.0.1 (AP Mode), 192.168.0.2 (SM mode) or the previously-configured static Device IP Address. Units may always be accessed via the Ethernet port at 169.254.1.1.

Note

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

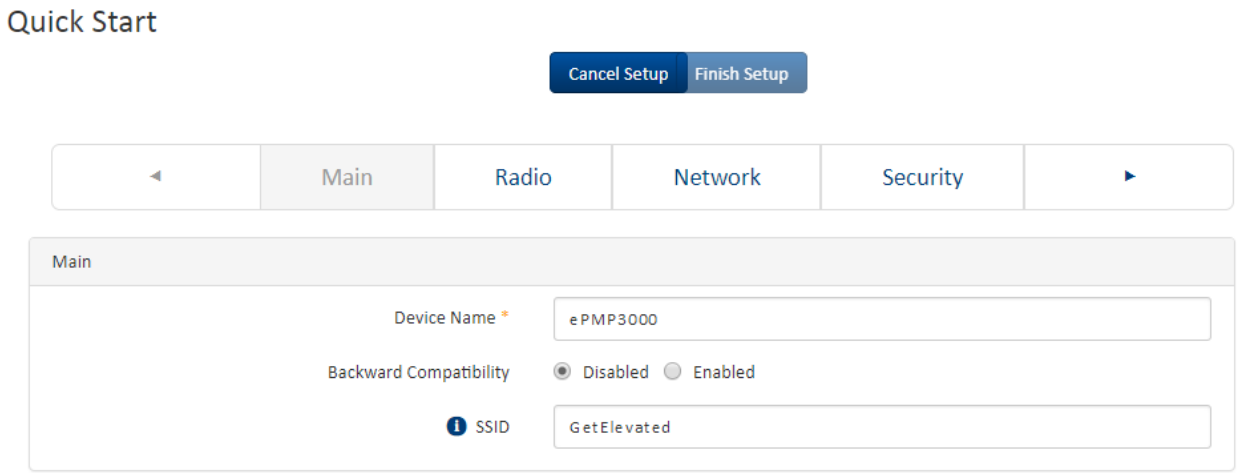
Using the installation wizard – Access Point

The ePMP device features a guided configuration mechanism for configuring key parameters for link operation.

This setup is accessed on the **Installation** page by clicking the **Start Setup** button.

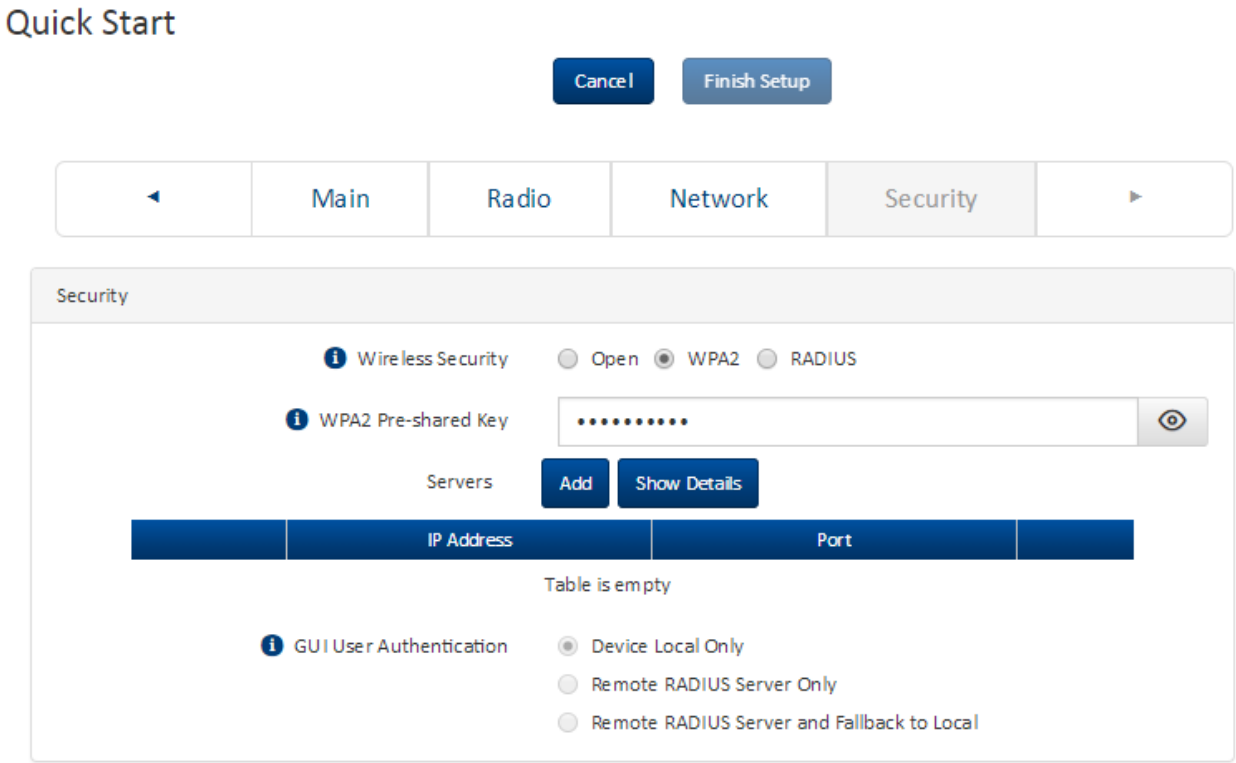
Click **Finish Setup** to commit the changes to the device.

Installation wizard step 1 – Main system parameters



Attribute	Meaning
Main	
Device Name	The configured identifier used in an NMS such as cnMaestro
Backward Compatibility	Enabled: 802.11n ePMP subscribers are able to register to the AP (requires subscriber software upgrade). Disabled: 802.11n ePMP subscribers are not able to register to the AP.
SSID	SSID is a unique identifier for a wireless LAN which is specified in the Access Point's beacon. (Access Point Mode). SSID must be the same at both ends and different to the site name.

Installation wizard step 4 – Security parameters



Attribute	Meaning
Network	
Wireless Security	**Open:** All Subscriber Module devices requesting network entry are allowed registration. **WPA2:** The WPA2 mechanism provides AES radio link encryption and Subscriber Module network entry authentication. When enabled, the Subscriber Module must register using the Authentication Pre-shared Key configured on the Access Point and Subscriber Module. **RADIUS**: Enables Subscriber Module authentication via a pre-configured Radius server.
WPA2 Pre-shared Key	Configure this key on the Access Point, then configure the Subscriber Module with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.
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. The default is 1812. **Secret:** Secret key that is used to communicate with the RADIUS server.
GUI User Authentication	This parameter applies to both the AP and its registered SMs. **Device Local Only:** The device GUI authentication is local to the device using one of the

Attribute	Meaning
	accounts configured under **Configuration > System > Account Management**. **Remote RADIUS Server Only:** The device GUI authentication is performed using a RADIUS server. **Remote RADIUS Server and Fallback to Local:** The device GUI authentication is performed using a RADIUS server. Upon failure of authentication through a RADIUS server, the authentication falls back to one of the local accounts configured under **Configuration > System > Account Management**.

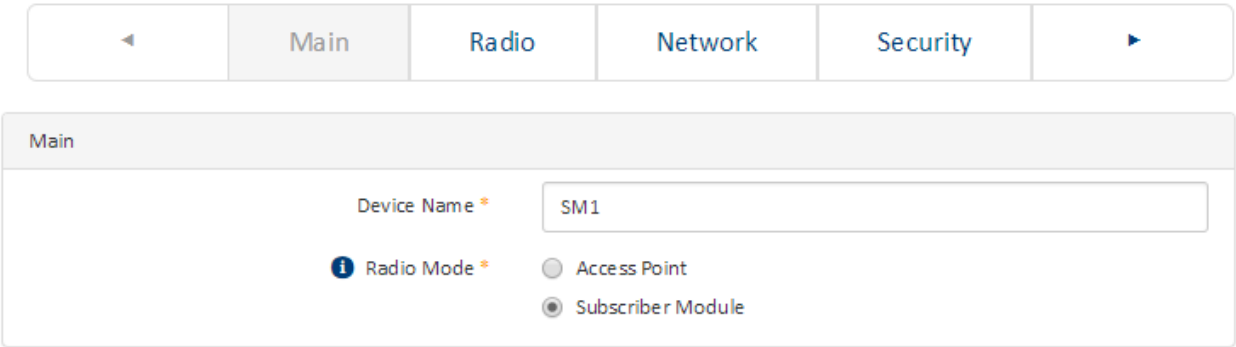
Using the installation wizard – Subscriber Module

The ePMP device features a guided configuration mechanism for configuring key parameters for link operation.

This setup is accessed on the **Installation** page by clicking the **Start Setup** button.

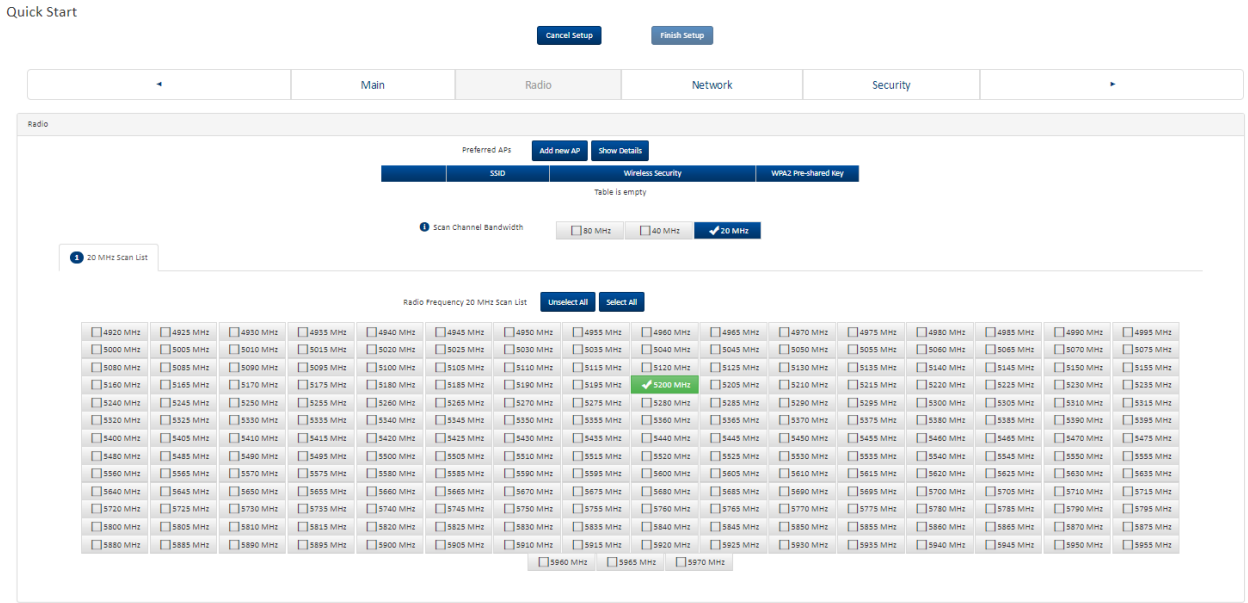
Click **Finish Setup** to commit the changes to the device.

Installation wizard step 1 – Main system parameters



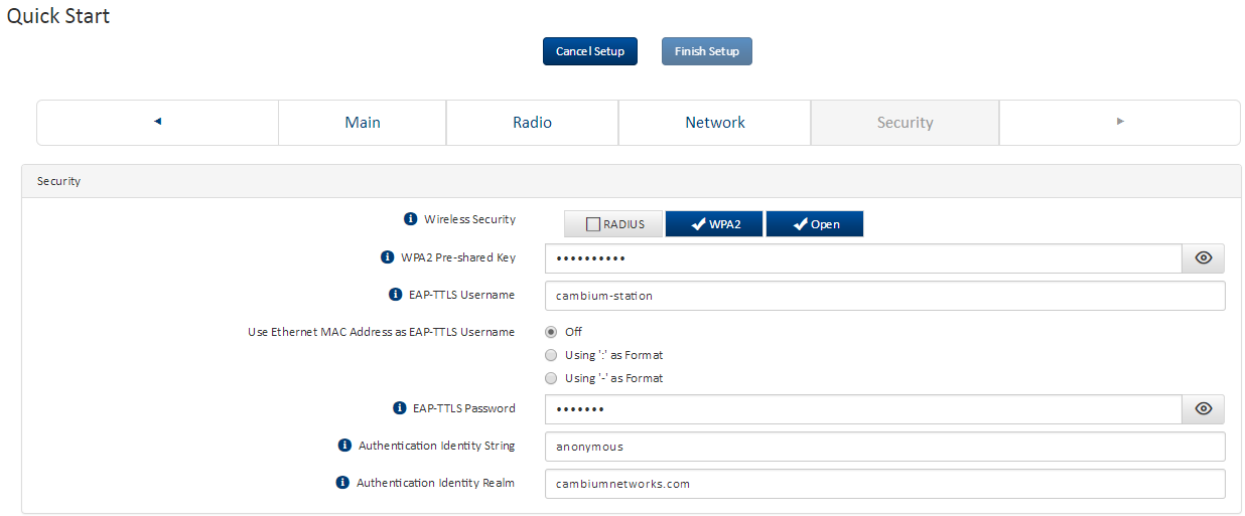
Attribute	Meaning
Main	
Device Name	The configured identifier used in an NMS such as cnMaestro
Radio Mode	This parameter controls the function of the device – All ePMP devices may be configured to operate as an **Access Point** (AP) or a **Subscriber Module** (SM).

Installation wizard step 2 – Radio parameters



Attribute	Meaning
Radio	
Preferred APs	
SSID	The **Preferred Access Points SSID** defines the Access Point SSID to which the Subscriber Module device will attempt registration.
Wireless Security	**Open:** The Subscriber Module device will attempt registration to the Preferred Access Points SSID with no security mechanism. **WPA2**: The WPA2 mechanism provides AES radio link encryption and Subscriber Module network entry authentication. When enabled, the Subscriber Module must register using the Authentication Pre-shared Key configured on the Access Point and Subscriber Module.
WPA2 Pre-shared Key	The **Preferred Access Points WPA2 Pre-shared Key** must be configured on the Subscriber Module device to match the pre-shared key configured on the Access Point for registration with WPA2 security.
Scan Channel Bandwidth	Configure the channel size used by the radio for RF transmission.
Radio Frequency Scan List	Configure the frequency carrier for RF transmission. This list is dynamically adjusted to the regional restrictions based on the setting of the **Country** parameter. Ensure that a thorough spectrum analysis has been completed prior to configuring this parameter.

Installation wizard step 4 – Security parameters



Attribute	Meaning
Network	
EAP-TTLS Username	Configure the EAP-TTLS Username to match the credentials on the RADIUS server being used for the network.
Use Ethernet MAC Address at EAP-TTLS Username	The device MAC Address can be used as the EAP-TTLS Username in either ":" or "-" delimited format.
EAP-TTLS Password	Configure the EAP-TTLS Password to match the credentials on the RADIUS server being used for the network.
Authentication Identity String	Configure this Identity string to match the credentials on the RADIUS server being used for the network. The default value for this parameter is "anonymous".
Authentication Identity Realm	Configure this Identity string to match the credentials on the RADIUS server being used for the network. The default value for this parameter is "cambiumnetworks.com".

Using the menu options

Use the menu navigation bar in the left panel to navigate to each web page. Some of the menu options are only displayed for specific system configurations. Use Table 43 Menu options and web pages to locate information about using each web page.

Table 43 Menu options and web pages

Main menu	Menu option	Web page information
Status		Status page on page "Status page" on page 90

Main menu	Menu option	Web page information
Installation		Installation page on page "Installation page" on page 93
Configuration		Installation page on page "Installation page" on page 93
	Radio	Configuration > Radio page on page "Configuration > Radio page" on page 93
	System	Configuration > System page on page "Configuration > System page" on page 100
	Network	Configuration > Network page on page "Configuration > Network page" on page 105
	Security	Configuration > Security page on page "Configuration > Security page" on page 121
Monitor		Monitor menu on page "Monitor menu" on page 126
	Performance	Monitor > Performance page on page "Monitor > Performance page" on page 127
	System	Monitor > System page on page "Monitor > System page" on page 132
	Wireless	Monitor > Wireless Page on page "Monitor > Wireless Page" on page 134
	Throughput Chart	Monitor > Throughput Chart page on page "Monitor > Throughput Chart page" on page 140
	GPS	Monitor > GPS page (Access Point Mode) on page "Monitor > GPS page (Access Point Mode)" on page 140
	Network	Monitor > Network page on page "Monitor > Network page" on page 142
	System Log	Monitor > System Log Page on page "Monitor > System Log Page" on page 145
Tools		Tools menu on page "Tools menu" on page 145
	Software Upgrade	Tools > Software Upgrade page on page "Tools > Software Upgrade page" on page 145
	Backup / Restore	Tools > Backup/Restore page on page "Tools > Backup/Restore page" on page 147
	License Management	Tools > License Management page (Access Point Mode) on page "Tools > License Management page (Access Point Mode)" on page 149
	Spectrum Analyzer	Tools > Spectrum Analyzer page on page "Tools > Spectrum Analyzer page" on page 151
	eAlign	Tools > eAlign page on page "Tools > eAlign page" on page 153
	Wireless Link Test	Tools > Wireless Link Test page on page "Tools > Wireless Link Test page" on page 154
	Watchdog	Tools > Watchdog page on page "Tools > Watchdog page" on page 155

Main menu	Menu option	Web page information
	Ping	Tools > Ping page on page "Tools > Ping page" on page 156
	Traceroute	Tools > Traceroute page on page "Tools > Traceroute page" on page 157

Status page

Figure 16 Status page

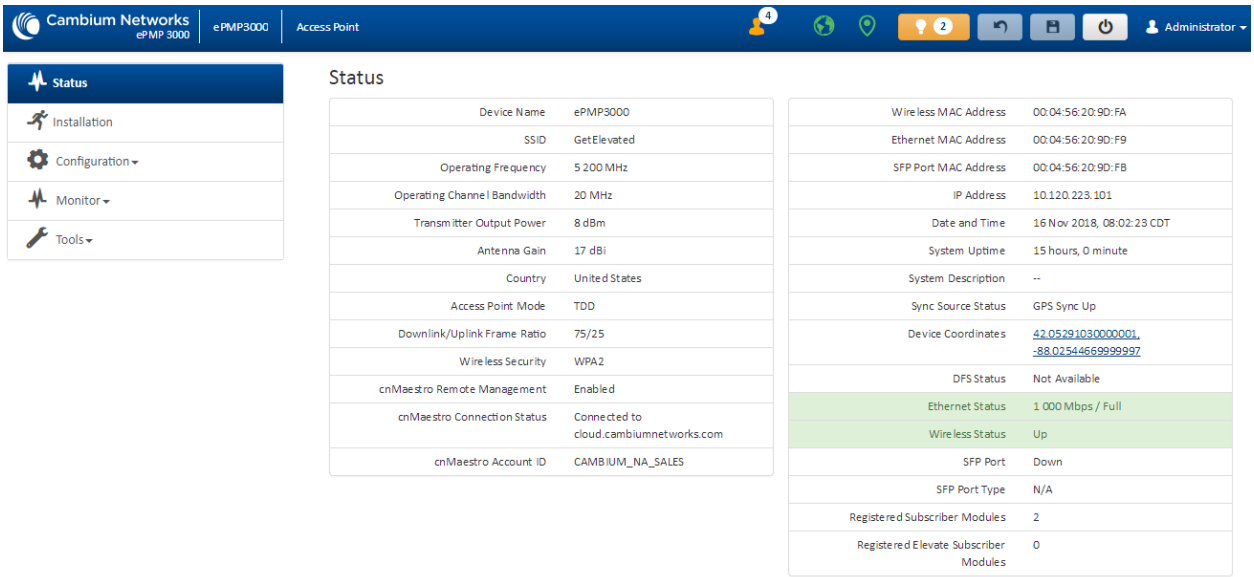


Table 44 Status page attributes

Attribute	Meaning
Device Name	The configured device name of the AP, used for identifying the device in an NMS such as the Cambium Network Services Server (CNSS).
SSID	The current configured name/SSID of the AP.
Operating Frequency	The current frequency carrier used for radio transmission, based on the configuration of the **Frequency Carrier** parameter (in DFS regions, if radar has been detected, this field may display either **DFS Alternate Frequency Carrier 1** or **DFS Alternate Frequency Carrier 2**).
Operating Channel Bandwidth	The current channel bandwidth used for radio transmission, based on the configuration of the **Channel Bandwidth** parameter.
Transmitter Output Power	The current operating transmit power of the AP.
Antenna Gain	The configured gain of the external antenna.

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

Attribute	Meaning
	Time Zone.
System Uptime	The total uptime of the radio since the last reset.
System Description	The current configured system description.
Sync Source Status	Displays the current status of sync timing for the AP.
Device Coordinates	The current configured Latitude and Longitude coordinates in decimal format.
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 the 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.
Ethernet Status	**Up**: The Ethernet (LAN) interface is functioning properly. This also displays the current port speed and duplex mode to which the Ethernet port has auto-negotiated to or configured for. **Down**: The Ethernet (LAN) interface is either disconnected or has encountered an error and is not servicing traffic.
Wireless Status	**Up**: The radio (WAN) interface is functioning properly **Down**: The radio (WAN) interface has encountered an error and is not servicing traffic.
SFP Port	Displays the current port speed and duplex mode to which the SFP port has auto-negotiated, or displays the current port speed and duplex mode that have been configured manually.
SFP Port Type	Displays the type of SFP module connected to the device.
Registered Subscriber Modules	The total number of SMs currently registered to the AP.

Attribute	Meaning
Registered Elevate Subscriber Modules	The total number of ePMP Elevate (third- party software solution) subscribers registered to the AP.

Installation page

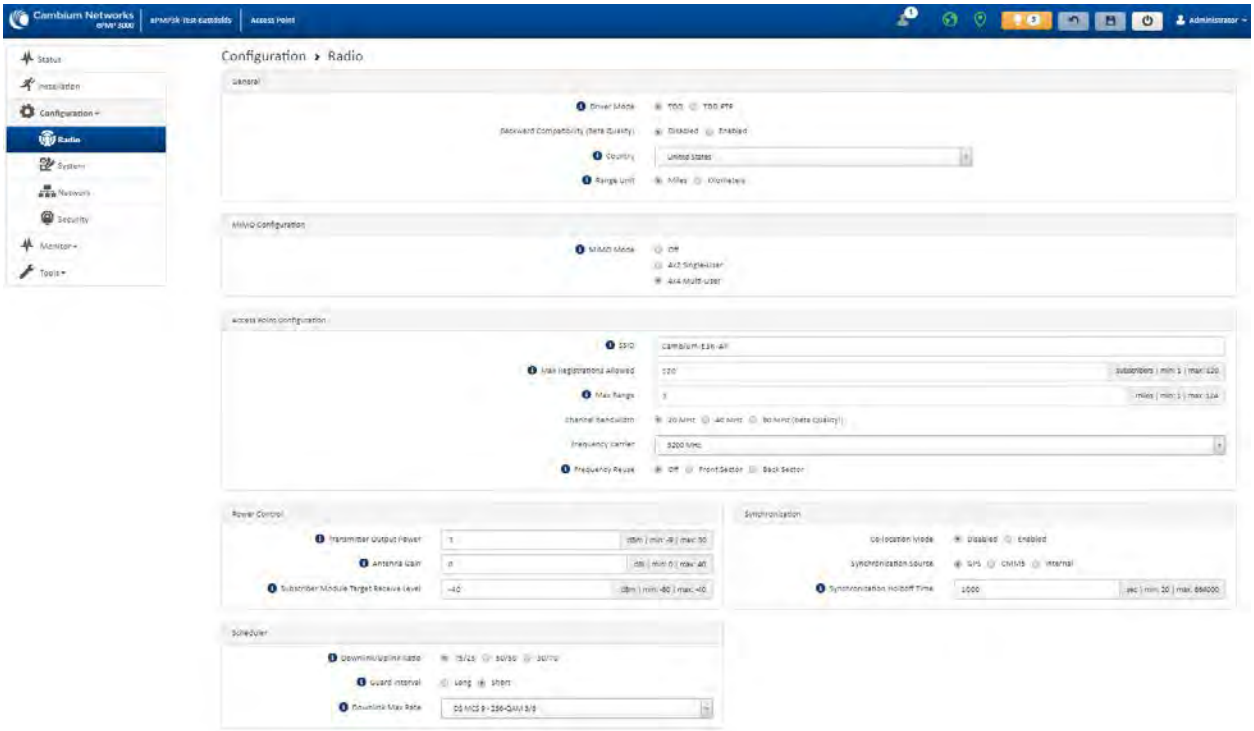
See Using the installation wizard – Access Point on page "Using the installation wizard – Access Point" on page 83 and Using the installation wizard – Subscriber Module on page "Using the installation wizard – Subscriber Module" on page 86.

Configuration menu

Use the **Configuration** menu to access all applicable device configuration parameters.

Configuration > Radio page

Figure 17 Configuration > Radio page (Access Point Mode)



Note

The Trial Configuration allows you to try a configuration change without applying the configuration.

Figure 18 Configuration > Radio page (Subscriber Module Mode)

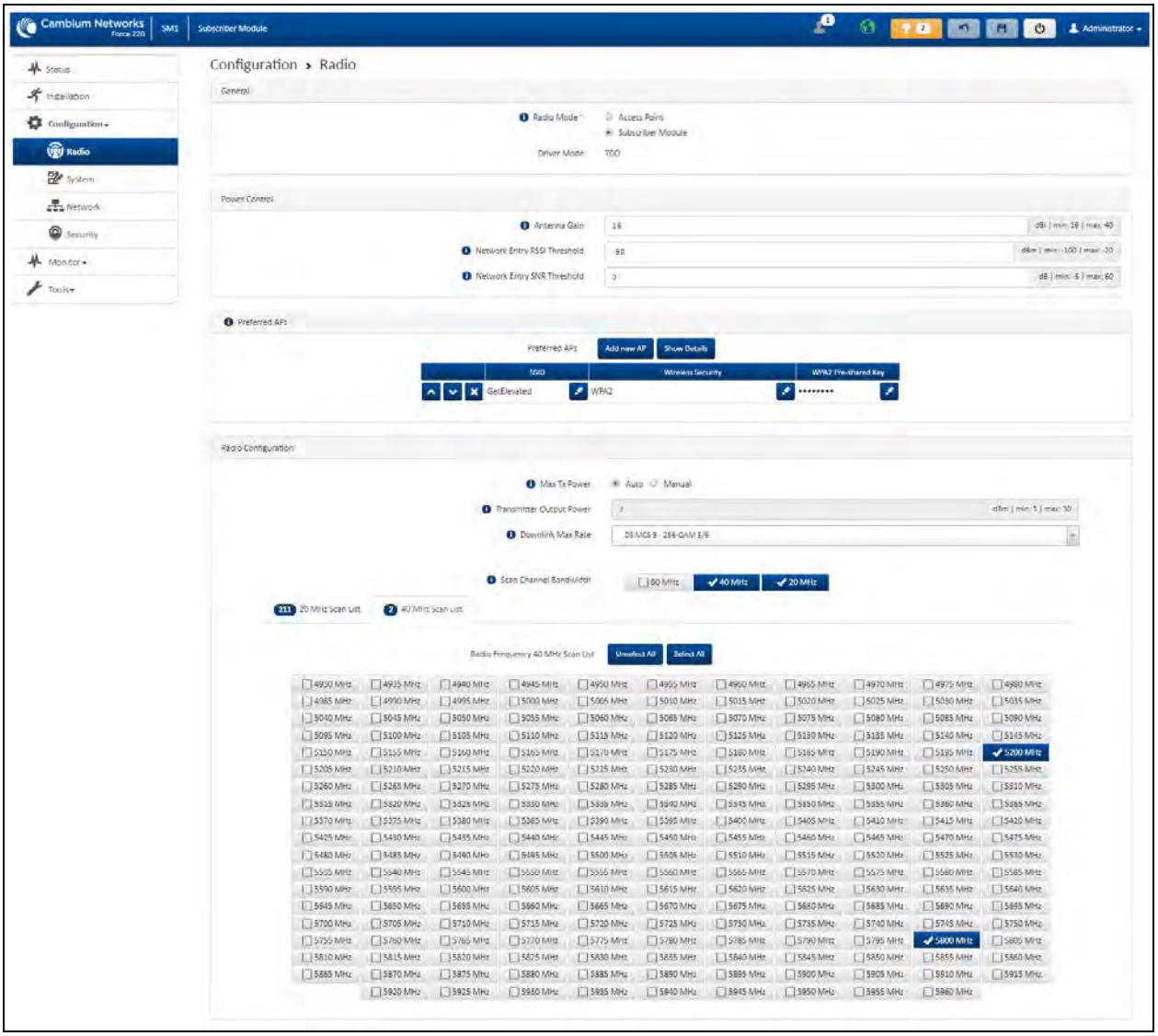
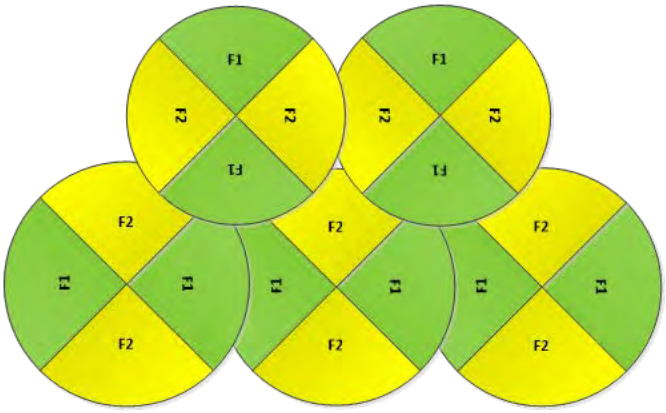


Table 45 Configuration > Radio page attributes

Attribute	Meaning
General	
Driver Mode	**TDD**: The device is operating in point-to-multipoint (PMP) mode using TDD scheduling. The AP is able to GPS synchronize in this mode. **TDD PTP**: The Access Point is operating in point-to-point (PTP) mode using TDD scheduling. The AP is able to GPS synchronize in this mode.
Radio Mode	**Access Point**: The unit controls the point-to-point link and its maintenance. On startup, the Access Point transmits until a link with the Subscriber Module is made. **Subscriber Module**: The unit listens for its peer and only transmits when the peer has

Attribute	Meaning
	been identified.
Backward Compatibility (Access Point Mode)	**Enabled**: 802.11n ePMP subscribers are able to register to the AP (requires subscriber software upgrade). **Disabled**: 802.11n ePMP subscribers are not able to register to the AP.
Country (Access Point Mode)	Defines the country code being used by the device. The country code of the Subscriber Module follows the country code of the associated Access Point unless it is an FCC SKU in which case the country code is the United States or Canada. Country code defines the regulatory rules in use for the device.
Range Unit (Access Point Mode)	Units of measurement on the device are displayed in either miles (m) or kilometers (km).
MIMO Configuration (Access Point Mode)	
MIMO Mode (Access Point Mode)	Downlink beamforming modes based on channel measurement via sounding procedure: **OFF:** Sounding and beamforming are disabled **4x2 Single-User:** Enables Single User beamforming mode based on periodic sounding **4x4 Multi-User:** Extends Single User beamforming mode with MU-MIMO to transmit data frames to 2 subscribers simultaneously
Access Point Configuration (Access Point Mode)	
SSID (Access Point Mode)	SSID is a unique identifier for a wireless LAN which is specified in the Access Point's beacon. (Access Point Mode). SSID must be the same at both ends and different to the site name.
Max Registrations Allowed (Access Point Mode)	Based on sector/network planning and subscriber service level implementations, this parameter allows setting the maximum number of subscribers that are allowed to register/gain network entry. The maximum number of subscribers allowed for each channel bandwidth is as follows: 20/40 MHz: 120 subscribers 10 MHz: 60 subscribers 5 MHz: 30 subscribers The maximum registrations allowed depending on the channel bandwidth of the current Operating Frequency which can be the primary **Frequency Carrier** or one of the alternate Frequency Carriers. For DFS regions, the maximum number of subscribers is based on the channel bandwidth of the current operating channel, i.e. **Frequency Carrier**, **Alternate Frequency Carrier 1** or **Alternate Frequency Carrier 2**. The number of Elevate devices that are allowed to register is specified by the applied license.

Attribute	Meaning
Max Range (Access Point Mode)	This parameter represents the cell coverage radius. Subscriber Modules outside the configured radius will not be able to connect. It is recommended to configure Max Range to match the actual physical distance of the farthest subscriber.
Channel Bandwidth (Access Point Mode)	Configure the channel size used by the radio for RF transmission.
Frequency Carrier (Access Point Mode)	Configure the frequency carrier for RF transmission. This list is dynamically adjusted to the regional restrictions based on the setting of the **Country** parameter. Ensure that a thorough spectrum analysis has been completed prior to configuring this parameter.
Frequency Reuse (Access Point Mode)	The **Frequency Reuse** 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. A network in which two frequencies “F1” and “F2” are reused throughout the installation is shown in Figure 19 Frequency reuse installation. Please note, while CMM3 and CMM4 devices cannot be used as synchronization sources for ePMP 3000, the parameter setting suggestions below server as a guideline for mixed 802.11n and 802.11ac networks. **Figure 19** Frequency reuse installation  The set of APs to configure the **Frequency Reuse** option is dependent on the GPS synchronization sources in the whole network, CMM3, CMM4, CMM5 or GPS. 0B0B The GPS sync source is the same on all APs or is a combination of “GPS”, “CMM4”, “CMM5” In this configuration the GPS synchronization source in the whole network is one of the following: • GPS

Attribute	Meaning
	• CMM4 • CMM5 The rules in selecting the APs to enable the **Frequency Reuse** in this installation are: 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 **Back Sector**; the other AP must be configured with **Frequency Reuse** set to **Front Sector**. Also, APs on different towers facing each other with overlapped coverage must be configured with **Frequency Reuse** set to **Back Sector.** 1B1BThe GPS sync source is a mixture of all types (“CMM3”, “CMM4”, “CMM5” or “GPS”) In this configuration the GPS sync source in the whole network is one of the following: • (CMM3 and GPS) or • (CMM3 and CMM4 / CMM5) or • (CMM3 and CMM4 / CMM5 and GPS) The rules in selecting the APs to configure **Frequency Reuse** to **Frequency Reuse** to **Front Sector** or **Back Sector** in a mixture of sync sources installations are: Only ONE of the APs on the same tower configured with the same frequency must have **Frequency Reuse** set to **Back Sector** if the sync source of both APs is the same or the sync is a combination of GPS and CMM4 / CMM5; the other AP will have the **Front Sector** ON. For the APs on different towers facing each other with overlapped coverage: If both APs have the same sync source then only ONE of them must have the **Back Sector** ON; the other AP shall have the **Front Sector** ON. If one AP has GPS as sync source and the other one has CMM4 / CMM5 then only ONE of them must have **Back Sector** ON; the other AP shall have **Front Sector** ON. If one AP has GPS or CMM4 / CMM5 as sync source and the other one has CMM3 then: If the AP with CMM3 sync source has **Back Sector** ON, then the other AP (with GPS or CMM4 / CMM5 sync source) must have the **Back Sector ON**. If the AP with CMM3 sync source has **Frequency Reuse** set to **Off**, then the other AP (with GPS or CMM4 CMM5 sync source) must have **Frequency Reuse** set to **Off.**
Power Control	
Transmitter Output Power (Access Point Mode)	**Transmitter Output Power** is the total transmit power of the device. The device has four transmit chains and total transmit power sums the power from all chains. This does not include antenna gain. Transmitter Output Power may be limited by regulatory rules for the country in use.
Antenna Gain	The total gain of the antenna in use by the device.

Attribute	Meaning
Subscriber Module Target Receive Level (Access Point Mode)	Defines the desired received power level at the Access Point from the registered Subscriber Module. Access Points use this parameter to control the transmission power of the Subscriber Module in order to reduce system self-interference.
Network Entry RSSI Threshold (Subscriber Module Mode)	This defines the Downlink RSSI threshold below which a Subscriber Module will not register to an Access Point.
Network Entry SNR Threshold (Subscriber Module Mode)	This defines the Downlink Signal-to-Noise-Ratio (SNR) threshold below which the Subscriber Module will not register to an Access Point.
Synchronization (Access Point Mode)	
Co-location Mode (Access Point Mode)	**Disabled:** The ePMP device is able to synchronize only with other ePMP Access Points. **Enabled:** The ePMP device can be configured to synchronize with PMP 100 or PMP 450 series of radios in addition to other ePMP Access Points. Please refer to the ePMP and PMP 100 Co-location and Migration Recommendations Guide for guidance on synchronizing ePMP and PMP 100. Verify that frame size (ms) is configured equally across the co-located installations.
Synchronization Source (Access Point Mode)	**GPS**: Synchronization timing is received via the AP's connected GPS antenna. Co-located or in-range APs receiving synchronization via GPS or CMM transmits and receive at the same time, thereby reducing self-interference. **CMM5**: Synchronization timing is received via the AP's Ethernet port via a connected Cambium Cluster Management Module 5 (CMM5). Co-located or in-range APs receiving synchronization via GPS or CMM will transmit and receive at the same time, thereby reducing self-interference. For more information on CMM configuration, refer to the **PMP Synchronization Solutions User Guide**. If a CMM is being used, verify that the cables from the CMM to the network switch are at most 30 ft (shielded) or 10 ft (unshielded) and that the network switch is not PoE (802.3af). **Internal**: Synchronization timing is generated by the AP and the timing is not based on GPS pulses. APs using Synchronization Source of **Internal** will not transmit and receive in sync with other co-located or in-range APs, which introduces self-interference into the system.
Synchronization Holdoff Time (Access Point	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

Attribute	Meaning
Mode)	signal, the **Synchronization Holdoff** timer is started. During the holdoff interval, all SM registrations are maintained. If a valid GPS synchronization pulse is regained during the holdoff interval, then the AP continues to operate normally. If a valid synchronization pulse is not regained from the GPS source during the holdoff interval, then the AP ceases radio transmission. The default is **30 seconds**.
Preferred Access Points (Subscriber Module Mode)	
Preferred Access Points list (Subscriber Module Mode)	The **Preferred Access Points List** is comprised of a list of up to 16 Access Point devices to which the Subscriber Module device sequentially attempts registration. For each Access Point configured, if authentication is required, enter the **Wireless Security** type and **WPA2 Pre-shared Key** associated with the configured **SSID**.
Scheduler (Access Point Mode)	
Downlink/Uplink Ratio (Access Point Mode)	The schedule of downlink traffic to uplink traffic on the radio link. The 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.
Guard interval (Access Point Mode)	The purpose of the guard interval is to introduce immunity to propagation delays, echoes, and reflections, to which digital data is normally very sensitive. Longer guard periods allow more distant echoes to be tolerated. However, longer guard intervals reduce the channel efficiency.
Downlink Max Rate (Access Point Mode)	Specifies the maximum downlink MCS value that the Rate Adapt algorithm will choose for Radio 1. If an installation is exhibiting packet loss due to downlink interference, modifying **Downlink Max Rate** to limit the device's maximum MCS rate may result in more reliable packet delivery. This is especially true in installations among changing and unpredictable interference.
Radio Configuration	
Max Tx Power (Subscriber Module Mode)	**Auto**: The Access Point can control, using ATPC (Automatic Transmit Power Control), the TX power of the Subscriber Module up to the maximum capability of the Subscriber Module's transmitter (based on regulatory limits). **Manual**: The Access Point can control the TX power of the Subscriber Module up to the value configured in the **Transmitter Power** field.
Transmitter Output Power (Subscriber Module Mode)	The total transmit power of the radio interface. The device has four transmit chains for each channel and total transmit power sums the power from all chains. This does not include antenna gain. Transmitter Output Power may be limited by regulatory rules for the country in use.
Uplink Max Rate (Subscriber Module Mode)	Specifies the maximum uplink MCS value that the Rate Adapt algorithm will choose for Radio 1. If an installation is exhibiting packet loss due to uplink interference, modifying **Uplink Max Rate** to limit the device's maximum MCS rate may result in more reliable packet delivery. This is especially true in installations among changing and unpredictable interference.

Attribute	Meaning
Scan Channel Bandwidth (Subscriber Module Mode)	The selected scan channel bandwidths are scanned by the Subscriber Module. Any combination may be selected. When bandwidth is selected, a tab for the bandwidth appears and a listing of all available channels is presented once the tab for the bandwidth is selected. Each bandwidth tab may contain a number on the left side. This number defines how many channels have been selected for that bandwidth. If no channels are selected for bandwidth, then all channels are scanned.

Configuration > System page

Figure 20 Configuration > System page

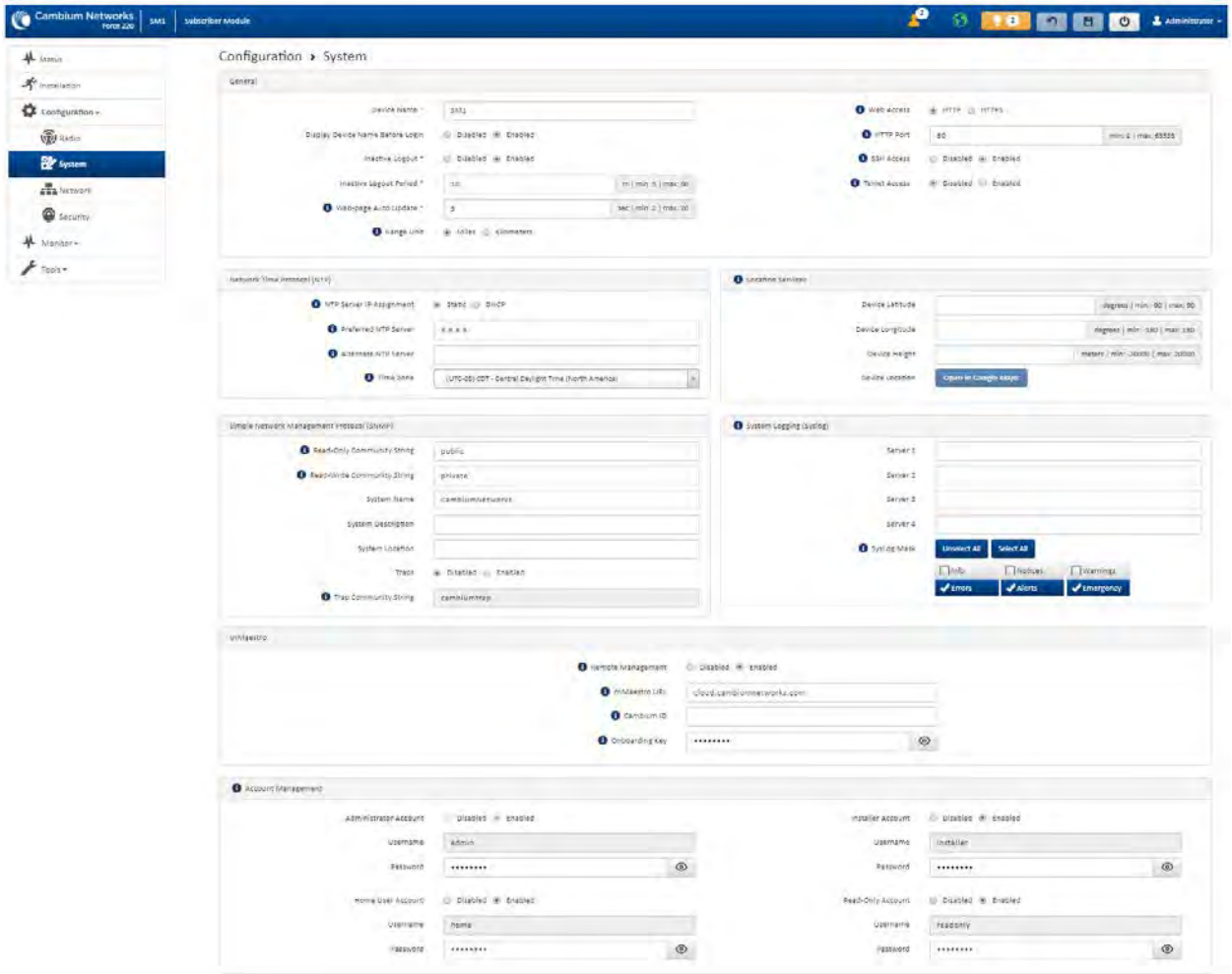


Table 46 Configuration > System page attributes

Attribute	Meaning
General	

Attribute	Meaning
Device Name	The configured identifier used in an NMS such as cnMaestro.
Display Device Name Before Login	**Disabled**: For security, the configured **Device Name** is hidden on the device login screen. **Enabled**: The configured **Device Name** is displayed upper-left on the device login screen.
Inactive Logout	**Disabled**: The device will not automatically log out users after a period of inactivity. **Enabled**: After the period configured in the **Inactive Logout Period** has elapsed, the device will automatically log out the user.
Inactive Logout Period	Represents the amount of time for which a user will remain logged in. After this period has elapsed, the user will be automatically logged out.
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). Webpage Auto Update is a session only configuration change. It is updated with the <Enter> key and is not savable when using the save button.
Range Unit	Units of measurement on the device are displayed in either miles (m) or kilometers (km).
Web Access	**HTTP**: The device web management interface is accessed via HTTP. **HTTPS:** The device web management interface may only be accessed via secure HTTPS.
HTTP Port	This specifies the TCP/UDP port to be used with HTTP or HTTPS. The default value for HTTP is 80 and HTTPS is 443.
SSH Access	**Disabled**: Access to the device through SSH is not possible. **Enabled:** Cambium engineers can access the device through SSH which enables them to log in to the radio and troubleshoot. **SSH Access** is **Enabled** by default.
Telnet Access	**Disabled**: Command Line Interface access via Telnet is not allowed **Enabled:** Command Line Interface access via Telnet is allowed
Network Time Protocol (NTP)	
NTP Server IP Assignment	**Static**: The device retrieves NTP time data from the servers configured in fields NTP Server IP Address. **DHCP**: The device retrieves NTP time data from the server IP issued via a network DHCP server.
Preferred NTP Server	Configure the primary NTP server IP addresses from which the device will retrieve time and date information.
Alternate NTP Server	Configure an alternate or secondary NTP server IP addresses from which the device retrieves time and date information.
Time Zone	The Time Zone option may be used to offset the received NTP time to match the operator's local time zone.

Attribute	Meaning
Location Services	
On-board GPS Latitude	GPS-retrieved Latitude information for the device in decimal format.
On-board GPS Longitude	GPS-retrieved Longitude information for the device in decimal format.
On-board GPS Height	GPS-retrieved height information for the device in meters.
Use GPS Coordinates	Click **Update** to retrieve device location and height information via the connected GPS source.
Device Latitude	Configure Latitude information for the device in decimal format.
Device Longitude	Configure Longitude information for the device in decimal format.
Device Height	Configure height above sea level for the device in meters.
Device Location	Hyperlink to display the device location in Google Maps
Simple Network Management Protocol (SNMP)	
Read-Only Community String	Specify a control string that can allow a Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. This password will never authenticate an SNMP user or an NMS to read/write access. The **Read-only Community String** value is clear text and is readable by a packet monitor.
Read-Write Community String	Specify a control string that can allow a Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string.
System Name	Specify a string to associate with the physical module. This parameter can be polled by the NMS. Special characters are supported.
System Description	Specify a description string to associate with the physical module. This parameter can be polled by the NMS. Special characters are supported.
System Location	Specify a description string to associate with the physical location. This parameter can be polled by the NMS. Special characters are supported.
Traps	**Disabled**: SNMP traps for system events are not sent from the device.

Attribute	Meaning
	Enabled: SNMP traps for system events are sent to the servers configured in table **Trap Servers**.
Trap Community String	Configure an SNMP Trap Community String which is processed by the servers configured in **Trap Servers**. This string is used by the trap server to decide whether or not to process the traps incoming from the device (i.e. for traps to successfully be received by the trap server, the community string must match).
System Logging (Syslog)	
Server 1-4	Specify up to four Syslog servers to which the device sends Syslog messages.
Syslog Mask	Configure the levels of Syslog messages which the devices send to the servers configured in parameters **Server 1-4.** Caution Choose only the Syslog levels appropriate for your installation. Excessive logging can cause the device log file to fill and begin overwriting previous entries.
cnMaestro	
Remote Management	When **Enabled**, the device will be managed by cnMaestro - the Cambium Remote Management System, which allows all Cambium devices to be managed in the cloud.
cnMaestro URL	Configure the URL of cnMaestro. The default value is https://cloud.cambiumnetworks.com.
Cambium ID	Configure the Cambium ID that the device will use for on-boarding on to cnMaestro.
Onboarding Key	Configure the password/key associated with the **Cambium-ID** that the device will use for on-boarding on to cnMaestro.
Account Management	
Administrator Account	The Administrator account has full read and write permissions for the device. **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.
Username	The username associated with the administrator account used upon device login.
Password	Configure a custom password to secure the device. Only the 'Administrator' account can override this password. The password character display may be toggled using the visibility icon.
Installer Account	The Installer account has permissions to read and write parameters applicable to unit installation and monitoring. **Disabled**: The disabled user is not granted access to the device management interface. **Enabled**: The user is granted access to the device management interface.

Attribute	Meaning
Username	The username associated with the installer account used upon device login.
Password	Configure a custom password to secure the device. Only the 'Administrator' account can override this password. The password character display may be toggled using the visibility icon .
Home User Account	The Home User account has permission to access pertinent information for support purposes. **Disabled**: The disabled user is not granted access to the device management interface. **Enabled**: The user is granted access to the device management interface.
Username	The username associated with the home user account used upon device login.
Password	Configure a custom password to secure the device. Only the 'Administrator' account can override this password. The password character display may be toggled using the visibility icon .
Read- Only Account	The Read-Only account has permissions to view the **Monitor** page only. **Disabled**: The disabled user is not granted access to the device management interface. **Enabled**: The user is granted access to the device management interface.
Username	The username associated with the read-only account used upon device login.
Password	Configure a custom password to secure the device. Only the 'Administrator' account can override this password. The password character display may be toggled using the visibility icon .

Configuration > Network page

Figure 21 Configuration > Network page (Access Point Mode)

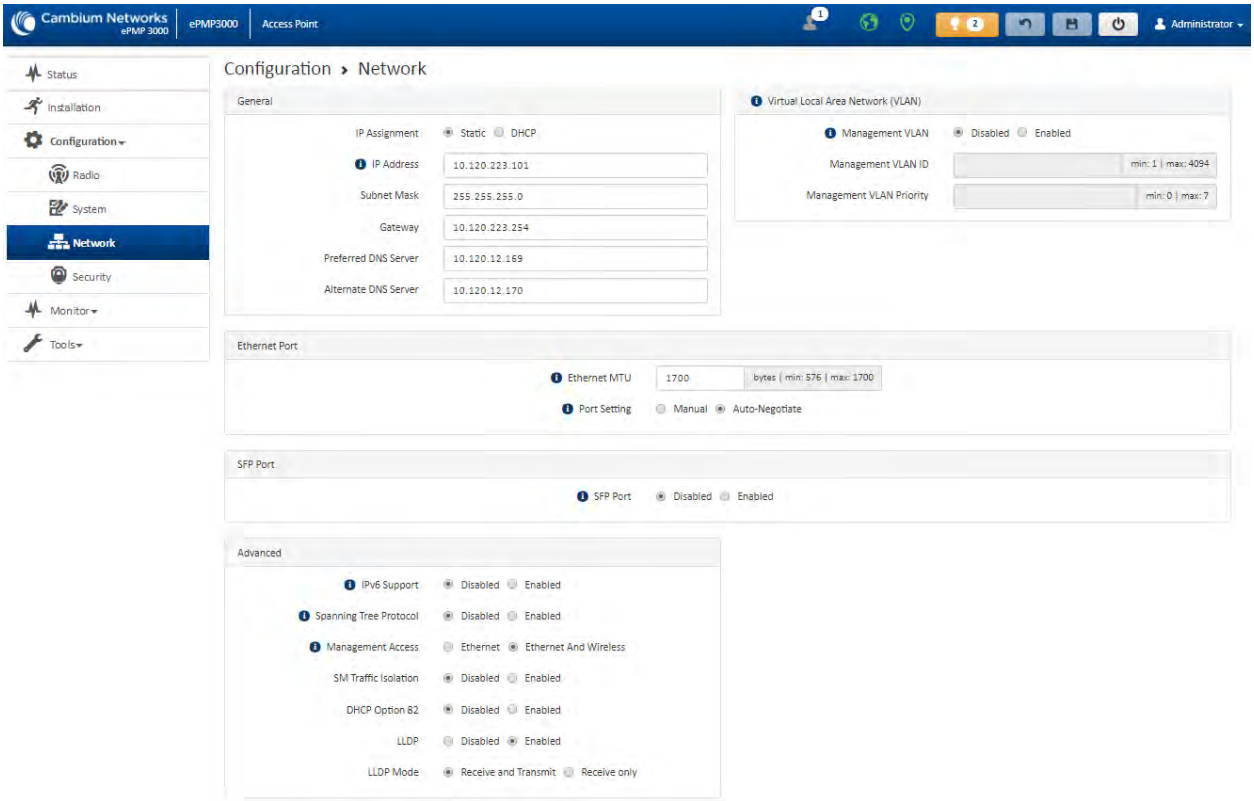


Figure 22 Configuration > Network page (Subscriber Module Mode, Bridge Network Mode)

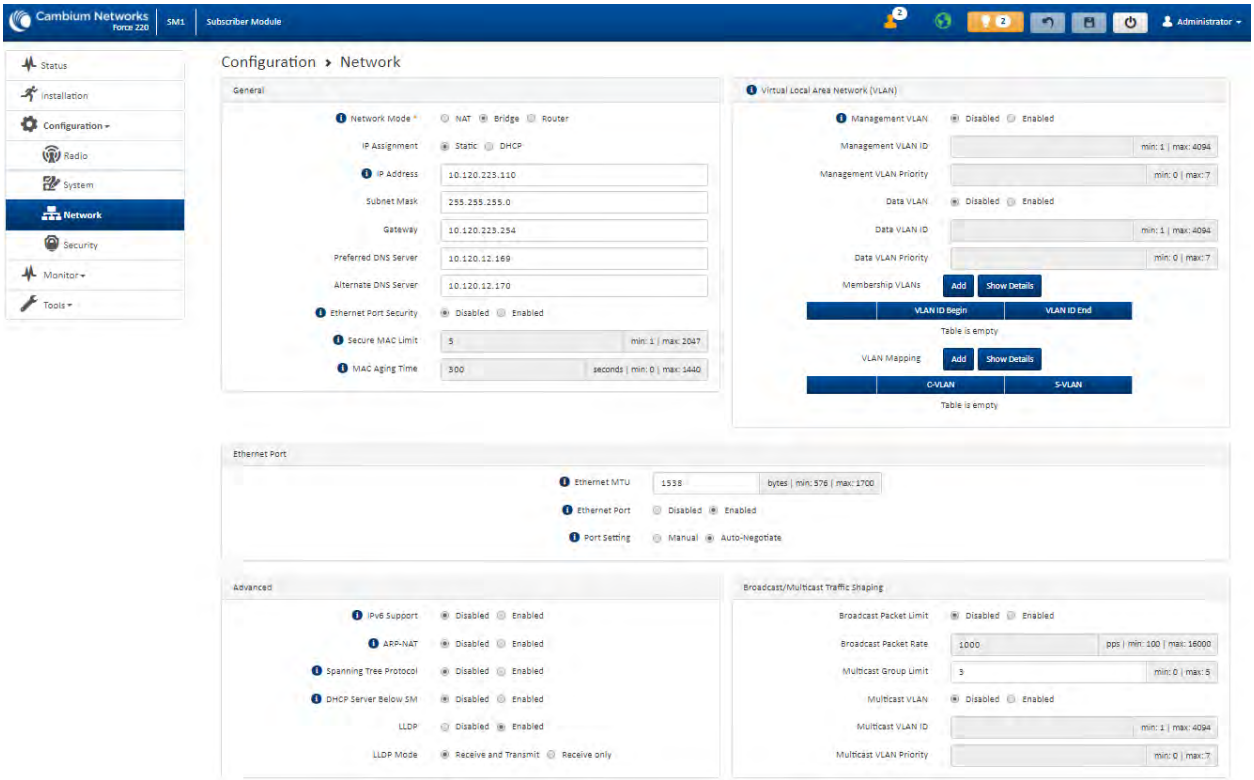


Figure 23 Configuration > Network page (Subscriber Module Mode, NAT Network Mode)

Figure 24 Configuration > Network page (Subscriber Module Mode, Router Mode)

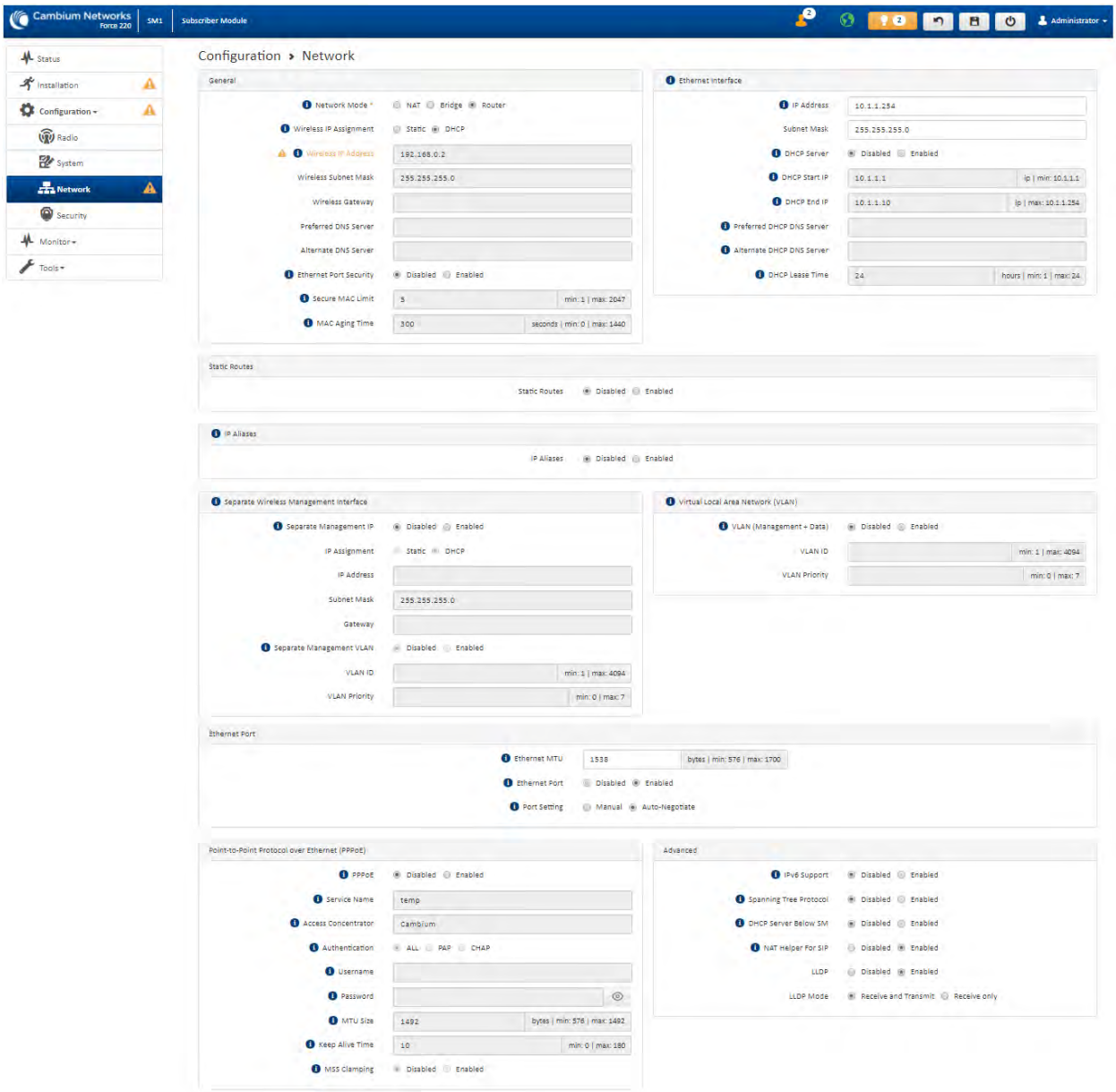


Table 47 Configuration > Network page attributes

Attribute	Meaning
General	
Network Mode	**NAT**: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination). **Bridge**: The SM acts as a switch and packets are forwarded or filtered based on their MAC destination address.

Attribute	Meaning
	Router: The SM acts as a router and packets are forwarded or filtered based on their IP header (source or destination) using specific static routes and IP aliases configured by the operator.
IP Assignment	**Static:** Device management IP addressing is configured manually in fields **IP Address, Subnet Mask, Gateway, Preferred DNS Server,** and **Alternate DNS Server**. **DHCP:** Device management IP addressing (**IP address, Subnet Mask, Gateway, and DNS Server**) is assigned via a network DHCP server, and parameters **IP Address, Subnet Mask, Gateway, Preferred DNS Server,** and **Alternate DNS Server** are not configurable.
Wireless IP Assignment (NAT Mode, Router Mode)	Static: Wireless IP address is configured manually in fields **Wireless IP Address, Wireless IP Subnet Mask, Wireless Gateway IP Address, Preferred DNS IP Address** and **Alternate DNS IP Address**. DHCP: Device management IP addressing (**Wireless IP address, Wireless Subnet mask, Wireless Gateway,** and **DNS server**) is assigned via a network DHCP server.
IP Address Wireless IP Address (NAT Mode, Router Mode)	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. If IP Address Assignment 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 (Access Point) or 192.168.0.2 (Subscriber Module).
Subnet Mask Wireless IP Address (NAT Mode, Router Mode)	Defines the address range of the connected IP network. For example, if Device IP Address (LAN) is configured to 192.168.2.1 and IP Subnet Mask (LAN) is configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.
Gateway Wireless Gateway (NAT Mode, Router Mode)	Configure the IP address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Preferred DNS Server	Configure the primary IP address of the server used for DNS resolution.
Alternate DNS Server	Configure the secondary IP address of the server used for DNS resolution.
IPv6 Assignment	IPv6 Assignment specifies how the IPv6 address is obtained. Static: Device management IP addressing is configured manually in fields IPv6 Address and IPv6 Gateway. DHCPv6: Device management IP addressing (IP address and gateway) is assigned via a network DHCP server, and parameters IPv6 Address and IPv6 Gateway are unused. If the DHCPv6 server is not available previous static IPv6 address will be used as a fallback IPv6 address. If no previous static IPv6 address is available, no IPv6 address will be assigned. DHCPv6 will occur over the wireless interface by default.

Attribute	Meaning
IPv6 Address	Internet protocol version 6 (IPv6) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. IPv6 addresses are represented by eight groups of four hexadecimal digits separated by colons.
IPv6 Gateway	Configure the IPv6 address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Ethernet Port Security (Subscriber Module Mode)	**Disabled:** No MAC address limit/gaining timers are imposed for bridging at the Subscriber Module device Ethernet port. **Enabled:** By configuring **Secure MAC Limit** and **MAC Aging Time**, a limit is imposed on the number and duration of bridged devices connected to the Subscriber Module Ethernet port.
Secure MAC Limit (Subscriber Module Mode)	Configure the number of simultaneous secure MAC addresses that will be allowed at the Ethernet interface of the Subscriber Module
MAC Aging Time (Subscriber Module Mode)	Configure the time for which the secure MAC addresses should be allowed to age. Once the Aging timer expires for a MAC address, it will be removed from the internal table and no longer count as an active MAC. Set the time to 0 to disable aging.
Ethernet Interface (Subscriber Module NAT Mode, Router Mode)	
IP Address (Subscriber Module NAT Mode, Router Mode)	Ethernet interface Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Subnet Mask (Subscriber Module NAT Mode, Router Mode)	Defines the address range of the connected IP network. For example, if Device IP Address (LAN) is configured to 192.168.2.1 and IP Subnet Mask (LAN) is configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.
DHCP Server (Subscriber Module NAT Mode, Router Mode)	Disabled: Use this setting when SM is in NAT or Router mode if there is an existing DHCP Server below the SM handing out IP Addresses or if all devices below the SM will be configured with static IP Addresses. Enabled: Use this setting when SM is in NAT or Router mode, to use the SM's local/onboard DHCP server to hand out IP addresses to its clients.
DHCP Start IP (Subscriber Module NAT Mode, Router	Configure the first address which will be issued to a DHCP client. Upon additional DHCP requests, the DHCP Start IP is incremented until local DHCP End IP is reached.

Attribute	Meaning
Mode)	
DHCP End IP (Subscriber Module NAT Mode, Router Mode)	Configure the highest IP address in the DHCP pool that can be issued to a DHCP client.
Preferred DHCP DNS Server (Subscriber Module NAT Mode, Router Mode)	Configure the primary DNS Server IP address which will be used to configure DHCP clients (if local DHCP Server is set to Enabled).
Alternate DHCP DNS Server (Subscriber Module NAT Mode, Router Mode)	Configure the secondary DNS Server IP address which will be used to configure DHCP clients (if local DHCP Server is set to Enabled).
DHCP Lease Time (Subscriber Module NAT Mode, Router Mode)	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.
Static Routes (Subscriber Module Router Mode)	
Static Routes (Subscriber Module Router Mode)	When Enabled, it allows the operator to create static routes that will apply to both the Wireless and Ethernet interface of the SM. This allows operators to configure a custom table of explicit paths between networks. Static routing is often used as a method to reduce the overhead of processing dynamic routes through a network when the specific path is known (or, it is simpler to define a specific path). Static routing is also used as a backup when dynamic routing protocols fail to complete a route from one network to another. In router mode, the Static Routes table is referenced by the SM to forward/filter packets to a particular destination configured by the user based on the IP addressing information contained in the table. Since static routes do not change with network changes, it is recommended to only use static routes for simple network paths that are not prone to frequent changes (requiring updates to the routes configured on the ePMP SM). It is important to consider each hop in a static route's path to ensure that the routing

Attribute	Meaning
	equipment has been configured to statically or dynamically route packets to the proper destination. Otherwise, network communication will fail. Network Address Translation (NAT) is not performed when the SM is in Router mode.
Target Network IP (Subscriber Module Router Mode)	Configure the target subnet/network's IP address to which the SM should route the packets.
Subnet Mask (Subscriber Module Router Mode)	Configure the subnet mask for the **Target Network IP** address.
Gateway (Subscriber Module Router Mode)	Configure the gateway to which packets that match the **Target Network IP Address** and **Subnet Mask** are sent.
Description (Subscriber Module Router Mode)	Provide a description to easily identify the static route and its purpose.
IP Aliases (Subscriber Module Router Mode)	
IP Aliases (Subscriber Module Router Mode)	When Enabled, IP aliases allow the operator to associate more than one IP address to the Ethernet interface of the SM. This configuration of multiple IP addresses for the SM's Ethernet interface allows connections to multiple networks, often used as a mechanism for management access to the device from a convenient networking path.
IP Address (Subscriber Module Router Mode)	Configure the IP address for the alias.
Subnet Mask (Subscriber Module Router Mode)	Configure the subnet mask for the alias.
Description (Subscriber Module Router Mode)	Provide a description to easily identify the IP alias and its purpose/connected network.

Attribute	Meaning
Separate Wireless Management Interface (Subscriber Module NAT Mode, Router Mode)	
Separate Management IP (Subscriber Module NAT Mode, Router Mode)	**Disabled:** When disabled, the Wireless IP is the management interface for the SM. **Enabled:** When enabled, the IP Address below is the management interface for the SM.
IP Assignment (Subscriber Module NAT Mode, Router Mode)	**Static:** Separate Wireless Management Interface is configured manually in fields **IP Address, Subnet Mask** and **Gateway**. **DHCP:** Management IP addressing (**IP Address, Subnet Mask, Gateway and DNS Server**) is assigned via a network DHCP server.
IP Address (Subscriber Module NAT Mode, Router Mode)	Configure the IP address that will be used to access the SM's management interface when in NAT mode. The Wireless IP (public IP) will not allow management access.
Subnet Mask (Subscriber Module NAT Mode, Router Mode)	Defines the address range of the connected IP network. For example, if the IP Address is configured to 192.168.2.1 and Subnet Mask is configured to 255.255.255.0, the device wireless interface will belong to the subnet 192.168.2.X.
Gateway (Subscriber Module NAT Mode, Router Mode)	Configure the IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Separate Management VLAN (Subscriber Module NAT Mode, Router Mode)	**Enabled:** A VLAN configuration establishes a logical group within the network. Each computer in the VLAN, regardless of initial or eventual physical location, has access to the same data based on the VLAN architecture. For the network operator, this provides flexibility in network segmentation, simpler management, and enhanced security. When the SM is in NAT mode, the Separate Wireless Management VLAN configuration is applicable to management data. **Disabled**: When disabled, the SM does not have a unique management VLAN.
VLAN ID (Subscriber Module NAT Mode, Router Mode)	Configure this parameter to include the device's management traffic on a separate VLAN network.

Attribute	Meaning
VLAN Priority (Subscriber Module NAT Mode, Router Mode)	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 management data. This parameter only takes effect if the Separate Wireless Management VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for management traffic on the configured VLAN ID originating from the SM. The default value is 0.
Virtual Local Area Network (VLAN)	
Management VLAN (Access Point Mode)	**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.
VLAN (Management + Data) (Subscriber Module Mode)	**Enabled:** The device 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, the 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.
VLAN ID (NAT Mode, Router Mode)	Configure this parameter to include the device's management traffic on a separate VLAN network.
VLAN Priority (NAT Mode, Router Mode)	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 management data. This parameter only takes effect if the Separate Wireless Management VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for management traffic on the configured VLAN ID originating from the SM. The default value is 0.
Management	Configure this parameter to include the device's management traffic on a separate

Attribute	Meaning
VLAN ID (Access Point Mode) (Subscriber Module Bridge Mode)	VLAN network. For example, if Management VLAN ID is set to 2, GUI access will only be allowed from frames tagged with VLAN ID 2. This parameter only takes effect if the MGMT VLAN parameter is enabled.
Management VLAN Priority (Access Point Mode) (Subscriber Module Bridge Mode)	ePMP devices can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. **Management VLAN Priority** represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to device management traffic. This parameter only takes effect if the Management VLAN parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the management VLAN originating from the Subscriber Module. The default value is 0.
Data VLAN (Subscriber Module Mode) (Bridge Mode)	Enabled: A VLAN tag will be added to all untagged traffic entering the Salve device LAN port before sending it to the Access Point and remove tags in the opposite direction from traffic (tagged with Data VLAN ID) entering on the Subscriber Module device WAN port before sending to the Subscriber Module device LAN port. Disabled: When disabled, no changes are made to untagged traffic passing through the Subscriber Module device.
Data VLAN ID (Subscriber Module Mode) (Bridge Mode)	Configure this parameter to include this VLAN tag to all untagged traffic entering on the Subscriber Module device LAN port before sending it to the Access Point device and remove tags in the opposite direction from traffic (tagged with Data VLAN ID) entering on the Subscriber Module device WAN port before sending to the Subscriber Module device LAN port.
Data VLAN Priority (Subscriber Module Mode) (Bridge Mode)	ePMP devices 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. This parameter only takes effect if the **Data VLAN** parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the **Data VLAN** originating from the Subscriber Module device. The default value is 0.
Membership VLAN (Subscriber Module Bridge Mode)	Configure the **Membership VLAN Table** to include the SM in one or more VLANs. When the SM receives a packet tagged from either the Ethernet (LAN) or Wireless (WAN) side with a VLAN ID which is contained in the **Membership VLAN Table**, the packet is forwarded and sent out the other interface. When the SM receives a packet tagged with a VLAN ID which is not present in the **Membership VLAN Table**, the frame is dropped (assuming there is at least one VLAN ID present in the Membership VLAN table or configured as a Data VLAN).
VLAN Mapping (Subscriber	Configure the **VLAN Mapping Table** to map the C-VLAN of traffic ingressing the Ethernet (LAN) port of the SM to an S-VLAN before being forwarded to the air interface on the UL. In the DL direction, the SM will automatically un-map the S-VLAN to the C-

Attribute	Meaning
Module Bridge Mode)	VLAN before forwarding the tagged packets to the Ethernet (LAN) interface of the SM.
C-VLAN (Subscriber Module Bridge Mode)	Configure the C-VLAN ID of the tagged traffic for which the mapping needs to occur. The C-VLAN ID must be entered in the SM VLAN Membership VLAN table.
S-VLAN (Subscriber Module Bridge Mode)	Configure the S-VLAN ID to which the tagged traffic needs to be mapped to. The S-VLAN ID must be entered in the SM VLAN Membership VLAN table.
Ethernet Port	
Ethernet MTU	Specify the device MTU or Maximum Transmission Unit; the size in bytes of the largest data unit that the device is configured to process. Larger MTU configurations can enable the network to operate with greater efficiency, but in the case of retransmissions due to packet errors, efficiency is reduced since large packets must be resent in the event of an error.
Ethernet Port (Subscriber Module Mode)	**Disabled**: The primary Ethernet port is disabled (a mechanism for restricting access for non-payment). **Enabled:** The primary Ethernet port is enabled.
Port Setting	Allows the Gigabit Ethernet port duplex settings and port speed to be either manually configured or auto-negotiate with the connected Ethernet device on the other end of the link. Guidelines for using **Port Setting**: When auto-negotiation is turned on, this applies to both **Port Speed** and **Port Duplex Mode**. If the other end of the Ethernet connection supports auto-negotiation, then **Auto-Negotiate** should be selected. If the other end of the Ethernet connection does not support auto-negotiation, then **Manual** should be selected and both ends of the link should manually set the port speed and port duplex mode.
Port Speed	With **Port Setting** configured to **Manual**, the Gigabit Ethernet port speed can be forced to 1000 Mbps, 100 Mbps or 10 Mbps.
Port Duplex Mode	With **Port Setting** configured to **Manual**, the Gigabit Ethernet port duplex mode can be forced to **Full** or **Half**.
Port Forwarding (Subscriber Module Mode) (NAT Mode)	
UPnP IGD (Subscriber Module Mode)	Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and

Attribute	Meaning
(NAT Mode)	entertainment. UPnP is intended primarily for residential networks without enterprise-class devices. With UPnP IGD and PCP protocols, ePMP will support explicit dynamic port mappings. Enable UPnP IGD (Internet Gateway Device) to allow the ePMP device to use the IGD profile for UPnP support.
NAT PMP (PCP) (Subscriber Module Mode) (NAT Mode)	The PCP (Port Control Protocol) allows an IPv6 or IPv4 host to control how incoming IPv6 or IPv4 packets are translated and forwarded by a Network Address Translator (NAT) or simple firewall, and also allows a host to optimize its outgoing NAT keepalive messages. PCP was standardized as a successor to the NAT Port Mapping Protocol (NAT-PMP), with which it shares similar protocol concepts and packet formats. Enable this parameter to allow the ePMP device to use the PCP protocol for UPnP support.
Data Port Forwarding (Subscriber Module Mode) (NAT Mode)	The Data Port Forwarding Table is used to define which range of wireless ports that are forwarded to a LAN (SM local network) IP address below the SM.
Protocol (Subscriber Module Mode) (NAT Mode)	UDP: Packet forwarding decisions are based on UDP packets. TCP: Packet forwarding decisions are based on TCP packets.
Port Begin (Subscriber Module Mode) (NAT Mode)	Configure the beginning of the range of wireless ports to match for forwarding to LAN IP.
Port End (Subscriber Module Mode) (NAT Mode)	Configure the end of the range of wireless ports to match for forwarding to LAN IP.
Forwarding IP (Subscriber Module Mode) (NAT Mode)	Configure the LAN IP of the device situated below the SM which receives the packets forwarded based on the Separate Management IP Port Forwarding Table configuration.
Mapped Port (Subscriber Module Mode) (NAT Mode)	Configure the port of the device situated below the SM which receives the packets forwarded based on the Data Port Forwarding Table configuration.

Attribute	Meaning
Point-to-Point Protocol over Ethernet (PPPoE) (Subscriber Module Mode) **(NAT Mode, Router Mode)**	
PPPoE (Subscriber Module Mode) (NAT Mode, Router Mode)	Point-to-Point Protocol over Ethernet: Used for encapsulating PPP frames inside Ethernet frames.
Service Name (Subscriber Module Mode) (NAT Mode, Router Mode)	Optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the SM accepts the first service option that comes back from the Access Concentrator specified below, if any. This is limited to 32 characters.
Access Concentrator (Subscriber Module Mode) (NAT Mode, Router Mode)	Optional entry to set a specific Access Concentrator to connect to for the PPPoE session. If this is blank, the SM accepts the first Access Concentrator which matches the service name (if specified). This is limited to 32 characters.
Authentication (Subscriber Module Mode) (NAT Mode, Router Mode)	**ALL:** This means that CHAP authentication will be attempted first, then PAP authentication. The same password is used for both types. **CHAP:** This means that CHAP authentication will be attempted. **PAP:** This means that PAP authentication will be attempted.
Username (Subscriber Module Mode) (NAT Mode, Router Mode)	This is the CHAP/PAP username that is used. This is limited to 32 characters.
Password (Subscriber Module Mode) (NAT Mode, Router Mode)	This is the CHAP/PAP password that is used. This is limited to 32 characters.
MTU Size (Subscriber Module Mode)	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

Attribute	Meaning
(NAT Mode, Router Mode)	in LCP negotiations is less than this user-specified value, the SM uses the smaller value as its MTU for the PPPoE link.
Keep Alive Time (Subscriber Module Mode) (NAT Mode, Router Mode)	Configure the Keep Alive Time to allow the radio to keep the PPPoE session up after establishment. As an example, if this field is set to 5, the PPPoE client will send a keep-alive message to the PPPoE server every 5 seconds. If there is no acknowledgment, it sends the 'Keep alive' message to the server 4 more times (for a total of 5 times) before tearing down the PPPoE session. Setting this to 12 will mean the keep-alive message will be sent every 12 seconds and when there is no acknowledgment, the client will try for a total of 12 times every 12 seconds before tearing down the PPPoE session.
MSS Clamping (Subscriber Module Mode) (NAT Mode, Router Mode)	**Disabled:** The SM PPPoE session allows any MTU size determined by other devices in the PPPoE session during the LCP negotiations. **Enabled:** The SM PPPoE session enforces a max MTU size determined by the PPPoE MTU Size setting for all devices in the PPPoE session during the LCP negotiations unless one of the devices enforces an MTU setting that is smaller in value.
SFP Port (Access Point Mode)	
SFP Port (Access Point Mode)	**Disabled**: The SFP port is inactive. **Enabled**: The SFP port is active.
Advanced	
IPv6 Support	System-wide IPv6 Protocol Support. When enabled, appropriate IPv6 modules and services will be loaded.
Spanning Tree Protocol	Disabled: When disabled, Spanning Tree Protocol (802.1d) functionality is disabled at the Access Point. Enabled: When enabled, Spanning Tree Protocol (802.1d) functionality is enabled at the Access Point, allowing for the prevention of Ethernet bridge loops.
DHCP Server Below Subscriber Module (Subscriber Module Mode)	Disabled: This blocks DHCP servers connected to the Subscriber Module device LAN side from handing out IP addresses to DHCP clients above the Subscriber Module device (wireless side). Enabled: This allows DHCP servers connected to the Subscriber Module device LAN side to assign IP addresses to DHCP clients above the Subscriber Module device (wireless side). This configuration is typical in PTP links.
Management Access (Access Point Mode)	Ethernet: Only allow access to the Access Point's web management interface via a local Ethernet (LAN) connection. In this configuration, the Access Point's web management interface may not be accessed from over the air (i.e. from a device situated below the Subscriber Module). Ethernet and Wireless: Allow access to the Access Point's web management interface via a local Ethernet (LAN) connection and from over the air (i.e. from a device situated below the Subscriber Module). Access Points configured with Management Access Interface set to Ethernet and

Attribute	Meaning
	Ethernet and Wireless are susceptible to unauthorized access.
SM Traffic Isolation (Access Point Mode)	**Disabled**: This is the default mode. When SM isolation is disabled, an SM is able to communicate with another SM, when both the SMs are associated to the same Access Point (AP). **Enabled**: When SM Isolation feature is **Enabled**, an SM is unable to communicate with another SM (peer-to-peer traffic) when both the SMs are associated with the same Access Point (AP). This feature essentially enables the AP to drop the packets to avoid peer-to-peer traffic scenarios.
DHCP Option 82 (Access Point Mode)	**Disabled:** The device does not insert the "remote-id" (option ID 0x2) and the "circuit-id" (ID 0x01). DHCP Option 82 is 'Disabled' by default. **Enabled**: The device inserts "remote-id" (option ID 0x2) to be the Subscriber Module MAC address and the "circuit-id" (ID 0x01) to be the Access Point's MAC address. Those two fields are used to identify the remote device and connection from which the DHCP request was received.
LLDP	The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol (as specified in IEEE 802.1AB) used by ePMP for advertising its identity, capabilities, and neighbors on the Ethernet/wired interface. **Disabled:** ePMP does not receive or transmit LLDP packets from/to its neighbors. **Enabled:** ePMP can receive LLDP packets from its neighbors and send LLDP packets to its neighbors, depending on the LLDP Mode configuration below.
LLDP Mode	**Receive and Transmit**: ePMP sends and receives LLDP packets to/from its neighbors on the Ethernet/LAN interface. **Receive Only**: ePMP receives LLDP packets from its neighbors on the Ethernet/LAN interface and discovers them.
Broadcast / Multicast Traffic Shaping (Subscriber Module Mode) (Bridge Mode)	
Broadcast Packet Limit (Subscriber Module Mode) (Bridge Mode)	**Enabled**: This allows the user to set the **Broadcast Packet Rate** below. Configure this parameter to limit the number of broadcast packets that will be allowed on the ingress of the radio's Ethernet port. Set the packets per second value to limit the impact of events such as broadcast storms. **Disabled**: There is no limit on the amount of broadcast traffic that will be allowed into the ingress of the radio's Ethernet port.
Broadcast Packet Rate (Subscriber Module Mode) (Bridge Mode)	Set the packets per second value to limit the amount of broadcast traffic that will be allowed on the ingress on the radio's Ethernet port. The packets per second limit can be set individually on each ePMP radio. The range is 100 to 16000 packets per second. The default is **1000**.
Multicast Group Limit (Subscriber	Configure the maximum number of simultaneous multicast groups that the SM will allow from devices below it. The default is **3**.

Attribute	Meaning
Module Mode) (Bridge Mode)	
Multicast VLAN (Subscriber Module Mode) (Bridge Mode)	**Enabled:** A VLAN tag will be added to all untagged multicast traffic entering the SM's LAN port before sending it to the AP and remove tags in the opposite direction from traffic (tagged with Multicast VLAN ID) entering on the SM's WAN port before sending to the SM's LAN port. **Disabled:** When disabled, no changes are made to untagged multicast traffic passing through the SM.
Multicast VLAN ID (Subscriber Module Mode) (Bridge Mode)	Configure this parameter to include this VLAN tag to all untagged **multicast** traffic entering on the SM's LAN port before sending it to the AP and remove tags in the opposite direction from multicast traffic (tagged with Multicast VLAN ID) entering on the SM's WAN port before sending to the SM's LAN port.
Multicast VLAN Priority (Subscriber Module Mode) (Bridge Mode)	ePMP radios can prioritize VLAN traffic based on the eight priorities described in the IEEE 802.1p specification. **Multicast VLAN Priority** represents the VLAN Priority or Class of Service (CoS). Operators may use this prioritization field to give precedence to device **multicast** data. This parameter only takes effect if the **Multicast VLAN** parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the **Multicast VLAN** originating from the SM. The default value is 0.
De-Militarized Zone (Subscriber Module NAT Mode)	
DMZ (Subscriber Module NAT Mode)	**Disabled:** Packets arriving on the wireless interface destined for the Ethernet side of the network are dropped if a session does not exist between the Source IP (Wireless) and Destination IP (Ethernet). By default, NAT requires the sessions to be initiated from the Ethernet side before a packet is accepted from the Wireless to the Wired side. **Enabled:** Any packets with an unknown destination port (not associated with an existing session or not defined in the port forwarding rules) are automatically sent to the device configured with DMZ IP Address.
IP Address (Subscriber Module NAT Mode)	Configure the IP address of an SM-connected device that is allowed to provide network services to the wide-area network.
Allow ICMP to DMZ (Subscriber Module NAT Mode)	**Enabled:** ICMP packets are forwarded to the DMZ IP **Disabled:** SM answers ICMP requests, and SM **Wireless IP Address** becomes reachable by ping when DMZ enabled

Configuration > Security page

The Security page is used to configure system security features including authentication and Layer2/Layer3 Firewall rules.

Attention

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

Figure 25 Configuration > Security page (Access Point Mode)

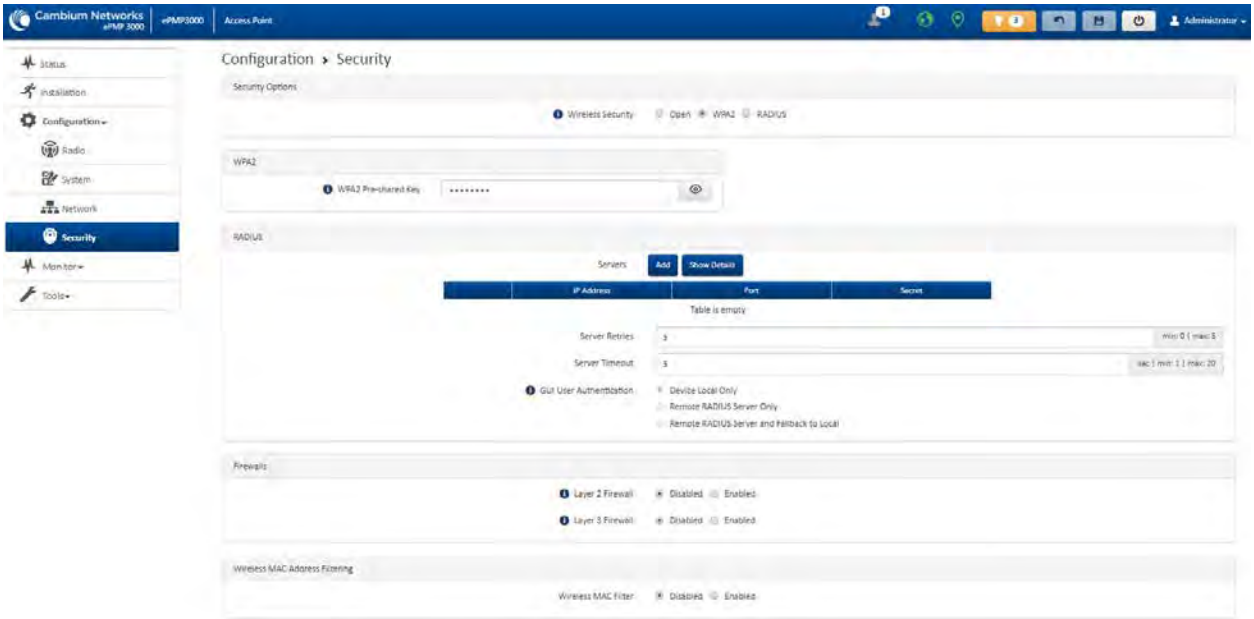


Figure 26 Configuration > Security page (Subscriber Module Mode)

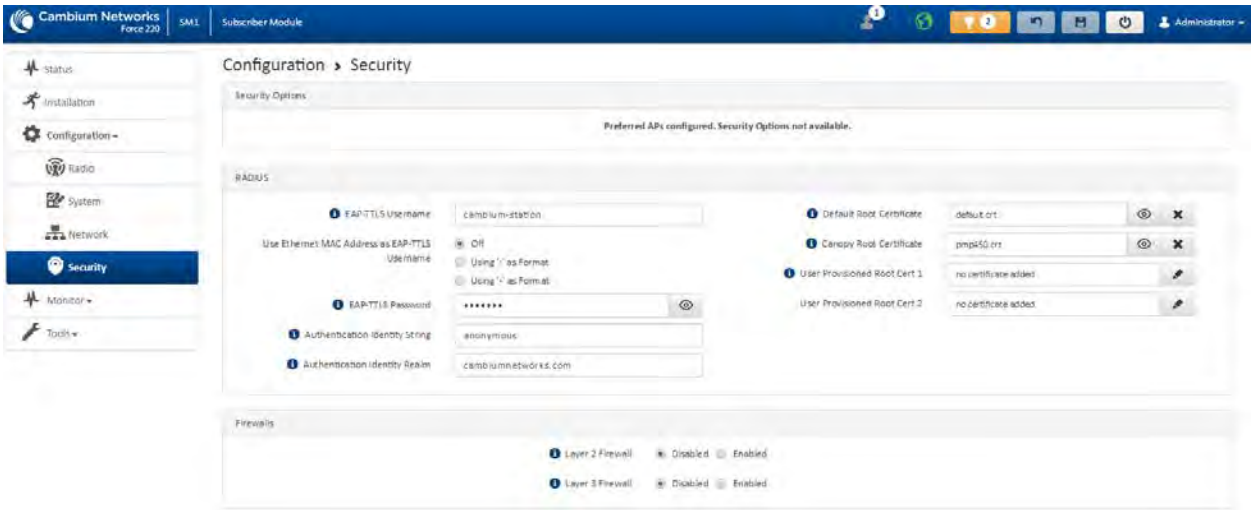


Table 48 Configuration > Security page attributes

Attribute	Meaning
Security Options	
Wireless Security (Access Point Mode)	For Access Point mode devices, select the security mode enforced upon network entry. For Subscriber Module mode devices, select the security mode utilized upon network entry attempts. Open: All Subscriber Module devices requesting network entry are allowed registration. WPA2: The WPA2 mechanism provides AES radio link encryption and Subscriber Module network entry authentication. When enabled, the Subscriber Module must register using the Authentication Pre-shared Key configured on the Access Point and Subscriber Module. RADIUS: Enables Subscriber Module authentication via a pre-configured Radius server.
WPA2	
WPA2 Pre-shared Key	Configure this key on the Access Point, then configure the Subscriber Module with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.
RADIUS (Access Point Mode)	
Servers (Access Point Mode)	For more Radio servers, click Add. 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. The default is 1812. Secret: Secret key that is used to communicate with the Radius server.
Server Retries (Access Point Mode)	The number of times the radio will retry authentication with the configured Radius server before it fails authentication of the SM.
Server Timeout (Access Point Mode)	Timeout between each retry with the configured Radius server before it fails authentication of the SM.
GUI User Authentication (Access Point Mode)	This applies to both the AP and its registered SMs. Device Local Only: The device's GUI authentication is local to the device using one of the accounts configured under Configuration->System->Account Management. Remote RADIUS Server Only: The device's GUI authentication is performed using a RADIUS server. Remote RADIUS Server and Fallback to Local: The device's GUI authentication is performed using a RADIUS server. Upon failure of authentication through a RADIUS

Attribute	Meaning
	server, the authentication falls back to one of the local accounts configured under Configuration->System->Account Management.
EAP- TTLS Username (Subscriber Module Mode)	Configure the EAP-TTLS Username to match the credentials on the RADIUS server being used for the network.
Use Ethernet MAC Address at EAP- TTLS Username (Subscriber Module Mode)	The device MAC Address can be used as the EAP-TTLS Username in either ":" or "-" delimited format.
EAP- TTLS Password (Subscriber Module Mode)	Configure the EAP-TTLS Password to match the credentials on the RADIUS server being used for the network.
Authentication Identity String (Subscriber Module Mode)	Configure this Identity string to match the credentials on the RADIUS server being used for the network. The default value for this parameter is anonymous.
Authentication Identity Realm (Subscriber Module Mode)	Configure this Identity string to match the credentials on the RADIUS server being used for the network. The default value for this parameter is cambiumnetworks.com.
Default Root Certificate (Subscriber Module Mode)	Default EAP-TTLS root certificate that must match the certificate on the RADIUS server.
Canopy Root Certificate (Subscriber Module Mode)	PMP 450 default EAP-TTLS root certificate to match the certificate on the RADIUS server used with current PMP 450 installations.
User Provisioned Root Cert 1 (Subscriber Module Mode)	Import a user certificate if a certificate different from the default certificates is needed.
User Provisioned	Import a second user certificate if a certificate different from the default or 1st user provisioned certificate is needed.

Attribute	Meaning
Root Cert 2 (Subscriber Module Mode)	
Firewalls	
Layer 2 Firewall	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 Rules	The Layer 2 firewall table may be used to configure rules matching layer 2 (MAC layer) traffic which results in forwarding or dropping the traffic over the radio link or Ethernet interface.
Layer 3 Firewall	Disabled: Modifications to the Layer 3 Firewall Table are not allowed and rules are not enforced. Enabled: Modifications to the Layer 3 Firewall Table are allowed and rules are enforced.
Layer 3 Firewall Rules	The Layer 3 firewall table may be used to configure rules matching layer 3 (IP layer) traffic which results in forwarding or dropping the traffic over the radio link or Ethernet interface.
Wireless MAC Address Filtering (Access Point Mode)	
Wireless MAC Filter (Access Point Mode)	Disabled: SMs with any MAC Address are allowed to register to the AP. Enabled: SMs with specific MAC addresses can be allowed (Permit) or denied (Prevent) registration with the AP as configured under the MAC Filter List.
Wireless MAC Filter Policy (Access Point Mode)	Prevent: All MAC Addresses configured under the MAC Filter List are denied registration to the AP. Permit: Only the MAC Addresses configured under the MAC Filter List are allowed to register to the AP.
Wireless MAC Filter List (Access Point Mode)	Configure the SM's MAC addresses that will be permitted or prevented from registering to the AP.
MAC Address (Access Point Mode)	MAC Address of the SM
Description (Access Point Mode)	Friendly description to identify the SM

Monitor menu

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

Monitor > Performance page

Figure 27 Monitor > Performance page

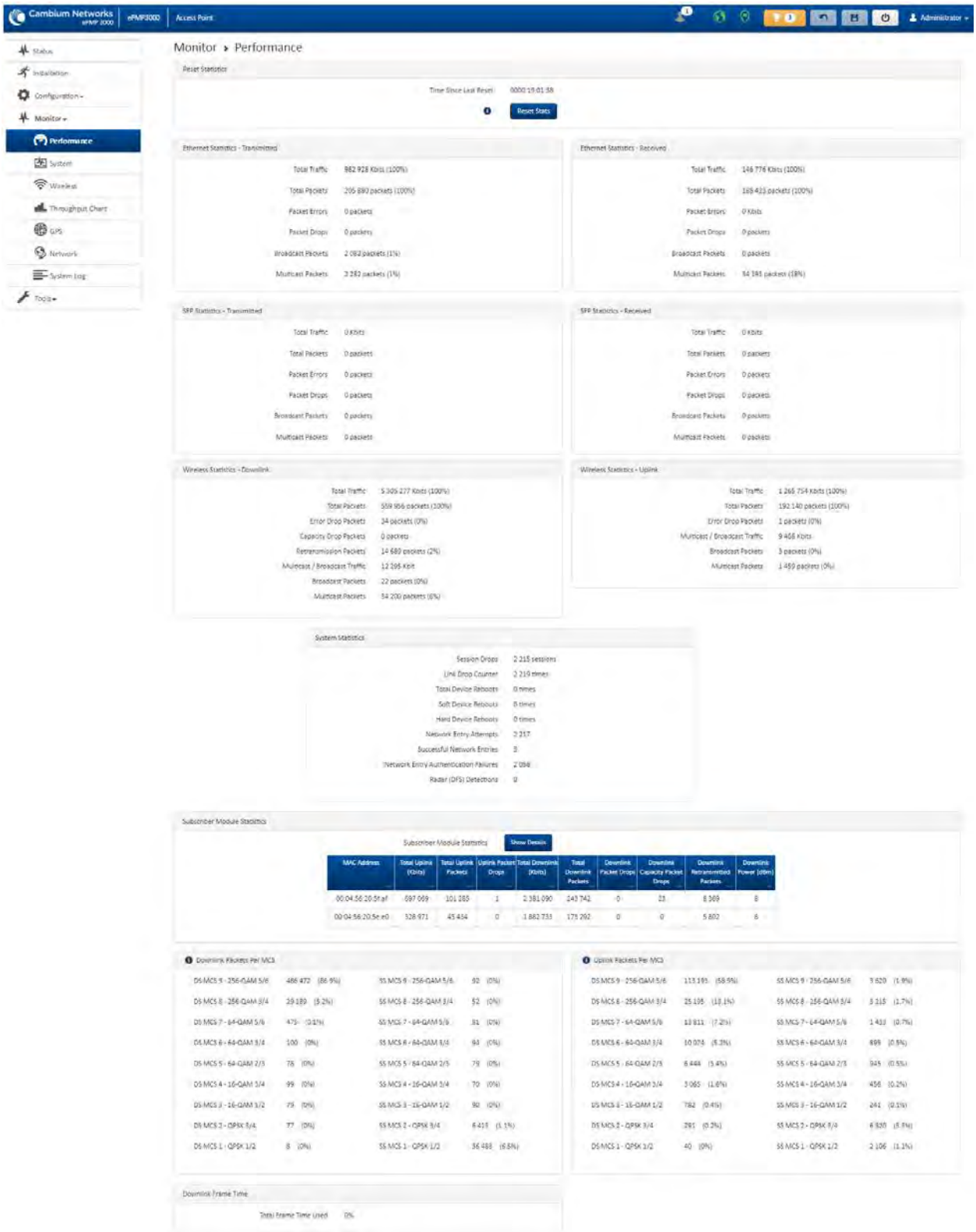


Table 49 Monitor > Performance page attributes

Attribute	Meaning
Reset Statistics	
Time Since Last Reset	Time since the stats were last reset.
Ethernet Statistics – Transmitted	
Total Traffic	The total amount of traffic in Kbits transferred from the device Ethernet interface.
Total Packets	The total number of packets transferred from the device Ethernet interface.
Packet Errors	The total number of packets transmitted out of the device Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	The total number of packets dropped prior to sending out of the device Ethernet interface due to Ethernet setup or filtering issues.
Broadcast Packets	The total number of broadcast packets sent via the device Ethernet interface.
Multicast Packets	The total number of multicast packets sent via the device Ethernet interface.
Ethernet Statistics – Received	
Total Traffic	The total amount of traffic in Kbits received by the device Ethernet interface.
Total Packets	The total number of packets received by the device Ethernet interface.
Packet Errors	The total number of packets received by the device Ethernet interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	The total number of packets dropped prior to sending out of the device wireless interface due to Ethernet setup or filtering issues.
Broadcast Packets	The total number of broadcast packets received via the device Ethernet interface.
Multicast Packets	The total number of multicast packets received via the device Ethernet interface.
SFP Statistics – Transmitted	
Total Traffic	The total amount of traffic in Kbits transferred from the device SFP interface.
Total Packets	The total number of packets transferred from the device SFP interface.
Packet Errors	The total number of packets transmitted out of the device SFP interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	The total number of packets dropped prior to sending out of the device SFP interface due to setup or filtering issues.
Broadcast Packets	The total number of broadcast packets sent via the device SFP interface.

Attribute	Meaning
Multicast Packets	The total number of multicast packets sent via the device SFP interface.
SFP Statistics - Received	
Total Traffic	The total amount of traffic in Kbits received by the device SFP interface.
Total Packets	The total number of packets received by the device SFP interface.
Packet Errors	The total number of packets received by the device SFP interface with errors due to collisions, CRC errors, or irregular packet size.
Packet Drops	The total number of packets dropped prior to sending out of the device wireless interface due to SFP setup or filtering issues.
Broadcast Packets	The total number of broadcast packets received via the device SFP interface.
Multicast Packets	The total number of multicast packets received via the device SFP interface.
Wireless Statistics – Downlink	
Total Traffic	The total amount of traffic transmitted out of the device wireless interface in Kbits.
Total Packets	The total number of packets transmitted out of the device wireless interface.
Error Drop Packets	The total number of packets dropped after transmitting out of the device Wireless interface due to RF errors (No acknowledgment and other RF related packet error).
Capacity Drop Packets (Access Point Mode)	The total number of packets dropped after transmitting out of the device wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).
Retransmission Packets (Access Point Mode)	The total number of packets re-transmitted after transmitting out of the device wireless interface due to the packets not being received by the receiving device.
Multicast / Broadcast Traffic	The total amount of multicast and broadcast traffic transmitted out of the device wireless interface in Kbits.
Broadcast Packets	The total number of broadcast packets transmitted out of the device wireless interface.
Multicast Packets	The total number of multicast packets transmitted out of the device wireless interface.
Wireless Statistics – Uplink	
Total Traffic	The total amount of traffic received via the device wireless interface in Kbits.
Total Packets	The total number of packets received via the device wireless interface.
Error Drop	The total number of packets dropped prior to sending out of the device Ethernet

Attribute	Meaning
Packets	interface due to RF errors (packet integrity error and other RF related packet error).
Capacity Drop Packets (Subscriber Module Mode)	The total number of packets dropped after transmitting out of the device wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).
Multicast / Broadcast Traffic	The total amount of multicast and broadcast traffic received on the device wireless interface in Kbits.
Broadcast Packets	The total number of broadcast packets received on the device wireless interface.
Multicast Packets	The total number of multicast packets received on the device wireless interface.
Link Quality (Uplink) (Subscriber Module Mode)	Defines the Packet Error Rate (PER) in the uplink direction by percentage. A background color corresponds to a percentage range. Blue is between 80 and 100%. Green is between 50 and 80%. Yellow is between 30 and 50%. Red is between 0 and 30%.
Link Capacity (Uplink) (Subscriber Module Mode)	Defines the capacity of the uplink as defined by MCS. DS MCS 9 provides the greatest capacity. SS MCS 1 provides the least. The capacity of the link is defined as the percentage throughput of the actual link as compared to a link that was always running at DS MCS 9. A background color corresponds to a percentage range. Blue is between 80 and 100%. Green is between 50 and 80%. Yellow is between 30 and 50%. Red is between 0 and 30%.
System Statistics	
Session Drops	Indicates the total number of Subscriber Module sessions dropped on the Access Point.
Link Drop Counter	Indicates the total number of times the wireless link was lost.
Total Device Reboots	Indicates the total number of times the device has been rebooted since the statistics were last reset from the GUI, CLI, or SNMP.
Soft Device Reboots	Indicates the number of times the device has been rebooted by the user through GUI, CLI or SNMP since the statistics were last reset from the GUI, CLI, or SNMP.

Attribute	Meaning
Hard Device Reboots	Indicates the number of times the device has been rebooted via power feeding and due to power outage since the statistics were last reset from the GUI, CLI, or SNMP.
Network Entry Attempts (Access Point Mode)	The total number of Network Entry Attempts by Subscriber Module devices.
Successful Network Entries (Access Point Mode)	The total number of successful network entry attempts.
Network Entry Authentication Failures (Access Point Mode)	The total number of failed Network Entry Attempts by Subscriber Module devices.
Radar (DFS) Detections	
Subscriber Module Statistics (Access Point Mode)	
MAC Address	MAC Address of the Subscriber Module connected to the Access Point.
Total Uplink (Kbits)	The total amount of traffic received via the Access Point wireless interface from the Subscriber Module in Kbits.
Total Uplink Packets	The total number of packets received via the Access Point wireless interface from this Subscriber Module.
Uplink Packet Drops	The total number of packets dropped prior to sending out of the Access Point Ethernet interface due to RF errors (packet integrity error and other RF related packet error) from the Subscriber Module.
Total Downlink (Kbits)	The total amount of traffic transmitted out of the Access Point wireless interface in Kbits.
Total Downlink Packets	The total number of packets transmitted out of the Access Point wireless interface.
Downlink Packet Drops	The total number of packets dropped after transmitting out of the Access Point wireless interface due to RF errors (No acknowledgment and other RF related packet error).
Downlink Capacity Packet Drops	The total number of packets dropped after transmitting out of the Access Point Wireless interface due to capacity issues (data buffer/queue overflow or other performance or internal packet errors).
Downlink Retransmitted Packets	The total number of packets re-transmitted after transmitting out of the Access Point Wireless interface due to the packets not being received by the Subscriber Module.

Attribute	Meaning
Downlink Power (dBm)	The transmit power of the Access Point for the downlink packets to the Subscriber Module.
Downlink Packets Per MCS	
MCS 1 – MCS 9 DS / SS	The number of packets (and percentage of total packets) transmitted out of the device wireless interface for every modulation mode used by the device transmitter, based on radio conditions. DS represents dual- stream transmissions and SS represents single- stream transmissions.
Uplink Packets Per MCS	
MCS 1 – MCS 9 DS / SS	The number of packets (and percentage of total packets) received on the device wireless interface for every modulation mode, based on radio conditions. DS represents dual- stream transmissions and SS represents single- stream transmissions.
Downlink Frame Time	
Total Frame Time Used (Access Point Mode)	Percentage of frame time used in the uplink.

Monitor > System page

Figure 28 Monitor > System page

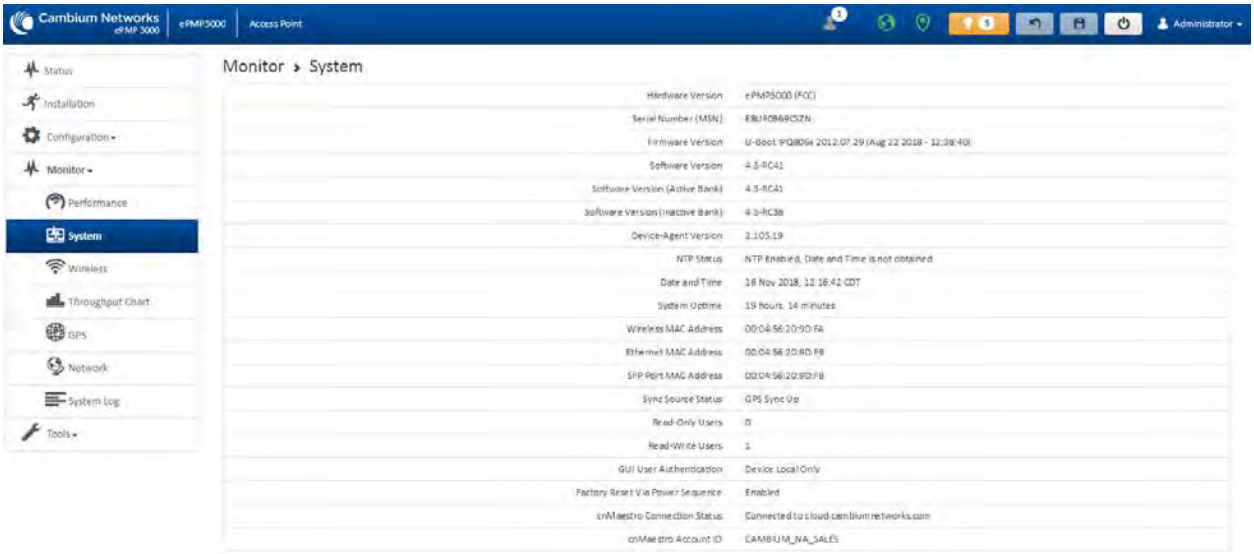


Table 50 Monitor > System page attributes

Attribute	Meaning
Hardware Version	Board hardware version information.
Serial Number (MSN)	Serial Number information.
Firmware Version	U-Boot version information.
Software Version	The currently operating version of software on the device.
Software Version (Active Bank)	The currently operating version of software on the device.
Software Version (Inactive Bank)	The backup software version on the device used upon failure of the active bank. Two software upgrades in sequence will update both the **Active Software Bank Version** and the **Inactive Software Bank Version**.
Device- Agent Version	The operating version of the device agent, which is used for communication with cnMaestro.
NTP Status	Indicates whether time and date have been obtained from the NTP server.
Date and Time	Current date and time, subject to time zone offset introduced by the configuration of the device Time Zone parameter. Until a valid NTP server is configured, this field will display the time configured from the factory.
System Uptime	The total system uptime since the last device reset.
Wireless MAC Address	The hardware address of the device wireless interface.
Ethernet MAC Address	The hardware address of the device LAN (Ethernet) interface.
SFP Port MAC Address	The hardware address of the device SFP interface.
Sync Source Status	The status of the configured GPS synchronization source.
Read- Only Users	Displays the number of active Read-Only users logged into the radio.
Read- Write Users	Displays the number of active Read-Write users logged into the radio.
GUI User Authentication	The method by which users are authenticated when logging into the device management interface.

Attribute	Meaning
Factory Reset Via Power Sequence	**Enabled**: When Enabled under **Tools** > **Backup/Restore** > Reset Via Power Sequence, it is possible to reset the radio's configuration to factory defaults using the power cycle sequence explained under Resetting ePMP to factory defaults by power cycling on page "Resetting ePMP to factory defaults by power cycling" on page 163. **Disabled**: When Disabled, it is not possible to factory default the radio's configuration using the power cycle sequence.
cnMaestro Connection Status	The current management status of the device with respect to the Cambium Cloud Server. When Enabled under Configuration->System, the device will be managed by the Cambium Remote Management System, which allows all Cambium devices to be managed from the Cambium Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Cloud Server.

Monitor > Wireless Page

Figure 29 Monitor > Wireless page (Access Point Mode)

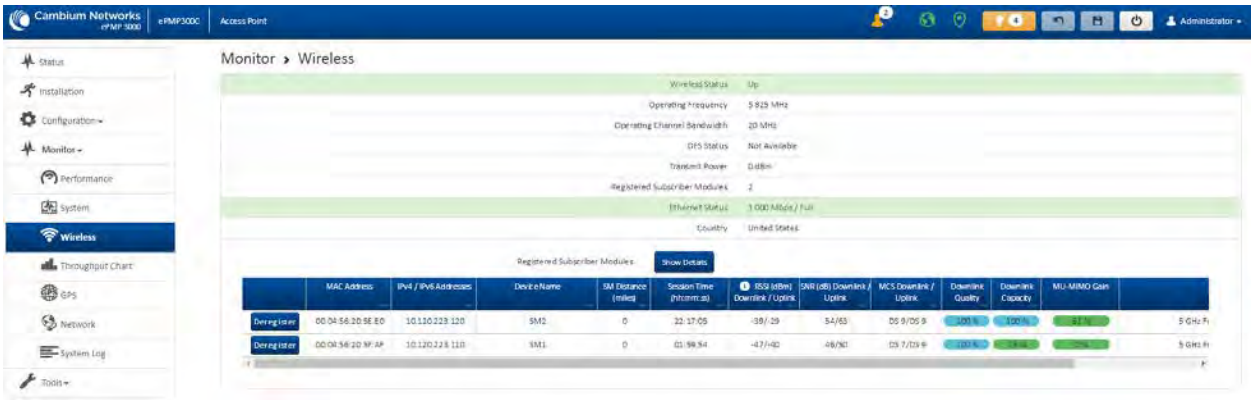


Figure 30 Monitor > Wireless page (Subscriber Module Mode)

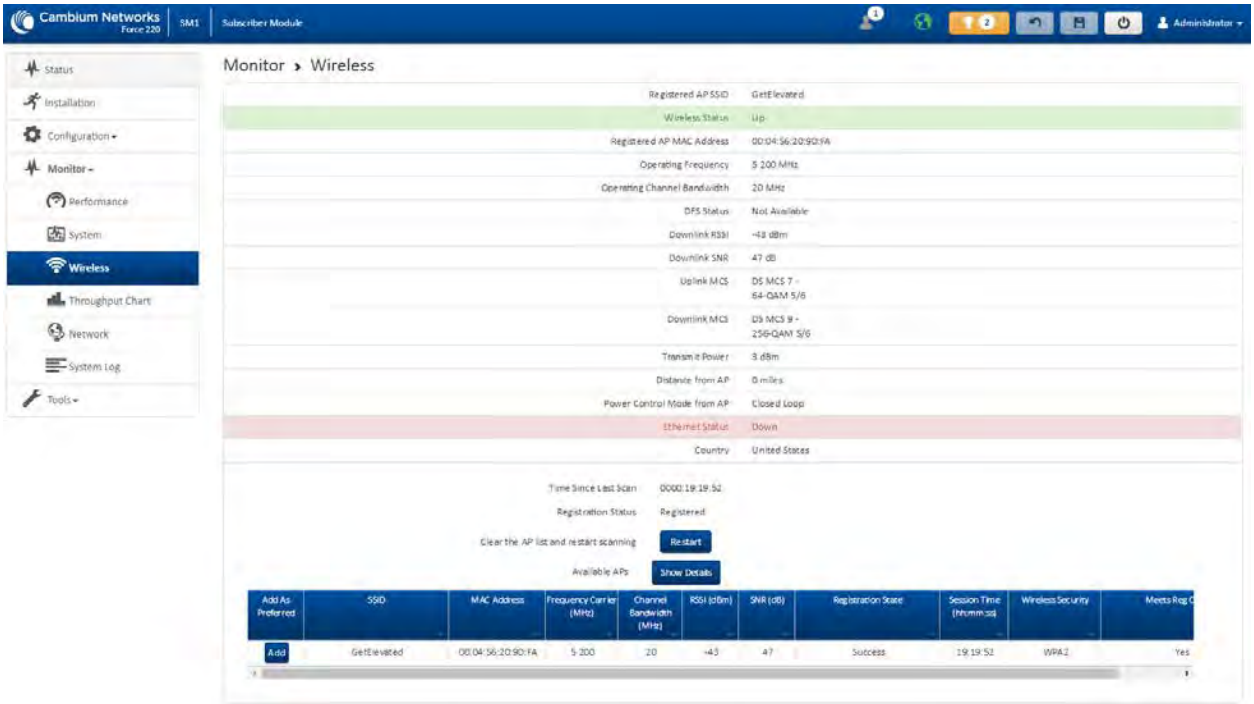


Table 51 Monitor > Wireless page attributes

Attribute	Meaning
Registered Access Point SSID (Subscriber Module Mode only	SSID of the Access Point to which the Subscriber Module is registered.
Wireless Status (Access Point Mode)	Up: The device wireless interface is functioning and sending beacons. Down: The device wireless interface has encountered an error disallowing full operation. Reset the device to reinitiate the wireless interface.
Wireless Status (Subscriber Module Mode)	Up: The device wireless interface is functioning and the device has completed network entry. Down: The device wireless interface has encountered an error disallowing full operation. Evaluate radio and security configuration on the Access Point and Subscriber Module device to determine the network entry failure.
Registered Access Point MAC Address (Subscriber	Wireless MAC address of the Access Point to which the Subscriber Module is registered.

Attribute	Meaning
Module Mode)	
Range (Subscriber Module Mode)	The calculated distance from the Access Point, determined by radio signal propagation delay.
Operating Frequency	The current frequency at which the device is operating.
Operating Channel Bandwidth	The current channel size at which the device is transmitting and receiving.
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 the 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.
Downlink RSSI (Subscriber Module Mode)	The level of the signal being received from the Access Point.
Downlink SNR (Subscriber Module Mode)	The Signal-to-Noise Ratio of the signal being received from the Access Point.
Transmitter Power	The current power level at which the device is transmitting.
Uplink MCS (Subscriber	Specifies the current MCS utilized for uplink transmission.

Attribute	Meaning
Module Mode)	
Registered Subscriber Modules (Access Point Mode)	The count of registered Subscriber Modules.
Ethernet Status	The speed and duplex at which the configured LAN port is operating.
Country	Defines the country code being used by the device. The country code of the Subscriber Module follows the country code of the associated Access Point unless it is an FCC SKU in which case the country code is the United States or Canada. Country code defines the regulatory rules in use for the device.
Registered Subscriber Modules (Access Point Mode) Deregister	Use the Registered Subscriber Modules table to monitor the registered Subscriber Module device, their key RF status, and statistics information. The Subscriber management interface may also be accessed by clicking the hyperlinks in the IPv4 / IPv6 Addresses and Device Name columns. Click the Deregister button to disassociate the Subscriber Module device from the Access Point.
MAC Address (Access Point Mode)	The MAC address of the Subscriber Module wireless interface.
IPv4 / IPv6 Addresses (Access Point Mode)	The IP address of the Subscriber Module wireless interface.
Device Name (Access Point Mode)	The configured device name of the Subscriber Module wireless interface.
SM Distance (miles)	Indicates the calculated distance of the Subscriber Module from the Access Point.
Session Time (hh:mm:ss) (Access Point Mode)	The time duration for which the Subscriber Module has been registered and in session with the Access Point.
RSSI (dBm)	Indicates the estimated RSSI of the AP at the SM (first value) and the RSSI of the SM

Attribute	Meaning
Downlink / Uplink	measured at the AP (second value).
SNR (dB) Downlink / Uplink	Indicates the estimated SNR of the AP at the SM (first value) and the SRN of the SM measured at the AP (second value).
MCS Downlink / Uplink (Access Point Mode)	Current MCS at which the downlink (first value) and uplink (second value) are operating.
Downlink Quality (Access Point Mode)	The downlink quality based on the current MCS and PER (Packet Error Rate) for this SM.
Downlink Capacity (Access Point Mode)	The downlink capacity based on the current DL MCS with respect to the highest supported MCS (MCS15). The downlink capacity based on the current DL MCS with respect to the highest supported MCS (MCS15).
MU- MIMO Gain	Indicates if MU-MIMO is supported by the subscriber and the MU-MIMO gain achieved by MU-MIMO capable subscribers.
Model Name	Model of Subscriber Module
Add As Preferred (Subscriber Module Mode)	Click the Add Add button to add the Access Point to the Preferred Access Points List under Configuration>Radio.
SSID (Subscriber Module Mode)	The SSID of the visible Access Point.
MAC Address (Subscriber Module Mode)	The MAC address of the visible Access Point.
Frequency Carrier (MHz) (Subscriber	The current operating frequency of the visible Access Point.

Attribute	Meaning
Module Mode)	
Channel Bandwidth (MHz) (Subscriber Module Mode)	The current operating channel bandwidth of the visible Access Point.
RSSI (dBm) (Subscriber Module Mode)	The current measured Received Signal Strength Indicator at the Access Point.
SNR (dB) (Subscriber Module Mode)	The current measured Signal-to-Noise Ratio of the Subscriber Module to Access Point link.
Registration State (Subscriber Module Mode)	The indication of the result of the Subscriber Module device network entry attempt: Successful: Subscriber Module registration is successful Failed: Out of Range: The Subscriber Module is out of the Access Point's configured maximum range (Max Range parameter) Failed: Capacity limit reached at Access Point: The Access Point is no longer allowing Subscriber Module network entry due to capacity reached Failed: No Allocation on Access Point: The Subscriber Module to Access Point handshaking failed due to a misconfigured pre-shared key between the Subscriber Module and Access Point Failed: SW Version Incompatibility: The version of software resident on the Access Point is older than the software version on the Subscriber Module Failed: PTP Mode: ACL Policy: The Access Point is configured with PTP Access set to MAC Limited and the Subscriber Module's MAC address is not configured in the Access Point's PTP MAC Address field Failed: Other: The Access Point does not have the required available memory to allow network entry
Session Time (hh:mm:ss) (Subscriber Module Mode)	This timer indicates the time elapsed since the Subscriber Module registered to the Access Point.
Wireless	This field indicates the security state of the Access Point to Subscriber Module link.

Attribute	Meaning
Security (Subscriber Module Mode)	
Meets Reg Criteria (Subscriber Module Mode)	Yes: The scanned Access Point meets the Network Entry criteria defined by the internal Network Algorithm. No: The scanned Access Point does not meet the Network Entry criteria defined by the internal Network Algorithm.

Monitor > Throughput Chart page

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

Figure 31 Monitor > Throughput Chart page

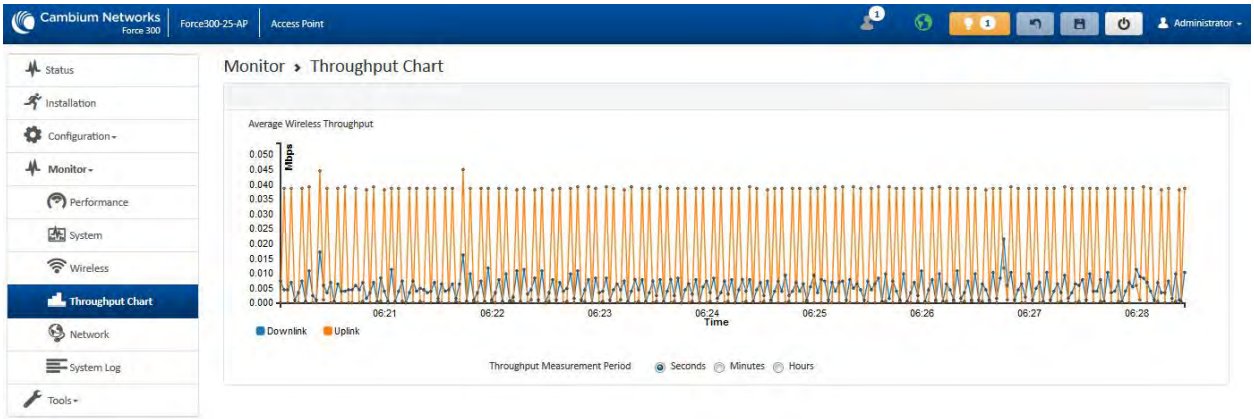


Table 52 Monitor > Throughput Chart page attributes

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

Monitor > GPS page (Access Point Mode)

Use the GPS Status page to reference key information about the device GPS readings, tracked satellites, and firmware version.

Figure 32 Monitor > GPS page attributes (Access Point Mode)

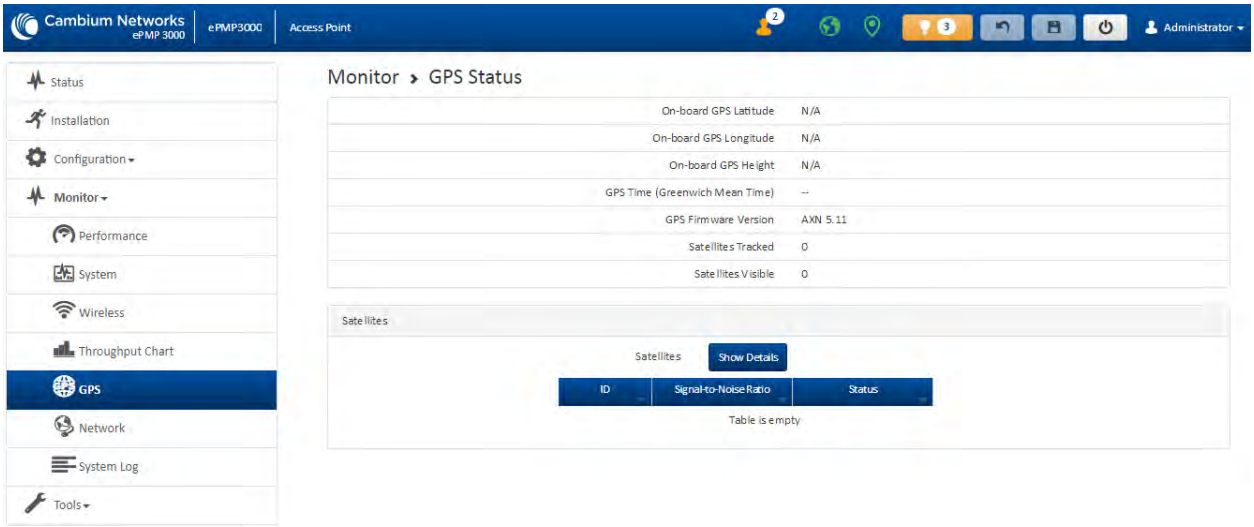


Table 53 Monitor > GPS page attributes (Access Point Mode)

Attribute	Meaning
On- board GPS Latitude (Access Point Mode)	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Latitude information from the on-board GPS chip.
On- board GPS Longitude (Access Point Mode)	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device Longitude information from the on-board GPS chip.
On- board GPS Height (Access Point Mode)	On a GPS Synchronized ePMP radio, the field is automatically populated with the Device height above sea level from the onboard GPS chip.
GPS Time (Greenwich Mean Time) (Access Point Mode)	On a GPS Synchronized ePMP radio, the field is automatically populated with the time from the onboard GPS chip.
GPS Firmware version (Access Point Mode)	On a GPS Synchronized ePMP radio, the field indicates the current firmware version of the onboard GPS chip.
Satellites Tracked	On a GPS Synchronized ePMP radio, the field indicates the number of satellites current tracked by the onboard GPS chip.

Attribute	Meaning
(Access Point Mode)	
Satellites Visible (Access Point Mode)	On a GPS Synchronized ePMP radio, the field indicates the number of satellites visible to the on-board GPS chip.
Satellites (Access Point Mode)	The **Satellites** table provides information about each satellite that is visible or tracked along with the Satellite ID and Signal to Noise Ratio (SNR) of the satellite.
ID (Access Point Mode)	Represents the Satellite ID.
Signal- to- Noise Ratio (Access Point Mode)	This is an expression of the carrier signal quality with respect to signal noise.
Status (Access Point Mode)	Status of each Satellite available.

Monitor > Network page

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

Figure 33 Monitor > Network page

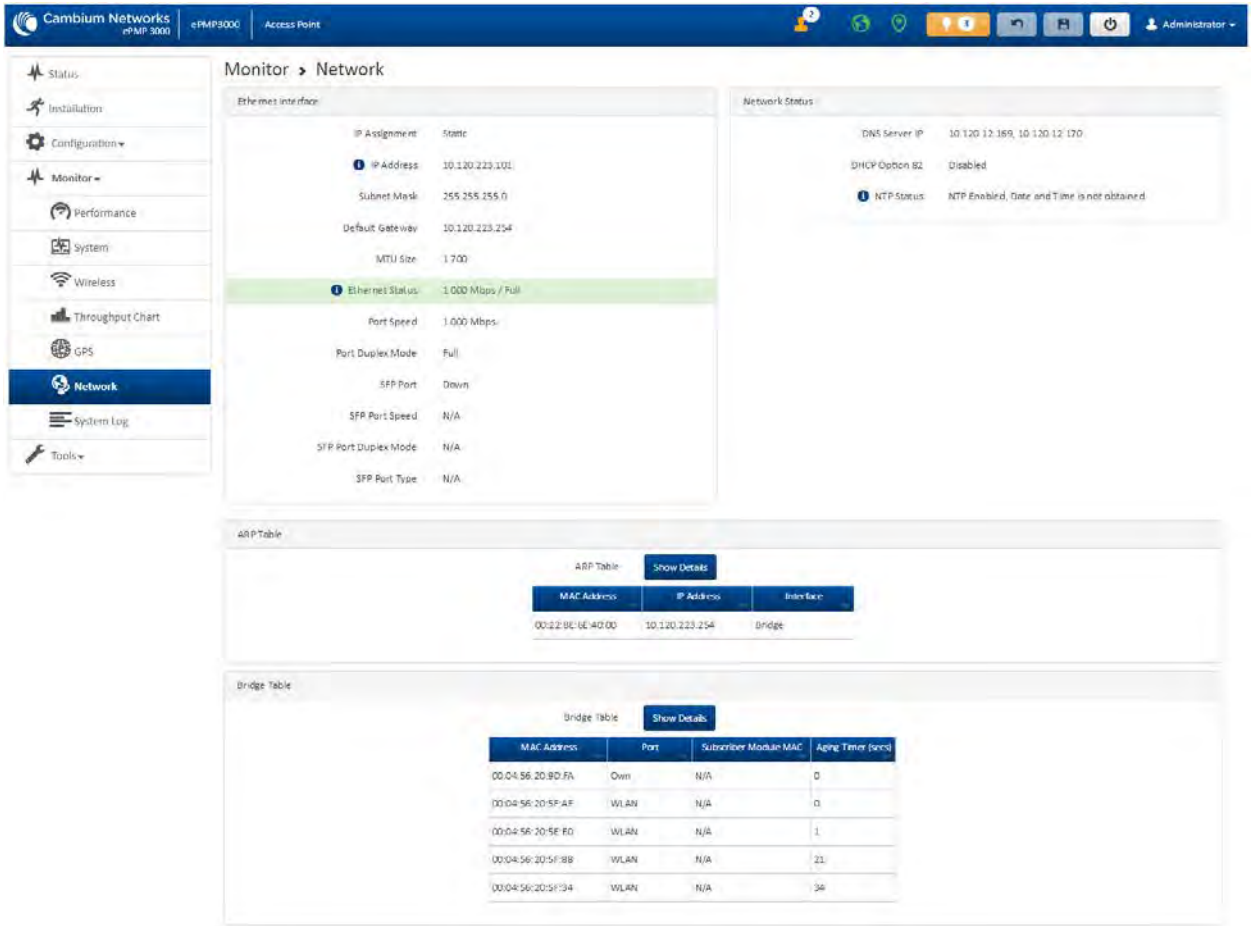


Table 54 Monitor > Network page attributes

Attribute	Meaning
Ethernet Interface	
IP Assignment	Static: Device management IP addressing is configured manually in fields IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server. DHCP: Device management IP addressing (IP Address, Subnet Mask, Gateway, and DNS Server) is assigned via a network DHCP server, and parameters IP Address, Subnet Mask, Gateway, Preferred DNS Server, and Alternate DNS Server are not configurable.
IP Address	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. If IP Address Assignment 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 (Access Point) or 192.168.0.2 (Subscriber Module).
Subnet	Defines the address range of the connected IP network. For example, if Device IP Address

Attribute	Meaning
Mask	(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.
Default Gateway	Configure the IP address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
MTU Size	The currently configured Maximum Transmission Unit for the device 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.
Main PSU Port	The speed and duplex at which the configured LAN port is operating.
Port Speed	The speed at which the configured LAN port is operating.
Port Duplex Mode	The duplex at which the configured LAN port is operating.
Network Status	
DNS Server IP	The configured IP address(es) of the network DNS servers.
DHCP Option 82	Status of DHCP Option 82 operation in the network.
NTP Status	Represents the status of NTP retrieval in the network.
ARP Table	
MAC Address	MAC Address of the devices on the bridge.
IP Address	IP Address of the devices on the bridge.
Interface	The interface on which the ePMP identified the devices on.
Bridge Table	
MAC Address	The hardware address of the ePMP device.
Port	The port to which the device is connected.
Subscriber Module MAC	MAC Address for the connected Subscriber Module device.
Aging Timer (secs)	Time set for the MAC addresses in the Bridge table before renewal.

Monitor > System Log Page

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

Figure 34 Monitor > System Log page

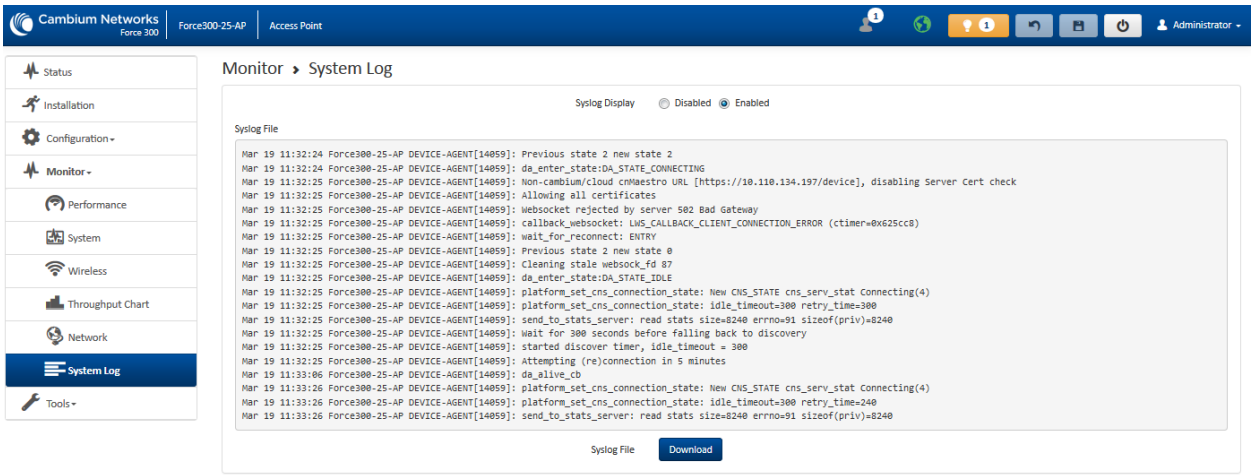


Table 55 Monitor > System Log page attributes

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

Tools menu

The Tools menu provides several options for upgrading device software, configuration backup/restore, managing licenses, analyzing RF spectrum, testing the wireless link, testing network connectivity, and analyzing interferers.

Tools > Software Upgrade page

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

Attention

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

The Release Notes may be accessed at the Cambium Support Center.

Figure 35 Tools > Software Upgrade page

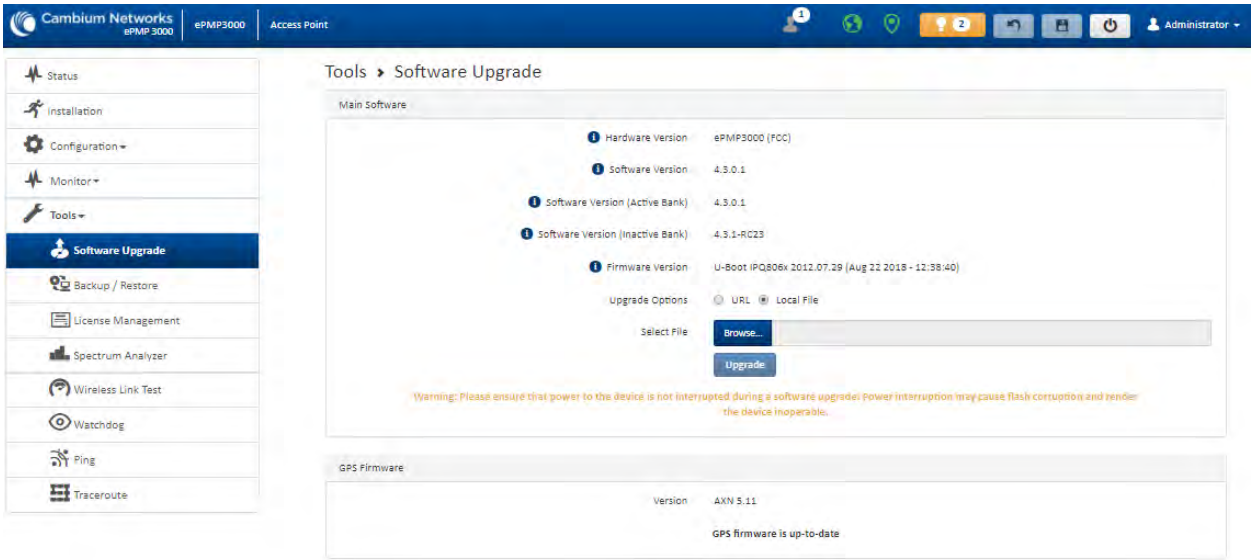


Table 56 Tools > Software Upgrade page attributes

Attribute	Meaning
Main Software	
Hardware Version	Defines the board type and frequency band of operation.
Software Version	Defines the current operating software version.
Software Version (Active Bank)	ePMP devices two banks of flash memory which each contain a version of the software. The version of the software last upgraded onto the Flash memory is made the Active Bank. This software will be used by the device when rebooted.
Software Version (Inactive Bank)	The version of the software that was the Active Bank is made the Inactive Bank when another version of the software is upgraded onto the Flash memory. The Inactive Bank of software will be used by the device in case the Active Bank cannot be used due to a failure condition.
Firmware Version	The current U-boot version.
Upgrade Options	URL: A web server may be used to retrieve software upgrade packages (downloaded to the device via the webserver). For example, if a web server is running at IP address 192.168.2.1 and the software upgrade packages are located in the home directory, an operator may select an option From URL and configure the Software Upgrade Source field to http://192.168.2.1/<software_upgrade_package>. Local File: Click Browse to select the local file containing the software upgrade package.
Select	Click Browse to select a local file (located on the device accessing the web management

Attribute	Meaning
File	interface) for upgrading the device software.
Upgrade	Click the Upgrade button to begin the software upgrade process. Please ensure that power to the device is not interrupted during a software upgrade. Power interruption may cause flash corruption and render the device inoperable.
GPS Firmware	
Firmware Version	The current firmware of the on-board GPS chip.
Upgrade Options	URL: A web server may be used to retrieve GPS firmware upgrade packages (downloaded to the device via the webserver). For example, if a web server is running at IP address 192.168.2.1 and the firmware upgrade packages are located in the home directory, an operator may select an option From URL and configure the GPS Firmware Upgrade Source field to http://192.168.2.1/<firmware_upgrade_package>. Local File: Click Browse to select the local file containing the GPS firmware upgrade package.
Select File	Click Browse to select a local file (located on the device accessing the web management interface) for upgrading the on-board GPS chip firmware.

Tools > Backup/Restore page

Use the Backup/Restore page to update the device radio software to take advantage of new software features and improvements.

Figure 36 Tools > Backup/Restore page

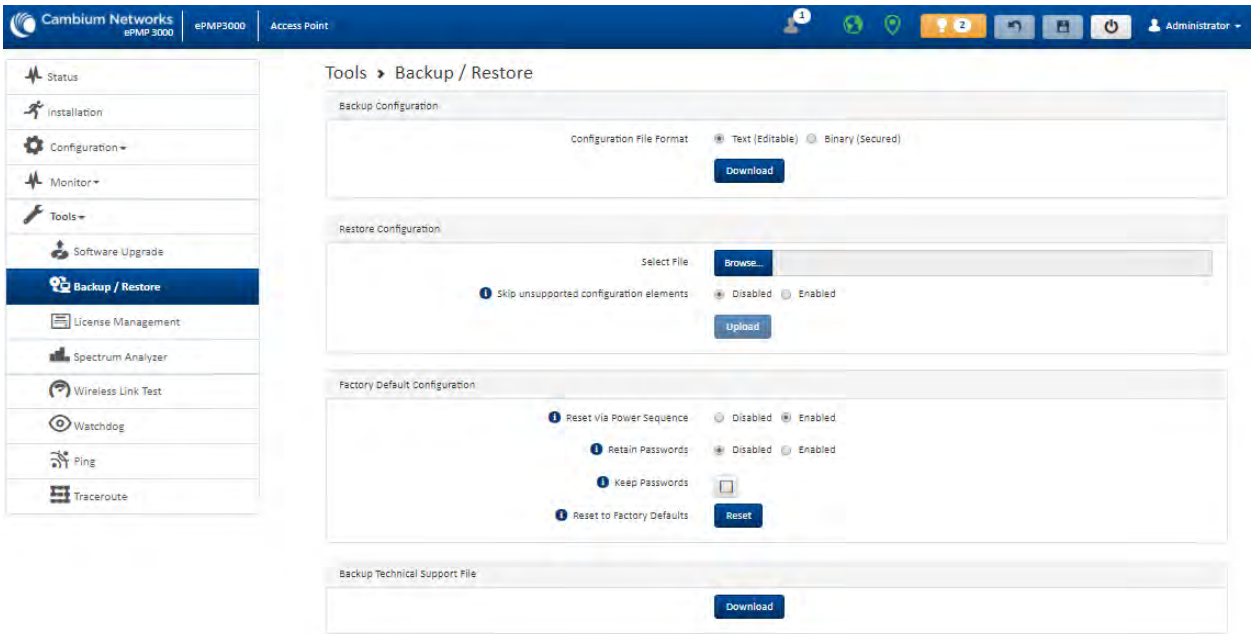


Table 57 Tools > Backup/Restore page attributes

Attribute	Meaning
Backup Configuration	
Configuration File Format	Text (Editable): Choosing this option will download the configuration file in the .json format and can be viewed and/or edited using a standard text editor. Binary (Secured): Choosing this option will download the configuration file in the .bin format, and cannot be viewed and/or edited using an editor. Use this format for a secure backup.
Restore Configuration	
Select File	Click Browse to select a local file (located on the device accessing the web management interface) for restoring the device configuration.
Skip unsupported configuration elements	In the case of configuration incompatibility, the unsupported configuration elements can be ignored and skipped.
Factory Default Configuration	
Reset Via Power Sequence	Enabled: When Enabled, it is possible to reset the radio's configuration to factory defaults using the power cycle sequence explained under Resetting ePMP to factory defaults by power cycling on page "Resetting ePMP to factory defaults by power cycling" on page 163. Disabled: When Disabled, it is not possible to factory default the radio's configuration using the power cycle sequence.
Retain Passwords	When set to Enabled, then after a factory default of the radio for any reason, the passwords used for GUI and CLI access will not be defaulted and will remain unchanged. The default value of this field is Disabled. If the passwords cannot be retrieved after the factory default, access to the radio will be lost/unrecoverable. This feature prevents unauthorized users from gaining access to the radio for any reason, including theft.
Keep Passwords	When the Keep Passwords checkbox is selected, the passwords used for GUI and CLI access will not be defaulted and will remain unchanged. This is a one-time option, and it does not apply to factory default procedures completed by power cycling (Reset Via Power Sequence).
Reset to Factory Defaults	Use this button to reset the device to its factory default configuration. A reset to factory default configuration resets all device parameters. With the Subscriber Module device in the default configuration, it may not be able to register to an Access Point device configured for your network.
Backup Technical Support File	
Download	The Backup Technical Support File is a compressed archive of the applicable statistics and configuration parameters used by Cambium Support for troubleshooting. This file is downloaded from the ePMP device to the accessing device.

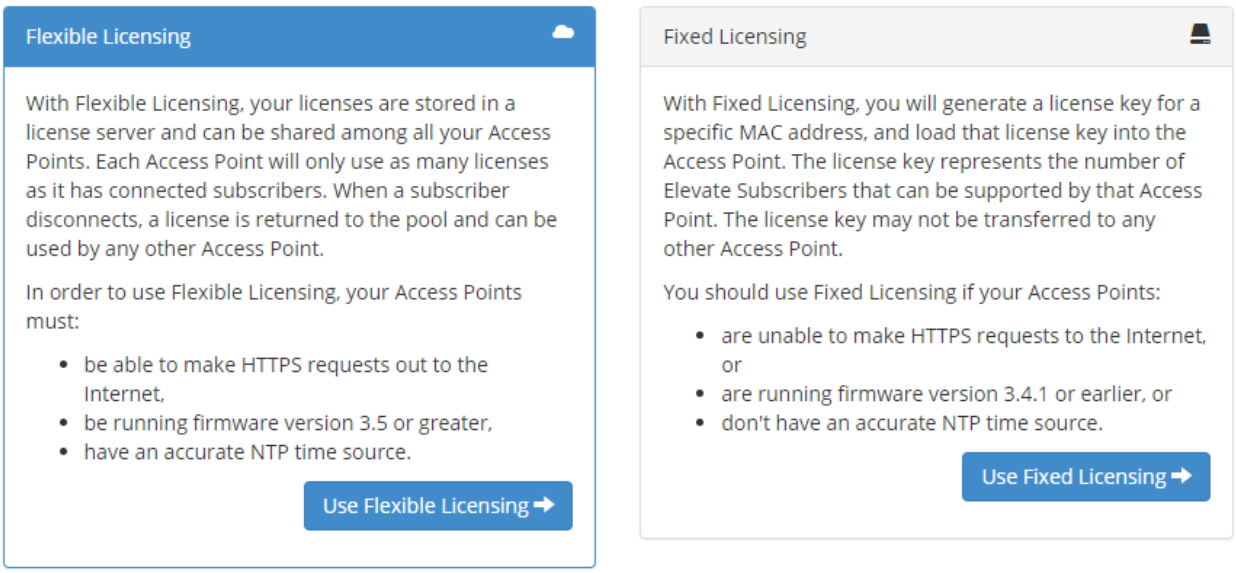
Tools > License Management page (Access Point Mode)

The AP's **License Management** page is used to:

- Install licensing for ePMP Elevate subscriber access allotments
- Convert the AP from Lite (10 subscribers) to Full (120 subscribers)
- Configure the Country Code ETSI-locked devices

There are two types of ePMP Elevate license management mechanisms available on the ePMP device – Flexible and Fixed, described below:

Figure 37 AP ePMP Elevate license management options



> **Note**
>
> Elevate Flexible Licensing is available only for ePMP AP devices with GPS sync.

Country Code configuration for ETSI locked device and Full Capacity Keys for AP Lite devices are available only via Fixed License Management. Elevate is available via Fixed or Flexible License Management.

> **Note**
>
> To use flexible licensing, the AP must have DNS server access to be able to resolve URLs (and communicate with the license server). Also, the AP must have a valid, accurate time server (NTP) connection.

Figure 38 Tools > License Management page

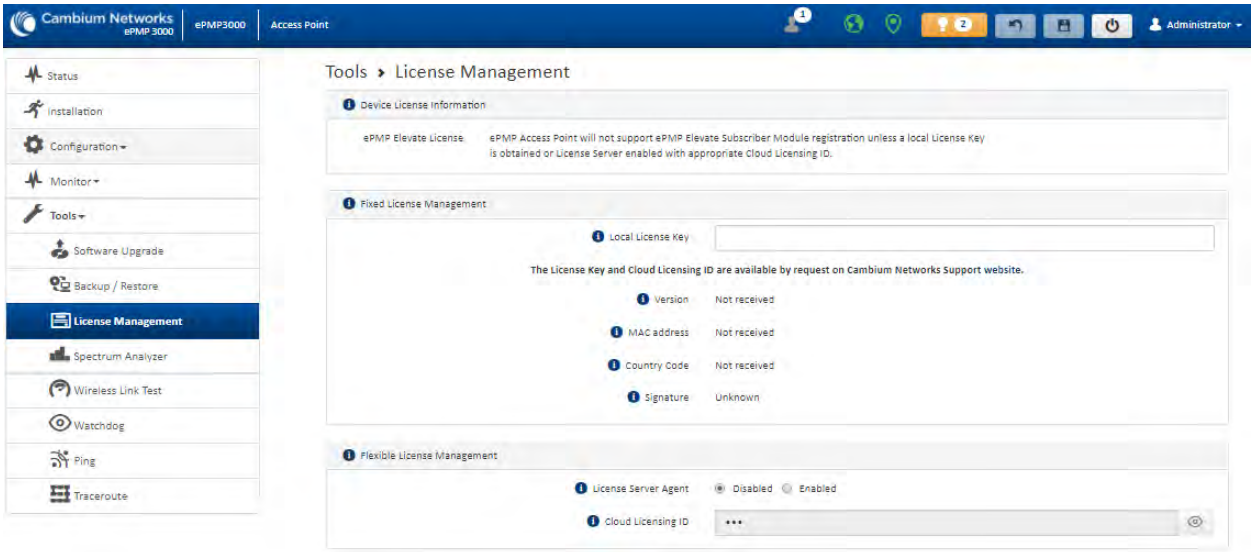


Table 58 Tools > License Management attributes

Attribute	Meaning
Flexible License Management	
License Server Agent	Disabled: No communication with the License Server is established Enabled: Enables License Server functionality to obtain the number of allowed ePMP Elevate SMs to be connected to the AP
Cloud Licensing ID	This field represents a Cambium Networks customer identification used for AP identification on the License Server. This identifier is generated upon License Entitlement activation at the Cambium Networks web-based Support Center.
Connection Status	The Connection Status displays the License Server process state when the License Server Agent is Enabled. This status may also be referenced on the device Home page.
Enable Proxy	Disabled: The AP must have a valid internet connection to reach the license server Enabled: A proxy server is specific for license server access from a private network
Proxy Server IP Address	Specify the IP address of the proxy server used for internet access from a private network
Proxy Server Port	Specify the port used on the proxy server for internet access from a private network
Refresh Requests Failed	The number of failed refresh (polling) requests to the License Server. The ePMP Elevate Subscriber Module Limit resets to 1 after the 3rd failed refresh request.
Update Requests Failed	The number of failed updates (licensing information transfer) requests to the License Server. The ePMP Elevate Subscriber Module Limit resets to 1 after the 5th failed updated request.

Attribute	Meaning
NTP Status	Represents whether or not the current time and date have been retrieved from the configured NTP server
ePMP Elevate Subscriber Module Limit	The number of ePMP Elevate devices allowed to register to the AP
Flexible License Management	
Local License Key	The "License Key" is obtained from support.cambiumnetworks.com and must be entered into this field to enable additional functionality (registration capacity, ePMP Elevate support) of the ePMP device.
Version	Specifies the licensing version scheme for the License Key
MAC address	The MAC Address is extracted from the License Key and must match the MAC Address of this device for the licenses to be enacted.
Country Code	A two-character value representing the licensed country
Subscriber Module Limit	ePMP Lite / Force 110 devices are limited to 10 SMs in AP TDD mode. SM Limit will display Unlocked if a license is present which allows no limit of SMs to register to the device in AP TDD mode.
Signature	A valid License Key must have a valid signature included. The status is displayed after a License Key is entered and saved. Licenses can only be used if the signature is valid.

Tools > Spectrum Analyzer page

Use the Spectrum Analyzer page to measure signal levels of frequencies across the full range of the device or in a custom range.

Figure 39 Tools > Spectrum Analyzer page

Table 59 Tools > Spectrum Analyzer page attributes

Attribute	Meaning
Spectrum Analyzer	Disabled: The Spectrum Analyzer process is not running on the device. Enabled: The Spectrum Analyzer process is running on the device, necessary for displaying results in the web management interface.
Range	Full Available Range: The entire operating range of the device will be scanned. Custom: The device scans only the range defined by Lower Frequency and Upper Frequency.
Lower / Upper Frequency	When Range is configured to Custom, it indicates the range in MHz for which the device will scan.
cnDiscovery Mode	Light: Only management frames will be captured for interferer detection. Some interferers may not be discovered. Scanning results may slightly vary from actual environmental conditions. Hard: Management, control, and data frames will be captured for interferer detection. All Interferers will be discovered. It is recommended to use this mode with caution, as it may result in performance degradation.
Scanning	Click Pause to pause scanning, and Clear Data to reset the displayed results.

Tools > eAlign page

Use the eAlign page to aid with subscriber link alignment.

Figure 40 Tools > eAlign page

Note

A valid link to an SM is required to provide meaningful RSSI measurements.

Attention

ePMP supports Automatic Transmit Power Control (ATPC) where the Subscriber Module devices are instructed by the Access Point to adjust their Tx power in order for the Subscriber Module device signal (UL RSSI) to arrive at the Access Point at a predetermined RSSI level (configurable on the Access Point under Configuration>Radio>Power Control>Subscriber Module Target Receive Level). This feature is beneficial to keep the overall noise floor in the sector to an acceptable level. However, the feature negates the purpose of eAlign measurements on the Access Point device since, during the alignment, the Subscriber Module may constantly change its Tx power. It is recommended to turn off ATPC and set the Subscriber Module Tx power to maximum allowable power during alignment.

While aligning the link using eAlign, please follow these steps:

Procedure:

1. On the Subscriber Module, set Configuration > Radio > Power Control > Max Tx Power to Manual.
2. Set Configuration > Radio > Power Control > Transmitter Power to 26

dBm (or maximum value allowed by regulations).

3. Click the Save button
4. Perform link alignment using eAlign
5. Once alignment is complete, set Configuration>Radio>Power Control>Max Tx Power back to Auto
6. Click the Save button

Tools > Wireless Link Test page

Use the Wireless Link Test page to conduct a simple test of wireless throughput. This allows the user to determine the throughput that can be expected on a particular link without having to use external tools.

Figure 41 Tools > Wireless Link Test page

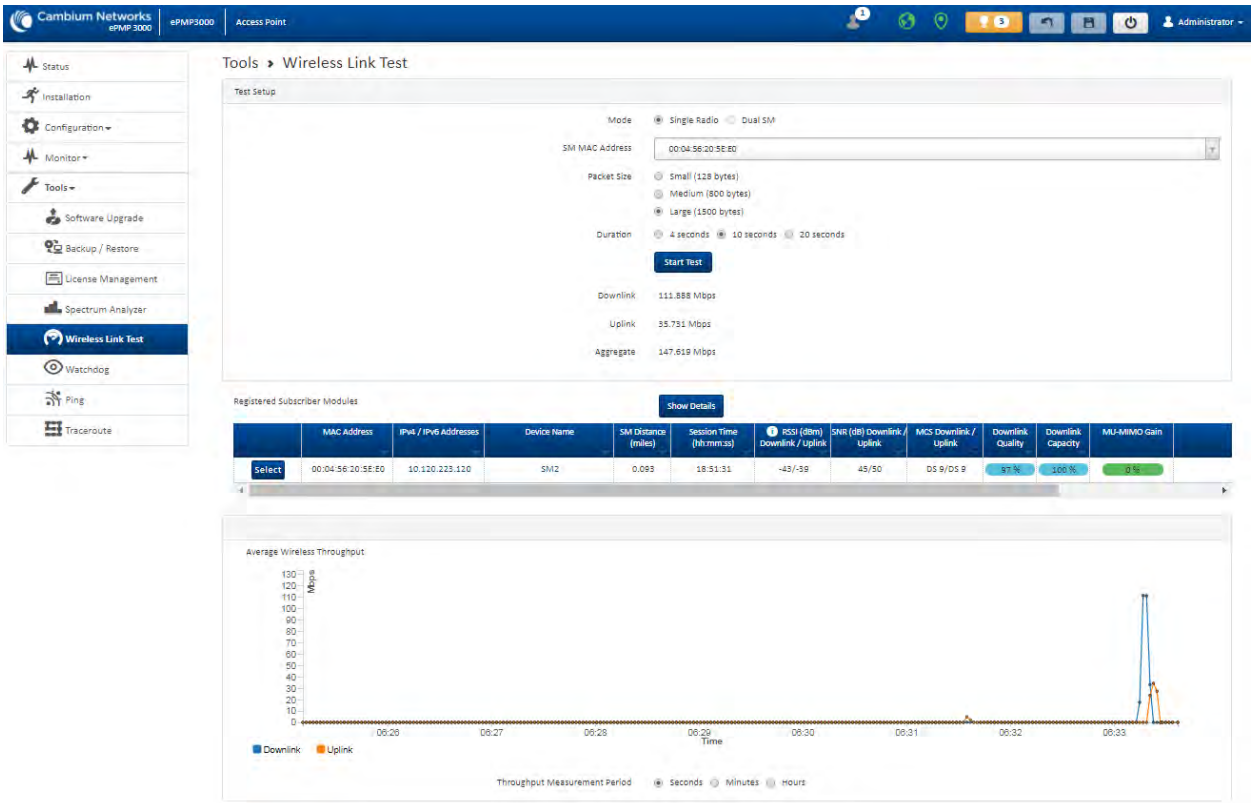


Table 60 Tools > Wireless Link Test page attributes

Attribute	Meaning
Test Setup	
Mode	Single Radio: The link test is conducted between the Access Point and one Subscriber Module Dual SM: The link test is conducted between the Access Point and two grouped Subscriber Modules (must be operating in MU-MIMO mode).

Attribute	Meaning
SM MAC Address	Choose the MAC Address of the Subscriber Module with which the wireless link test will be conducted.
Packet Size	Choose the Packet Size to use for the throughput test
Duration	Choose the time duration in seconds to use for the throughput test
Downlink	This field indicates the result of the throughput test on the downlink, in Mbps
Uplink	This field indicates the result of the throughput test on the uplink, in Mbps
Average	An auto-adjusting chart displaying the average throughput of the link
Registered Subscriber Modules	This table provides information about the wireless link of each registered Subscriber Module.

Tools > Watchdog page

Watchdog performs ping checks to determine the reachability of a target IP address. If the target IP address is unreachable, a chosen action is performed.

Figure 42 Tools > Watchdog page

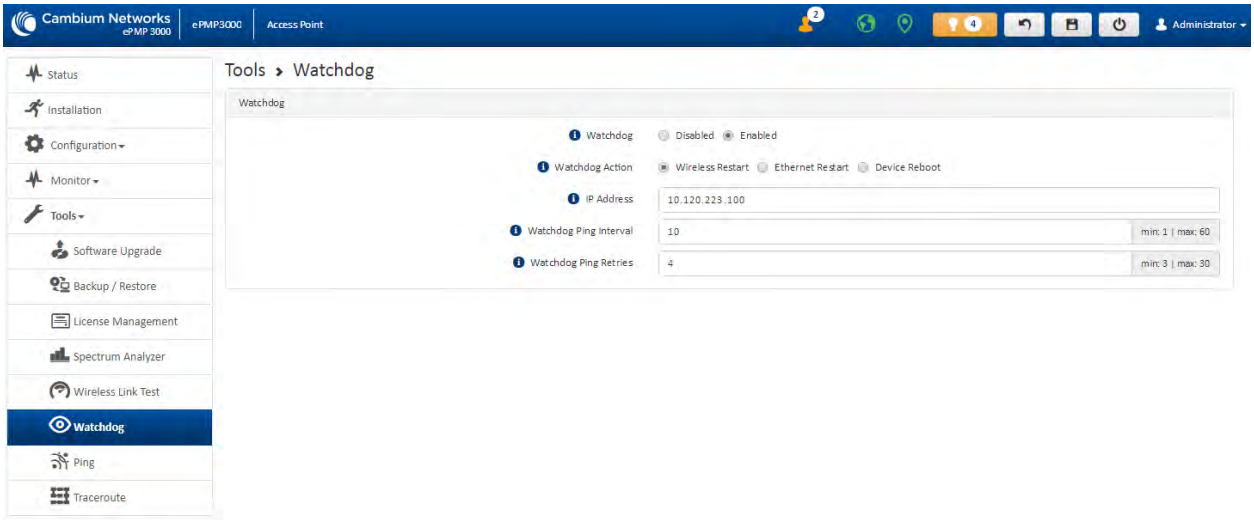


Table 61 Tools > Watchdog page attributes

Attribute	Meaning
Test Setup	
Watchdog	Disabled: The device does not ping a specified IP address periodically for verification of connectivity Enabled: The device periodically pings the IP address specified. If IP connectivity is lost, the action defined in Watchdog Action is performed.

Attribute	Meaning
Watchdog Action	Wireless Restart: In case of lost ping connectivity to the specified IP address, the device automatically restarts the wireless interface. Ethernet Restart: In case of lost ping connectivity to the specified IP address, the device automatically restarts the Ethernet interface. Device Reboot: In case of lost ping connectivity to the specified IP address, the device automatically reboots.
IP Address	Indicates the target IP address for which the device attempts ping connectivity diagnostics.
Watchdog Ping Interval	Indicates the interval in minutes between each ping connectivity diagnostic.
Watchdog Ping Retries	Indicates the number of ping retries executed by the device prior to considering the test failed (and conducting the action defined in Watchdog Action).

Tools > Ping page

Use the Ping page to conduct a simple test of IP connectivity to other devices that 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 device, or there may be a failure in the network hardware (i.e. DNS server failure).

Figure 43 Tools > Ping page

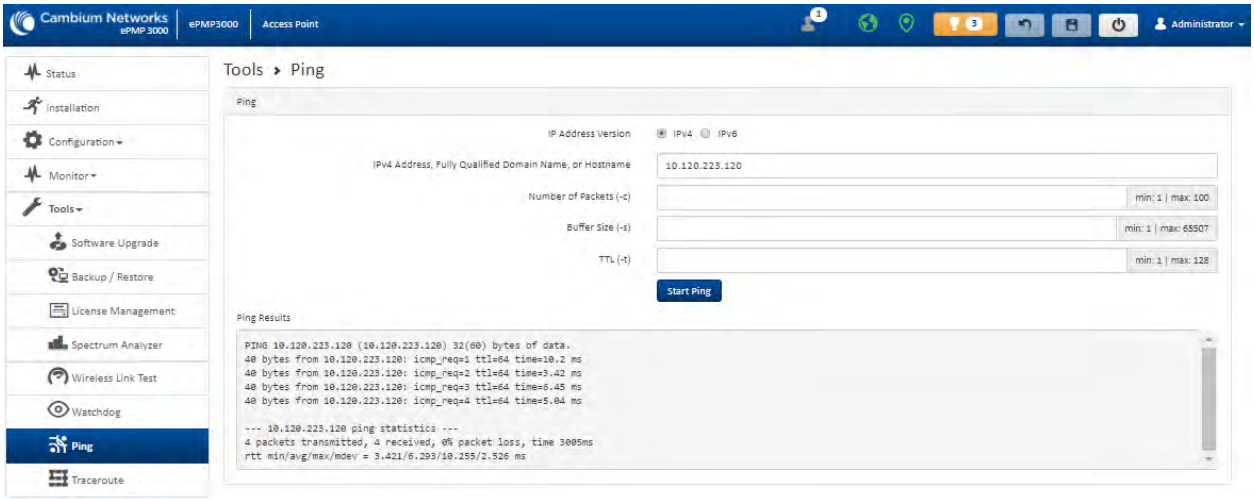


Table 62 Tools > Ping page attributes

Attribute	Meaning
Ping	
IP Address Version	IPv4: The ping test is conducted via the IPv4 protocol. IPv6: The ping test is conducted via the IPv6 protocol.

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.
Ping results	The results of the ping test are displayed in the box.

Tools > Traceroute page

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

Figure 44 Tools > Traceroute page

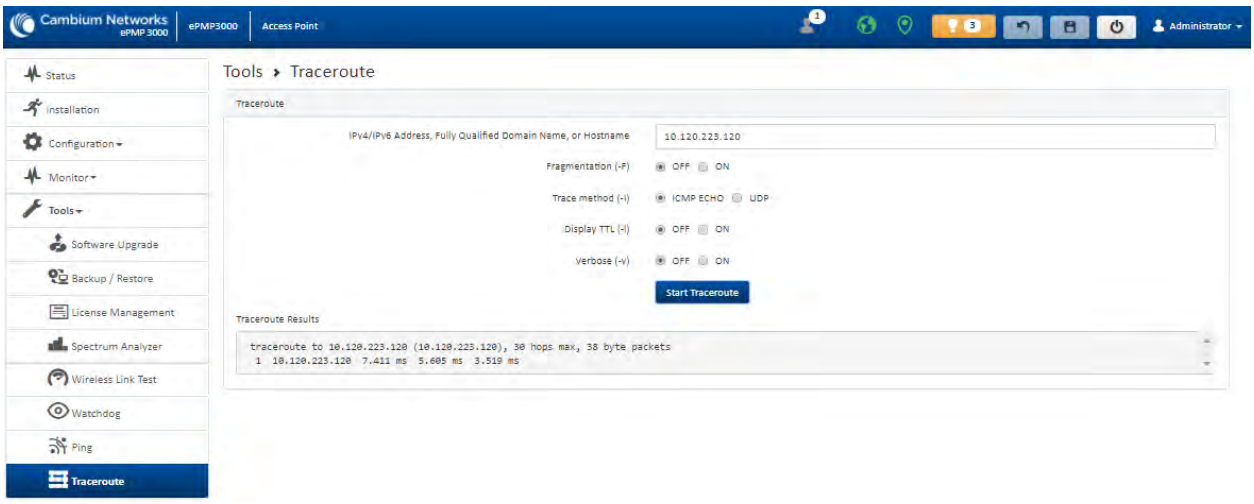


Table 63 Tools > Traceroute page attributes

Attribute	Meaning
Traceroute	
IP Address	Enter the IP address of the target of the traceroute diagnostic.
Fragmentation (-F)	ON: Allow the source and target to fragment probe packets. OFF: Do not fragment probe packets (on the source or target).
Trace method (-I)	ICMP ECHO: Use ICMP ECHO for traceroute probes. UDP: Use UDP for traceroute probes.
Display TTL (-l)	ON: Display TTL values for each hop on the route. OFF: Suppress display of TTL values for each hop on the route.

Attribute	Meaning
Verbose (-v)	ON: ICMP packets other than TIME_EXCEEDED and UNREACHABLE are displayed in the output. OFF: Suppress display of extraneous ICMP messaging.
Traceroute Results	Traceroute test results are displayed in the box.

Chapter 5: Operation and Troubleshooting

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

- General Planning for Troubleshooting on page "General Planning for Troubleshooting" below
- Upgrading device software on page "Upgrading device software" on the next page
- Testing hardware on page "Testing hardware" on the next page
- Troubleshooting the radio link on page "Troubleshooting the radio link" on page 162
- Resetting ePMP to factory defaults by power cycling on page "Resetting ePMP to factory defaults by power cycling" on page 163

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

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, follow this procedure:

Procedure:

1	Log in to the device GUI via the management IP
2	Navigate to page Tools, Software Upgrade
3	Under the Main Software section, set the Upgrade Option to URL to pull the software file from a network software server or select Local File to upload a file from the accessing device. If URL is selected, enter the server IP address, Server Port, and File path.
4	If Local File is selected, click Browse to launch the file selection dialogue
5	Click Upgrade Do not power off the unit in the middle of an upgrade process.
6	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 device to equipment inside the building, are of the supported type, as defined in Ethernet cabling on page "Ethernet cabling" on page 71

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 "Power LED is off" on the next page
- Ethernet LED is off on page "Ethernet LED is off" on the next page

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 device 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 device and the power supply.

Action: The fault may be in the LAN or device cable:

- Remove the LAN cable from the power supply, examine it and confirm it is not faulty.
- If the PC connection is working, remove the AP/SM cable from the power supply, examine it, and check that the wiring to pins 1,2 and 3,6 is correct and not crossed.

Test Ethernet packet errors reported by the device

Log in to the device 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 "Test ping packet loss" below.

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 device is connected to a managed Ethernet switch or router, it may be possible to monitor the error rate of Ethernet packets. Please refer to the user guide of the managed network equipment. The test has passed if the rate of packet errors reported by the managed Ethernet switch or router is less than 10 in 1 million packets.

Test ping packet loss

Using a computer, it is possible to generate and monitor packets lost between the power supply and the AP/SM. This can be achieved by executing the Command Prompt application which is supplied as standard with Windows and Mac operating systems.

Attention

This procedure disrupts network traffic carried by the device under test.

Procedure:

1. Ensure that the IP address of the computer is configured appropriately for connection to the device under test, and does not conflict with other devices connected to the network.
2. If the power supply is connected to an Ethernet switch or router then connect the computer to a spare port, if available.
3. If it is not possible to connect the computer to a spare port of an Ethernet switch or router, then the

power supply must be disconnected from the network 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 SM under test.

   If the computer is running a MAC operating system, this is achieved by typing:

   ping –c 1000 –s 1492 <ipaddress>

   where <ipaddress> is the IP address of the AP/SM under test.

6. Record how many Ping packets are lost. This is reported by Command Prompt on completion of the test.

   The test has passed if the number of lost packets is less than 2.

Troubleshooting the radio link

This section describes how to test the link when there is no radio communication, when it is unreliable, or when the data throughput rate is too low. It may be necessary to test both ends of the link.

The module has lost or does not establish radio connectivity

If there is no wireless activity, follow this:

Procedure:

1	Check that the devices are configured with the same Frequency Carrier.
2	Check that the Channel Bandwidth is configured the same at both ends of the link.
3	On the Access Point, verify that the Max Range setting is configured to a distance slightly greater than the distance between the Access Point and the other end of the link.
4	Check that the Access Point Synchronization Source is configured properly based on the network configuration.
5	Verify the authentication settings on the devices. if Authentication Type is set to WPA2, verify that the Pre-shared Key matches between the Access Point and the Subscriber Module Preferred Access Points List.
6	Check that the software at each end of the link is the same version.
7	Check that the desired Access Point SSID is configured in the Subscriber Module Preferred Access Points List.

8	On the Subscriber Module, check the DL RSSI and DL CINR values. Verify that for the Subscriber Module installed distance, that the values are consistent with the values reported by the LINKPlanner tool.
9	Check Tx Power on the devices
10	Check that the link is not obstructed or 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 device fault to Cambium Networks.

Module exhibiting frequent boots or disconnects

For any Force 300-16 units exhibiting frequent disconnects or reboots, the 4.4 official release must be applied twice to ensure both banks are updated. Once completed, please make sure both banks are running 4.4 under Monitor → System. In general, this practice can be followed for all 802.11ac models as they support two banks for software storage.

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 Access Point page Monitor, Wireless Status
2	Check that the RSSI values reported at the device are proper based on the distance of the link – the LINKPlanner tool is designed to estimate these values.
3	Check that the path loss is low enough for the communication rates required.
4	Check that the device has not become misaligned.
5	Review your Quality of Service configuration and ensure that traffic is properly classified and prioritized.

Resetting ePMP to factory defaults by power cycling

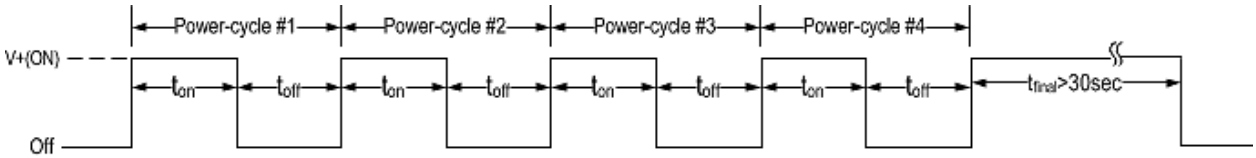
Operators may reset an ePMP radio to the default factory configuration by a sequence of power cycling (removing and re-applying power to the device). This procedure allows operators to perform a factory default reset without a tower climb or additional tools. The procedure is depicted in Figure 45 Power cycle timings.

Procedure:

1	Remove the Ethernet cable from PoE jack of the power supply for at least 10 seconds.
2	Reconnect the Ethernet cable to re-supply power to the ePMP device for 3-5 seconds and

	disconnect cable to power off the ePMP device for 3-5 seconds. (1st power cycle)
3	Reconnect the Ethernet cable to re-supply power to the ePMP device for 3-5 seconds and disconnect cable to power off the ePMP device for 3-5 seconds. (2nd power cycle)
4	Reconnect the Ethernet cable to re-supply power to the ePMP device for 3-5 seconds and disconnect cable to power off the ePMP device for 3-5 seconds. (3rd power cycle)
5	Reconnect the Ethernet cable to re-supply power to the ePMP device for 3-5 seconds and disconnect cable to power off the ePMP device for 3-5 seconds. (4th power cycle)
6	Reconnect the Ethernet cable to re-supply power to the ePMP device for at least 30 seconds and allow it to go through the boot-up procedure (Note: Device will go through an additional reset automatically). This will reset the current configuration files to factory default configuration (e.g. IP addresses, Device mode, RF configuration, etc.). The device can be pinged from a PC to check if boot up is complete (Successful ping replies indicates boot-up is complete).
7	Access the ePMP device using the default IP address of 192.168.0.1 (AP) or 192.168.0.2 (SM).

Figure 45 Power cycle timings



Where:	Is:
V+(ON)	Power through PoE has been applied to the device
Off	Power through PoE has been removed from the device
t_{on}	The time duration for which the device has been powered on. This should be 3-5 seconds.
t_{off}	The time duration for which the device has been powered off. This should be 3-5 seconds.

1. Chapter 6: Legal and reference information

This chapter provides legal notices including software license agreements.

> **Attention**
>
> 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 "Cambium Networks end user license agreement" below
- Hardware warranty on page "Hardware warranty" on page 231
- Limit of liability on page "Limit of liability" on page 231
- Compliance with safety standards on page "For up-to-date data, please refer to:" on page 231 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 "Compliance with radio regulations" on page 241 describes how the ePMP complies with the radio regulations that are enforced in various countries.
- Notifications on page "Notifications" on page 243 contain notes made to regulatory bodies for the ePMP.

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 are 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.

Source Code Requests

Where required under the terms of the open source software license applicable to Cambium's use of each of the following open source software packages, for at least three (3) years from the date of your receipt of the copy of such open source software, Cambium will provide to any party who contacts us at the contact information provided below a copy of the source code for the version of the requested open source software used in this Cambium product.

Cambium Networks

Atrium, 3800 Golf Rd #360

Rolling Meadows, IL 60008

QCA
Tensilica
Linux Kernel

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. 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 Library 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.

GNU GENERAL PUBLIC LICENSE
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 promo"
u-boot	"# (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 "
firewall	/* * firewall3 - 3rd OpenWrt UCI firewall implementation * * Copyright (C) 2013-2014 Jo-Philipp Wich <jow@openwrt.org> * * 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. */
fstools	/* * Copyright (C) 2014 John Crispin <blogic@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. */

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. */ /* * * Modified for AF_INET6 by Pedro Roque * * <roque@di.fc.ul.pt> *

	* Original copyright notice included bellow */ /* * 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. */
jsonfilter	/* * Copyright (C) 2013- 2014 Jo- Philipp Wich <jow@openwrt.org> * * 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. */
klish	Overview This package contains code which is copyrighted to multiple sources. ========== 3Com Corporation The intial public release of this software was developed by Graeme McKerrell whilst in the employment of 3Com Europe Ltd. Copyright (c) 2005, 3Com Corporation 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 3Com Corporation 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 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 THE COPYRIGHT OWNER 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. ========== Newport Networks Ltd. The 0.6-0.7 releases of this software was developed by Graeme McKerrell whilst in the employment of Newport Networks Ltd. As well as enhancing the existing code the new modules were developed. Copyright (c) 2005,2006, Newport Networks Ltd 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 Newport Networks Ltd 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 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 THE COPYRIGHT OWNER 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. ========== Serj Kalichev The klish is a fork of original clish. Copyright (c) 2010 Serj Kalichev. 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. The name of the author 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 THE COPYRIGHT OWNER 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.

librpc	/* * Sun RPC is a product of Sun Microsystems, Inc. and is provided for * unrestricted use provided that this legend is included on all tape * media and as a part of the software program in whole or part. Users * may copy or modify Sun RPC without charge, but are not authorized * to license or distribute it to anyone else except as part of a product or * program developed by the user. * * SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE * WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR * PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. * * Sun RPC is provided with no support and without any obligation on the * part of Sun Microsystems, Inc. to assist in its use, correction, * modification or enhancement. * * SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE * INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC * OR ANY PART THEREOF. * * In no event will Sun Microsystems, Inc. be liable for any lost revenue * or profits or other special, indirect and consequential damages, even if * Sun has been advised of the possibility of such damages. * * Sun Microsystems, Inc. * 2550 Garcia Avenue * Mountain View, California 94043 */ /* * Copyright (C) 1984, Sun Microsystems, Inc. */
libubox	/* * Copyright (C) 2010- 2012 Felix Fietkau <nbd@openwrt.org> * * 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.

	*/
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- 2012 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. ===== (end of COPYRIGHT)
LuaSrcDiet	LuaSrcDiet License - - - - - - - - - - - - - - - - - - LuaSrcDiet is licensed under the terms of the MIT license reproduced below. This means that LuaSrcDiet is free software and can be used for

	both academic and commercial purposes at absolutely no cost. Think of LuaSrcDiet as a compiler or a text filter; whatever that is processed by LuaSrcDiet is not affected by its license. It does not add anything new into your source code; it only transforms code that already exist. Hence, there is no need to tag this license onto Lua programs that are only processed. Given the liberal terms of this kind of license, the primary purpose is just to claim authorship of LuaSrcDiet. Parts of LuaSrcDiet is based on Lua 5 code. See the file COPYRIGHT_Lua51 (Lua 5.1.4) for Lua 5's license. ========== ===== Copyright (C) 2005-2008,2011 Kein-Hong Man <keinhong@gmail.com> Lua 5.1.4 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. ========== ===== (end of COPYRIGHT)
lzma	LZMA SDK 4.65

	- - - - - - - - - - - - - LZMA SDK provides the documentation, samples, header files, libraries, and tools you need to develop applications that use LZMA compression. LZMA is default and general compression method of 7z format in 7- Zip compression program (www.7- zip.org). LZMA provides high compression ratio and very fast decompression. LZMA is an improved version of famous LZ77 compression algorithm. It was improved in way of maximum increasing of compression ratio, keeping high decompression speed and low memory requirements for decompressing. LICENSE - - - - - - - LZMA SDK is written and placed in the public domain by Igor Pavlov. LZMA SDK Contents - - - - - - - - - - - - - - - - - LZMA SDK includes: - ANSI- C/C++/C#/Java source code for LZMA compressing and decompressing - Compiled file->file LZMA compressing/decompressing program for Windows system
nat46	* Copyright (c) 2013- 2014 Andrew Yourtchenko <ayourtch@gmail.com> * * 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.
netifd	/* * netifd - network interface daemon * Copyright (C) 2012 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. */
procd	/* * Copyright (C) 2013 Felix Fietkau <nbd@openwrt.org> * Copyright (C) 2013 John Crispin <blogic@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. */
rpcd	/* * rpcd - UBUS RPC server * * Copyright (C) 2013 Felix Fietkau <nbd@openwrt.org> * Copyright (C) 2013- 2014 Jo- Philipp Wich <jow@openwrt.org> * * 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. */
ubox	/* * Copyright (C) 2013 Felix Fietkau <nbd@openwrt.org> * Copyright (C) 2013 John Crispin <blogic@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. */
ubus	/* * Copyright (C) 2011- 2014 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. */
uci	/* * 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 Lesser General Public License for more details. */
uClibc++	/* Copyright (C) 2004 Garrett A. Kajmowicz This file is part of the uClibc++ Library. 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; either version 2.1 of the License, or (at your option) any later version. 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. You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA */
uhttpd	/*

	* uhttpd - Tiny single- threaded httpd * * Copyright (C) 2010- 2013 Jo- Philipp Wich <xm@subsignal.org> * Copyright (C) 2013 Felix Fietkau <nbd@openwrt.org> * * 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. */
usign	/* * usign - tiny signify replacement * * Copyright (C) 2015 Felix Fietkau <nbd@openwrt.org> * * 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. */
attr	/* * Copyright (c) 2001- 2003,2005 Silicon Graphics, Inc. * All Rights Reserved. * * This program 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, either version 2.1 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 Lesser General Public License for more details. * * You should have received a copy of the GNU Lesser General Public License * along with this program. If not, see <http://www.gnu.org/licenses/>. */
bc	/* A Bison parser, made by GNU Bison 2.1. */ /* Skeleton parser for Yacc- like parsing with Bison, Copyright (C) 1984, 1989, 1990, 2000, 2001, 2002, 2003, 2004, 2005 Free Software Foundation, Inc. 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, 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., 51 Franklin Street, Fifth Floor, Boston, MA 02110- 1301, USA. */ /* As a special exception, when this file is copied by Bison into a Bison output file, you may use that output file without restriction. This special exception was added by the Free Software Foundation in version 1.24 of Bison. */ /* Written by Richard Stallman by simplifying the original so called ``semantic'' parser. */ /* All symbols defined below should begin with yy or YY, to avoid infringing on user name space. This should be done even for local variables, as they might otherwise be expanded by user macros. There are some unavoidable exceptions within include files to define necessary library symbols; they are noted "INFRINGES ON USER NAME SPACE" below. */
bridge-utils	/* * Copyright (C) 2000 Lennert Buytenhek

	* 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., 675 Mass Ave, Cambridge, MA 02139, USA. */
busybox	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 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.
bzip2	This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996- 2010 Julian R Seward. 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. 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. 3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written

	permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``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 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. Julian Seward, jseward@bzip.org bzip2/libbzip2 version 1.0.6 of 6 September 2010
conntrack-tools	/* * (C) 2006- 2012 by Pablo Neira Ayuso <pablo@netfilter.org> * (C) 2011- 2012 by Vyatta Inc <http://www.vyatta.com> * * 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., 675 Mass Ave, Cambridge, MA 02139, USA. */
curl	COPYRIGHT AND PERMISSION NOTICE Copyright (c) 1996 - 2015, Daniel Stenberg, <daniel@haxx.se>. All rights reserved. Permission to use, copy, modify, and 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", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. 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. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.
device-agent	/* ========== == Name : common.c Author : Subi S S Version : Copyright : Copyright (C) 2013 Cambium Networks, Ltd. All Rights Reserved CAMBIUM NETWORKS CONFIDENTIAL PROPRIETARY Description : Functions which are useful for all platforms. ========== == */
dnsmasq	/* dnsmasq is Copyright (c) 2000- 2015 Simon Kelley 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. 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, see <http://www.gnu.org/licenses/>. */

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: Copyright (c) 2002-2014 Matt Johnston Portions copyright (c) 2004 Mihnea Stoenescu All rights reserved. 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. ===== 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: PuTTY is copyright 1997- 2003 Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A. 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 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. ===== curve25519-donna: /* Copyright 2008, Google Inc. * 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 Google Inc. 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 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 THE COPYRIGHT * OWNER 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. * * curve25519-donna: Curve25519 elliptic curve, public key function * * http://code.google.com/p/curve25519-donna/ * * Adam Langley <agl@imperialviolet.org> * * Derived from public domain C code by Daniel J. Bernstein <djb@cr.yp.to> * * More information about curve25519 can be found here * http://cr.yp.to/ecdh.html

	* * djb's sample implementation of curve25519 is written in a special assembly * language called qhasm and uses the floating point registers. * * This is, almost, a clean room reimplementation from the curve25519 paper. It * uses many of the tricks described therein. Only the crecip function is taken * from the sample implementation. */
ebtables	/* * ebtables.c, v2.0 July 2002 * * Author: Bart De Schuymer * * This code was stongly inspired on the iptables code which is * Copyright (C) 1999 Paul `Rusty' Russell & Michael J. Neuling * * 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., 675 Mass Ave, Cambridge, MA 02139, USA. */
ethtool	ethtool is available under the terms of the GNU Public License version 2. See COPYING for details.
eventlog	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.
expat	Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Expat maintainers. 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.
file	$File: COPYING,v 1.1 2008/02/05 19:08:11 christos Exp $ Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995. Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas. This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet. 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 immediately at the beginning of the file, without modification, 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. THIS SOFTWARE IS PROVIDED BY THE AUTHOR 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.
glib/glib2	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.]
haproxy	HAPROXY's license - 2006/06/15 Historically, haproxy has been covered by GPL version 2. However, an issue appeared in GPL which will prevent external non-GPL code from being built using the headers provided with haproxy. My long-term goal is to build a core system able to load external modules to support specific application protocols. Since some protocols are found in rare environments (finance, industry, ...), some of them might be accessible only after signing an NDA. Enforcing GPL on such modules would only prevent them from ever being implemented, while not providing anything useful to ordinary users. For this reason, I *want* to be able to support binary only external modules when needed, with a GPL core and GPL modules for standard protocols, so that people fixing bugs don't keep them secretly to try to stay over competition. The solution was then to apply the LGPL license to the exportable include files, while keeping the GPL for all the rest. This way, it still is mandatory to redistribute modified code under customer request, but at the same time, it

	is expressly permitted to write, compile, link and load non-GPL code using the LGPL header files and not to distribute them if it causes a legal problem. Of course, users are strongly encouraged to continue the work under GPL as long as possible, since this license has allowed useful enhancements, contributions and fixes from talented people around the world. Due to the incompatibility between the GPL and the OpenSSL licence, you must apply the GPL/LGPL licence with the following exception: This program is released under the GPL with the additional exemption that compiling, linking, and/or using OpenSSL is allowed. The text of the licenses lies in the "doc" directory. All the files provided in this package are covered by the GPL unless expressly stated otherwise in them. Every patch or contribution provided by external people will by default comply with the license of the files it affects, or be rejected. Willy Tarreau - w@1wt.eu
i2c-tools	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. /* i2cset.c - A user-space program to write an I2C register. Copyright (C) 2001-2003 Frodo Looijaard <frodol@dds.nl>, and Mark D. Studebaker <mdsxyz123@yahoo.com> Copyright (C) 2004-2012 Jean Delvare <jdelvare@suse.de> 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., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA. */
iperf	Copyright (c) 1999-2007, The Board of Trustees of the University of Illinois

	All Rights Reserved. Iperf performance test Mark Gates Ajay Tirumala Jim Ferguson Jon Dugan Feng Qin Kevin Gibbs John Estabrook National Laboratory for Applied Network Research National Center for Supercomputing Applications University of Illinois at Urbana- Champaign http://www.ncsa.uiuc.edu 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.

	/* * ip.c "ip" utility frontend. * * 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. * * Authors: Alexey Kuznetsov, <kuznet@ms2.inr.ac.ru> */
iptables	/* * Author: Paul.Russell@rustcorp.com.au and mneuling@radlogic.com.au * * (C) 2000-2002 by the netfilter coreteam <coreteam@netfilter.org>: * Paul 'Rusty' Russell <rusty@rustcorp.com.au> * Marc Boucher <marc+nf@mbsi.ca> * James Morris <jmorris@intercode.com.au> * Harald Welte <laforge@gnumonks.org> * Jozsef Kadlecsik <kadlec@blackhole.kfki.hu> * * Based on the ipchains code by Paul Russell and Michael Neuling * * iptables - - IP firewall administration for kernels with * firewall table (aimed for the 2.3 kernels) * * See the accompanying manual page iptables (8) for information * about proper usage of this program. * * 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., 675 Mass Ave, Cambridge, MA 02139, USA. */
iw	Copyright (c) 2007, 2008 Johannes Berg Copyright (c) 2007 Andy Lutomirski Copyright (c) 2007 Mike Kershaw Copyright (c) 2008-2009 Luis R. Rodriguez 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.
jansson	Copyright (c) 2009- 2014 Petri Lehtinen <petri@digip.org> 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.
json-c	Copyright (c) 2009- 2012 Eric Haszlakiewicz 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. - Copyright (c) 2004, 2005 Metaparadigm Pte Ltd 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.
libelf	/* * elf_ repl.h - public header file for systems that lack it. * Copyright (C) 1995 - 2006 Michael Riepe * * This 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. * * 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 * Library General Public License for more details. * * You should have received a copy of the GNU Library General Public * License along with this library; if not, write to the Free Software * Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA */
libevent	Libevent is available for use under the following license, commonly known as the 3-clause (or "modified") BSD license: ========== Copyright (c) 2000-2007 Niels Provos <provos@citi.umich.edu> Copyright (c) 2007-2012 Niels Provos and Nick Mathewson 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 name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``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 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. ========== Portions of Libevent are based on works by others, also made available by them under the three-clause BSD license above. The copyright notices are available in the corresponding source files; the license is as above. Here's a list: log.c: Copyright (c) 2000 Dug Song <dugsong@monkey.org> Copyright (c) 1993 The Regents of the University of California.

	strlcpy.c: Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com> win32select.c: Copyright (c) 2003 Michael A. Davis <mike@datanerds.net> evport.c: Copyright (c) 2007 Sun Microsystems ht-internal.h: Copyright (c) 2002 Christopher Clark minheap-internal.h: Copyright (c) 2006 Maxim Yegorushkin <maxim.yegorushkin@gmail.com> ========== The arc4module is available under the following, sometimes called the "OpenBSD" license: Copyright (c) 1996, David Mazieres <dm@uun.org> Copyright (c) 2008, Damien Miller <djm@openbsd.org> Permission to use, copy, modify, and 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.
libffi	libffi - Copyright (c) 1996- 2012 Anthony Green, Red Hat, Inc and others. See source files for details. 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. /* ---------- ffi.c - Copyright (c) 1996, 1998, 1999, 2001, 2007, 2008 Red Hat, Inc. Copyright (c) 2002 Ranjit Mathew Copyright (c) 2002 Bo Thorsen Copyright (c) 2002 Roger Sayle Copyright (C) 2008, 2010 Free Software Foundation, Inc. x86 Foreign Function Interface 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.
libiwinfo	* * iwinfo - Wireless Information Library - Broadcom wl.o Backend * * Copyright (C) 2009 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/. * * This code is based on the wlc.c utility published by OpenWrt.org . */
libnetfilter_conntrack	/* * (C) 2005- 2011 by Pablo Neira Ayuso <pablo@netfilter.org> * Harald Welte <laforge@netfilter.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; either version 2 of the License, or * (at your option) any later version. */
libnetfilter_cthelper	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.
libnetfilter_cttimeout	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.
libnetfilter_queue	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.
libnfnetlink	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.

libnl	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 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. [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.]
libpcap	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.
libwebsockets	/* * libwebsockets - small server side websockets and web server implementation * * Copyright (C) 2010-2014 Andy Green <andy@warmcat.com> * * 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. * * 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. * * You should have received a copy of the GNU Lesser General Public * License along with this library; if not, write to the Free Software * Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, * MA 02110-1301 USA */

libxml2	Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are: Copyright (C) 1998- 2012 Daniel Veillard. All Rights Reserved. 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, FIT- NESS 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.
lighttpd	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 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 THE COPYRIGHT OWNER 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.
Linux-PAM	Unless otherwise *explicitly* stated the following text describes the licensed conditions under which the contents of this Linux- PAM release may be distributed: --- Redistribution and use in source and binary forms of Linux- PAM, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties. 2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission. ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD- style copyright.) THIS SOFTWARE IS PROVIDED ``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(S) 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. ----------
lldpd	License - - - - - - - lldpd is distributed under the ISC license: > 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. Also, `lldpcli` will be linked to GNU Readline (which is GPL licensed) if available. To avoid this, use `- - without- readline` as a configure option. /* * Copyright (c) 2008 Vincent Bernat <bernat@luffy.cx> * * 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. */
lua-cjson	Copyright (c) 2010- 2012 Mark Pulford <mark@kyne.com.au>

	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.
mcproxy	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.
minicom	Minicom is Copyright (C) 1991,1992,1993,1994,1995,1996 Miquel van Smoorenburg. 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.
miniupnpd	MiniUPnPd Copyright (c) 2006- 2015, Thomas BERNARD 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 of the author 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 THE COPYRIGHT OWNER 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.
mtd-utils	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.
net-snmp	Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. - - - - Part 1: CMU/UCD copyright notice: (BSD like) - - - - - Copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998- 2000

	Copyright 1996, 1998- 2000 The Regents of the University of California All Rights Reserved Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission. CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE 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. - - - - Part 2: Networks Associates Technology, Inc copyright notice (BSD) - - - - - Copyright (c) 2001- 2003, Networks Associates Technology, Inc 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 Networks Associates Technology, Inc 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 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 THE COPYRIGHT HOLDERS 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. - - - - Part 3: Cambridge Broadband Ltd. copyright notice (BSD) - - - - - Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. 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 of Cambridge Broadband Ltd. 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 HOLDER ``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 COPYRIGHT HOLDER 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. - - - - Part 4: Sun Microsystems, Inc. copyright notice (BSD) - - - - - Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved. Use is subject to license terms below. This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. 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 Sun Microsystems, Inc. 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 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 THE COPYRIGHT HOLDERS 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. - - - - Part 5: Sparta, Inc copyright notice (BSD) - - - - - Copyright (c) 2003- 2011, Sparta, Inc 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 Sparta, Inc 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 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 THE COPYRIGHT HOLDERS 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. - - - - Part 6: Cisco/BUPTNIC copyright notice (BSD) - - - - - Copyright (c) 2004, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications. 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 Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may 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 THE COPYRIGHT HOLDERS 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. ---- Part 7: 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> 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 of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names 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 HOLDER ``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 COPYRIGHT HOLDER 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.
odhcp6c	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.
odhcpd	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.
openssl	LICENSE ISSUES ========== The OpenSSL toolkit stays under a double 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- 2017 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
-----------------------------------------------------------------------
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * 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.
pcre	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
pm-utils	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. /* * suspend functions for machines with Mac- style pmu * * Copyright 2006 Red Hat, Inc. * * Based on work from: * Peter Jones <pjones@redhat.com> * * This program is free software; you can redistribute it and/or modify * it under the terms of version 2 of the GNU General Public License 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. * * 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 * */
ppp	
rng-tools	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Suite 500, Boston, MA 02110-1335 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. * rngd.c - - Random Number Generator daemon * * rngd reads data from a hardware random number generator, verifies it * looks like random data, and adds it to /dev/random's entropy store. * * In theory, this should allow you to read very quickly from * /dev/random; rngd also adds bytes to the entropy store periodically * when it's full, which makes predicting the entropy store's contents * harder. * * Copyright (C) 2001 Philipp Rumpf * * 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., 51 Franklin Street, Suite 500, Boston, MA 02110-1335 USA */
rp-pppoe	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. /********** * * pppoe.c * * Implementation of user- space PPPoE redirector for Linux. * * Copyright (C) 2000- 2012 by Roaring Penguin Software Inc. * * This program may be distributed according to the terms of the GNU * General Public License, version 2 or (at your option) any later version. * * LIC: GPL
rstp	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. /********** Copyright (c) 2006 EMC Corporation. 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. The full GNU General Public License is included in this distribution in the file called LICENSE. Authors: Srinivas Aji <Aji_Srinivas@emc.com>
squashfs	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. * Squashfs * * Copyright (c) 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 * Phillip Lougher <phillip@lougher.demon.co.uk> * * 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, * 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, 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
strace	/* * Copyright (c) 1991, 1992 Paul Kranenburg <pk@cs.few.eur.nl> * Copyright (c) 1993 Branko Lankester <branko@hacktic.nl> * Copyright (c) 1993, 1994, 1995, 1996 Rick Sladkey <jrs@world.std.com> * Copyright (c) 1996- 1999 Wichert Akkerman <wichert@cistron.nl> * 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. The name of the author may not be used to endorse or promote products * derived from this software without specific prior written permission. * * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``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 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. */
syslog-ng	Copyright (c) 2002- 2015 Balabit Copyright (c) 1996- 2015 Balázs Scheidler syslog- ng is licensed under the combination of the GPL and LGPL licenses. The syslog- ng core contained in the following subdirectories 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; either version 2.1 of the License, or (at your option) any later version (please refer to the file LGPL.txt for more details): lib/ libtest/ syslog- ng/ modules/java- common/ modules/java/ (native|proxies|src)/ modules/native/ 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; either version 2.1 of the License, or (at your option) any later version. 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. You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
sysstat	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. * (C) 1998- 2015 by Sebastien GODARD (sysstat <at> orange.fr) * ********** * 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 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 * ********** */
tcpdump	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. /* * Copyright (c) 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 2000 * The Regents of the University of California. All rights reserved. * * Redistribution and use in source and binary forms, with or without * modification, are permitted provided that: (1) source code distributions * retain the above copyright notice and this paragraph in its entirety, (2) * distributions including binary code include the above copyright notice and * this paragraph in its entirety in the documentation or other materials * provided with the distribution, and (3) all advertising materials mentioning * features or use of this software display the following acknowledgement: * ``This product includes software developed by the University of California, * Lawrence Berkeley Laboratory and its contributors.'' 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 ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED * WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

	* Support for splitting captures into multiple files with a maximum * file size: * * Copyright (c) 2001 * Seth Webster <swebster@sst.ll.mit.edu> */
trace-cmd	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. The applications are licensed under the GNU General Public License 2.0 (see COPYING) and the libraries are licensed under the GNU Lesser General Public License 2.1 (See COPYING.LIB).
ubi-utils	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. /* * Copyright (c) International Business Machines Corp., 2006 * * 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., 675 Mass Ave, Cambridge, MA 02139, USA. */ /* * An utility to create UBI volumes. * * Authors: Artem Bityutskiy <dedekind@infradead.org> * Frank Haverkamp <haver@vnet.ibm.com> */

	Copyright (c) 2000- 2007 by Nicolas Devillard. MIT License 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.
uClibc-ng	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 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. [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.]
wget	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. /* Miscellaneous declarations. Copyright (C) 1995, 1996, 1997, 1998, 2003 Free Software Foundation, Inc. This file is part of GNU Wget. GNU Wget 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. GNU Wget 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 Wget; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA. In addition, as a special exception, the Free Software Foundation gives permission to link the code of its release of Wget with the OpenSSL project's "OpenSSL" library (or with modified versions of it that use the same license as the "OpenSSL" library), and distribute the linked executables. You must obey the GNU General Public License in all respects for all of the code used other than "OpenSSL". If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so. If you do not wish to do so, delete this exception statement from your version. */
wireless_ tools.29	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.
xtables-addons	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.
zlib	/* zlib.h - - interface of the 'zlib' general purpose compression library version 1.2.8, April 28th, 2013 Copyright (C) 1995- 2013 Jean- loup Gailly and Mark Adler 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 The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://tools.ietf.org/html/rfc1950 (zlib format), rfc1951 (deflate format) and rfc1952 (gzip format). */

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

For up-to-date data, please refer to:

- LINKPlanner

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 64 ePMP safety compliance specifications.

Table 64 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

The minimum separation distances for each frequency variant are specified in Calculated distances and power compliance margins on page "Calculated distances and power compliance margins" on page 234.

Safety distances for FCC are given below:

- Gain 28 = 211 cm
- Gain 2 = 20 cm
- 4.9G distance = 87 cm

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.

The EMC specification type approvals that have been granted for ePMP are listed under Table 65 EMC emissions compliance.

Table 65 EMC emissions compliance

Region	Specification (Type Approvals)
USA	FCC CFR 47 Part 15 class B
Canada	RSS210, Issue 8 RSS247, Issue 1 (May 2015)
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 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 http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites_e.html and Safety Code 6.
- EN 50383:2016 Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base Subscriber Modules and fixed terminal Subscriber Modules for wireless telecommunication systems (110 MHz - 40 GHz).
- BS EN 50385:2017 Product standard to demonstrate the compliances of radio base Subscriber Modules and fixed terminal Subscriber Modules 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 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 "Human exposure to radio frequency energy" on the previous page) is:

- 10 W/m^2 for RF energy in the 5 GHz frequency band.

Calculation of power density

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

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.

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

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

The calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination is shown in the tables below. 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:

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)

Table 66 ePMP 3000 Access Point Power compliance margins, 5.1 GHz, FCC through Table 71 ePMP 3000 Access Point Power compliance margins, 5.8 GHz (full Tx power) below list the power compliance margins for the following ePMP 3000 Access Point devices:

Part Number	FCC ID	Industry Canada
C058910A102A C050910A104A	Z8H89FT0024	109W-0024

Table 66 ePMP 3000 Access Point Power compliance margins, 5.1 GHz, FCC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
AP	20 MHz	Sector, 18 dBi	0.031	63	10	0.12	0.3
AP	80 MHz	Sector, 18 dBi	0.018	63	10	0.09	0.1

Table 67 ePMP 3000 Access Point Power compliance margins, 5.8 GHz, FCC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
AP	20 MHz	Sector, 18 dBi	0.062	63	10	0.18	0.3
AP	80 MHz	Sector, 18 dBi	0.017	63	10	0.09	0.1

Table 68 ePMP 3000 Access Point Power compliance margins, 5.8 GHz, ISEDC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	S @ 20 cm (W/m^2)
AP	20 MHz	Sector, 18 dBi	0.062	63	9.69	0.18	0.3	7.72
AP	80 MHz	Sector, 18 dBi	0.017	63	9.69	0.10	0.3	2.20

Note

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

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

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

Table 69 ePMP 3000 Access Point Power compliance margins, 5.8 GHz (EIRP 36 dBm)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
AP	20 MHz	Sector, 18 dBi	0.063	63	10	0.18	0.3
AP	80 MHz	Sector, 18 dBi	0.063	63	10	0.18	0.3

Note

If there are no EIRP limits in the country of installation, use the distance

calculations in Table 70 ePMP 3000 Access Point Power compliance margins, 5.1 GHz (full Tx power) and Table 71 ePMP 3000 Access Point Power compliance margins, 5.8 GHz (full Tx power).

Table 70 ePMP 3000 Access Point Power compliance margins, 5.1 GHz (full Tx power)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
AP	20 MHz	Sector, 18 dBi	1.585	63	10	1.41	2.0
AP	80 MHz	Sector, 18 dBi	1.585	63	10	1.41	2.0

Table 71 ePMP 3000 Access Point Power compliance margins, 5.8 GHz (full Tx power)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
AP	20 MHz	Sector, 18 dBi	1.585	63	10	1.41	2.0
AP	80 MHz	Sector, 18 dBi	1.585	63	10	1.41	2.0

Table 72 Force 300-25 Power compliance margins, 5.1 GHz, FCC through Table 75 Force 300-25 Power compliance margins, 5.8 GHz, ISEDC below list the power compliance margins for the following Force 300-25 devices:

Part Number	FCC ID	Industry Canada
C058910C102A C050910C104A	Z8H89FT0017	109W-0017

Table 72 Force 300-25 Power compliance margins, 5.1 GHz, FCC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	D (m)	R (m)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.000389	316	10	0.03	0.1
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.000141	316	10	0.02	0.1
PTP SM	20 MHz	On-board, 2 dBi	0.957194	2	10	0.11	0.3
PTP SM	80 MHz	On-board, 2 dBi	0.058614	2	10	0.03	0.1

Table 73 Force 300-25 Power compliance margins, 5.8 GHz, FCC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	D (m)	R (m)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.001660	316	10	0.06	0.1
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.000719	316	10	0.04	0.1
PTP SM	20 MHz	On-board, 2 dBi	0.997700	2	10	0.11	0.3
PTP/ SM	80 MHz	On-board, 2 dBi	0.276058	2	10	0.06	0.1

Table 74 Force 300-25 Power compliance margins, 5.1 GHz, ISEDC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	S @ 20 cm (W/m^2)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.000389	316	9.01	0.03	0.1	0.24
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.000141	316	9.01	0.02	0.1	0.09
PTP SM	20 MHz	On-board, 2 dBi	0.957194	2	9.01	0.12	0.3	3.02
PTP SM	80 MHz	On-board, 2 dBi	0.058614	2	9.01	0.03	0.1	0.18

Table 75 Force 300-25 Power compliance margins, 5.8 GHz, ISEDC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	S @ 20 cm (W/m^2)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.001660	316	9.69	0.07	0.1	1.04
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.000719	316	9.69	0.04	0.1	0.45
PTP SM	20 MHz	On-board, 2 dBi	0.997700	2	9.69	0.11	0.3	3.15

PTP SM	80 MHz	On-board, 2 dBi	0.276058	2	9.69	0.06	0.1	0.87

Note

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

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

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

Table 76 Force 300-25 Power compliance margins, 5.8 GHz (EIRP 36 dBm)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.012589	316	10	0.18	0.2
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.012589	316	10	0.18	0.2

Note

If there are no EIRP limits in the country of installation, use the distance calculations in Table 77 Force 300-25 Power compliance margins, 5.1 GHz (full Tx power) and Table 78 Force 300-25 Power compliance margins, 5.8 GHz (full Tx power).

Table 77 Force 300-25 Power compliance margins, 5.1 GHz (full Tx power)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.794	316	10	1.41	2.0
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.794	316	10	1.41	2.0

Table 78 Force 300-25 Power compliance margins, 5.8 GHz (full Tx power)

Conn Type	Channel Bandwidth	Antenna	P	G	S	d	R

			(W)		(W/m^2)	(m)	(m)
PTP SM	20 MHz	Integrated Dish, 25 dBi	0.794	316	10	1.41	2.0
PTP SM	80 MHz	Integrated Dish, 25 dBi	0.794	316	10	1.41	2.0

Table 79 Force 300-16 Power compliance margins, 5.1 GHz, FCC through Table 85 Force 300-16 Power compliance margins, 5.8 GHz (full Tx power) below list the power compliance margins for the following Force 300-16 devices:

Part Number	FCC ID	Industry Canada
C058910C112A C058910C114A	Z8H89FT0016	109W-0016

Table 79 Force 300-16 Power compliance margins, 5.1 GHz, FCC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Patch Array, 16 dBi	0.021	40	10	0.08	0.1
PTP SM	80 MHz	Patch Array, 16 dBi	0.013	40	10	0.06	0.1
PTP SM	20 MHz	On-board, 2 dBi	0.678	2	10	0.09	0.1
PTP SM	80 MHz	On-board, 2 dBi	0.089	2	10	0.03	0.1

Table 80 Force 300-16 Power compliance margins, 5.8 GHz, FCC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Patch Array, 16 dBi	0.830	40	10	0.51	0.7
PTP SM	80 MHz	Patch Array, 16 dBi	0.1	40	10	0.18	0.3
PTP	20 MHz	On-board, 2 dBi	0.830	2	10	0.11	0.3

SM							
PTP SM	80 MHz	On-board, 2 dBi	0.389	2	10	0.07	0.1

Table 81 Force 300-16 Power compliance margins, 5.1 GHz, ISEDC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	S @ 20 cm (W/m^2)
PTP SM	20 MHz	Patch Array, 16 dBi	0.021	40	9.01	0.09	0.1	1.69
PTP SM	80 MHz	Patch Array, 16 dBi	0.013	40	9.01	0.07	0.1	1.02
PTP SM	20 MHz	On-board, 2 dBi	0.678	2	9.01	0.10	0.3	2.14
PTP SM	80 MHz	On-board, 2 dBi	0.089	2	9.01	0.04	0.1	0.28

Table 82 Force 300-16 Power compliance margins, 5.8 GHz, ISEDC

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)	S @ 20 cm (W/m^2)
PTP SM	20 MHz	Patch Array, 16 dBi	0.830	40	9.69	0.18	0.3	65.72
PTP SM	80 MHz	Patch Array, 16 dBi	0.1	40	9.69	0.18	0.3	7.92
PTP SM	20 MHz	On-board, 2 dBi	0.830	2	9.69	0.10	0.2	2.62
PTP SM	80 MHz	On-board, 2 dBi	0.389	2	9.69	0.07	0.1	1.23

Note

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

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

At EU 5.8 GHz the products are generally limited to a fixed EIRP which can be

achieved with the Integrated Antenna. The calculations above assume that the maximum EIRP allowed by the regulations is being transmitted.

Table 83 Force 300-16 Power compliance margins, 5.8 GHz (EIRP 36 dBm)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Patch Array, 16 dBi	0.1	40	10	0.18	0.3
PTP SM	80 MHz	Patch Array, 16 dBi	0.1	40	10	0.18	0.3

Note

If there are no EIRP limits in the country of installation, use the distance calculations in Table 84 Force 300-16 Power compliance margins, 5.1 GHz (full Tx power) and Table 85 Force 300-16 Power compliance margins, 5.8 GHz (full Tx power).

Table 84 Force 300-16 Power compliance margins, 5.1 GHz (full Tx power)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Patch Array, 16 dBi	0.794	40	10	0.5	1.0
PTP SM	80 MHz	Patch Array, 16 dBi	0.794	40	10	0.5	1.0

Table 85 Force 300-16 Power compliance margins, 5.8 GHz (full Tx power)

Conn Type	Channel Bandwidth	Antenna	P (W)	G	S (W/m^2)	d (m)	R (m)
PTP SM	20 MHz	Patch Array, 16 dBi	0.794	40	10	0.5	1.0
PTP SM	80 MHz	Patch Array, 16 dBi	0.794	40	10	0.5	1.0

Compliance with radio regulations

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

Attention

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.

The radio specification type approvals that have been granted for ePMP frequency variants are listed under Table 65 EMC emissions compliance.

Table 86 Force 300-25 Radio certifications

Frequency band	Region	Regulatory approvals
5 GHz	USA	FCC Part 15 Class B
	Canada	IC RSS-210 Issue 8, Annex 8 (or latest) IC RSS247 Issue 1 (May 2015)
	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. To comply with FCC RF exposure limits for general population or uncontrolled exposure, the antenna(s) used for the ePMP transmitter must be installed to ensure a separation distance specified in Table 66 ePMP 3000 Access Point Power compliance margins, 5.1 GHz, FCC through Table 85 Force 300-16 Power compliance margins, 5.8 GHz (full Tx power) from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

End Product Labelling

The ePMP Module is labeled with its own FCC ID and IC Certification Number. If the FCC ID and IC Certification Number are not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. In that case, the final end product must be labeled in a visible area with the following:

Table 1 :ePMP Product labeling

Device	Label
ePMP 3000 Access Point	“Contains Transmitter Module FCC ID: Z8H89FT0024” or “Contains FCC ID: Z8H89FT0024”
Force 300-25	“Contains Transmitter Module FCC ID: Z8H89FT0017” or “Contains FCC ID: Z8H89FT0017”
Force 300-16	“Contains Transmitter Module FCC ID: Z8H89FT0016” or “Contains FCC ID: Z8H89FT0016”

Notifications

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

5.1 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.

5.1 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). To comply with FCC/IC RF exposure limits for general population or uncontrolled exposure, the antenna(s) used for the ePMP transmitter must be installed at a separation distance specified in Table 66 ePMP 3000 Access Point Power compliance margins, 5.1 GHz, FCC through Table 85 Force 300-16 Power compliance margins, 5.8 GHz (full Tx power).

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 46 FCC and IC certifications on 5 GHz product labels).

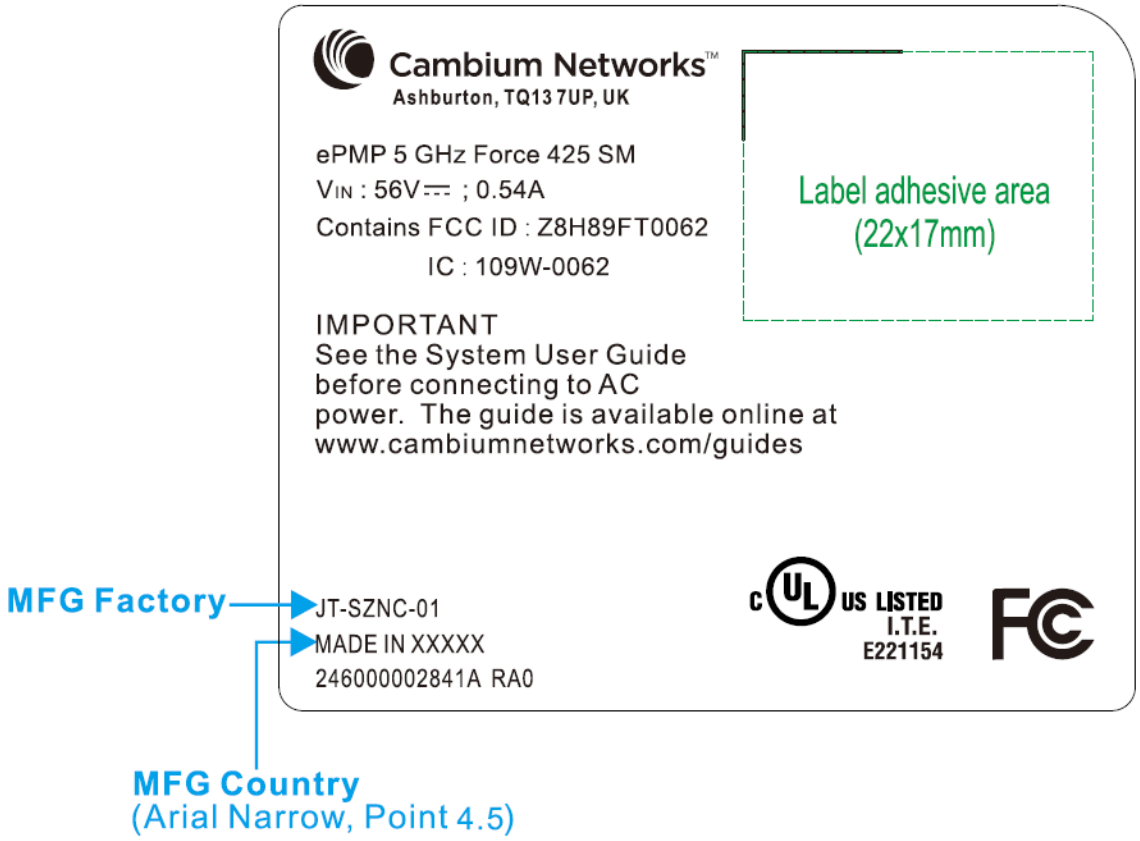
End Product Labelling

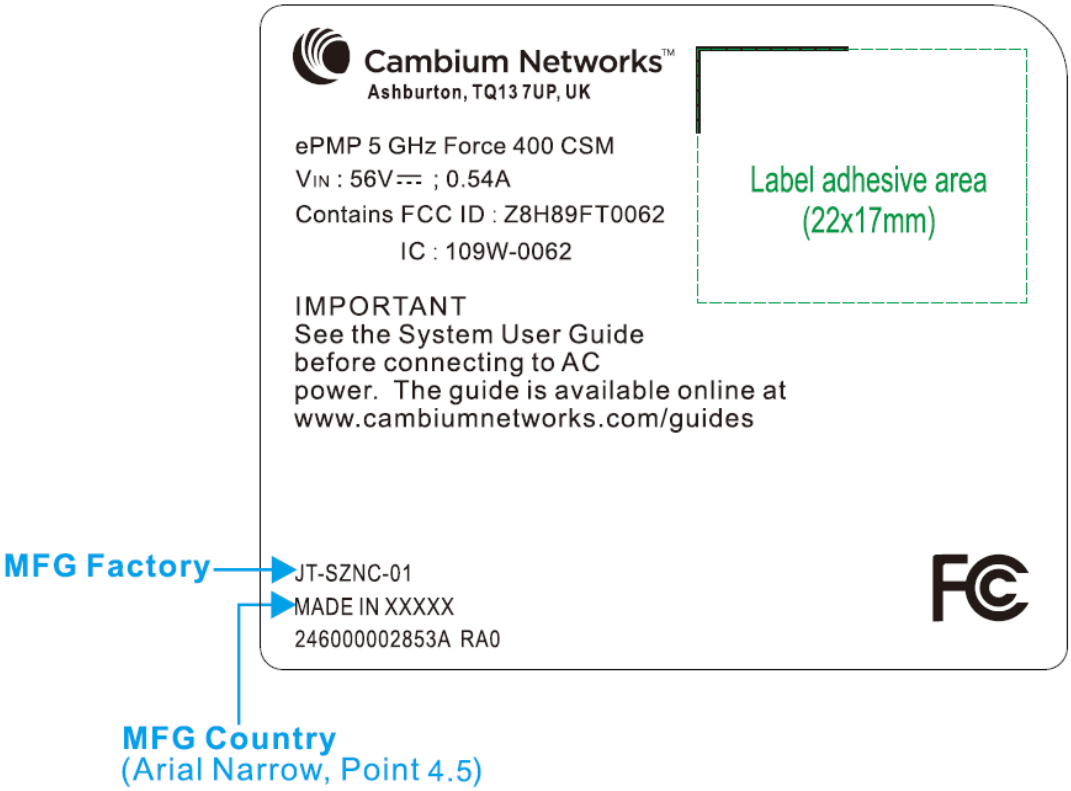
The ePMP Module is labeled with its own FCC ID and IC Certification Number. If the FCC ID and IC Certification Number are not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. In that case, the final end product must be labeled in a visible area with the following:

Table 88 Product labeling

Device	Label
ePMP 3000 Access Point	“Contains Transmitter Module FCC ID: Z8H89FT0024” or “Contains FCC ID: Z8H89FT0024”
Force 300-25	“Contains Transmitter Module FCC ID: Z8H89FT0017” or “Contains FCC ID: Z8H89FT0017”
Force 300-16	“Contains Transmitter Module FCC ID: Z8H89FT0016” or “Contains FCC ID: Z8H89FT0016”

Figure 46 FCC and IC certifications on 5 GHz product labels


Cambium Networks™
Ashburton, TQ13 7UP, UK
ePMP 5 GHz Force 425 SM
VIN : 56V⎓ ; 0.54A
Contains FCC ID : Z8H89FT0062
IC : 109W-0062
Label adhesive area
(22x17mm)
IMPORTANT
See the System User Guide
before connecting to AC
power. The guide is available online at
www.cambiumnetworks.com/guides
MFG Factory
JT-SZNC-01
MADE IN XXXXX
246000002841A RA0
c UL US LISTED
I.T.E.
E221154
MFG Country
(Arial Narrow, Point 4.5)



Wherever 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.

Radio Specifications

Product Specifications

For up-to-date performance and mechanical specifications for ePMP products, please visit:

https://www.cambiumnetworks.com/products/pmp-distribution/