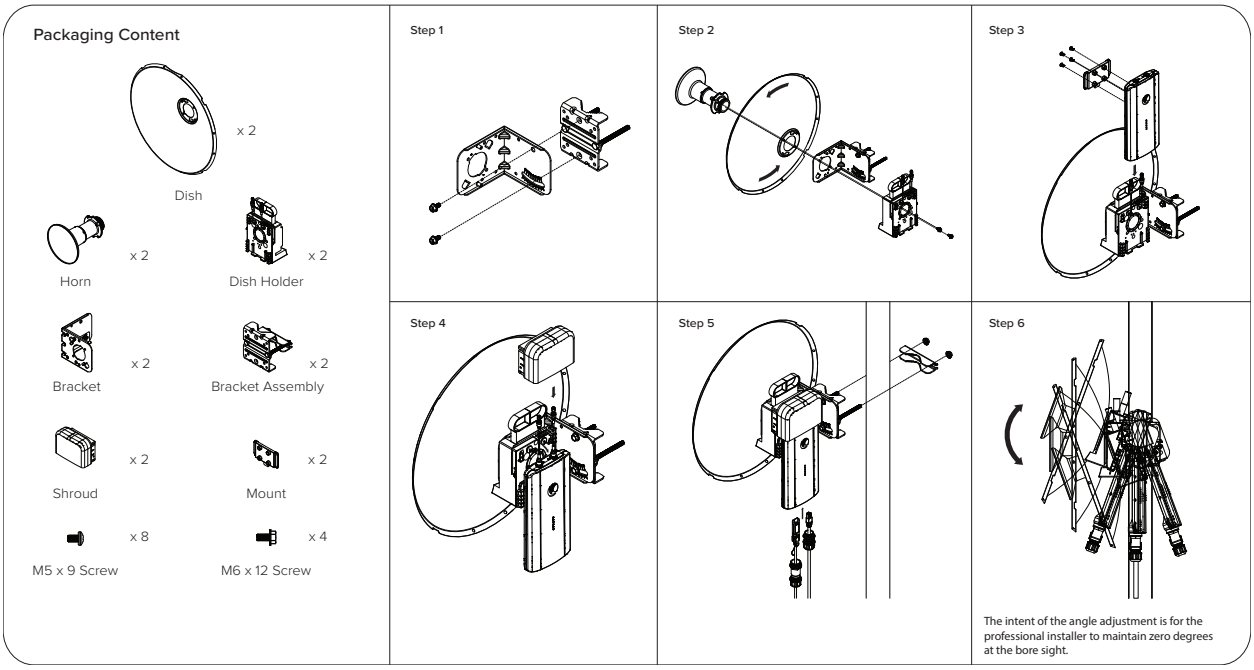
Force 4600C Access Point mounting instructions

Note

A professional installation is required.



Force 4600C software packages

Force 4600C devices can be upgraded by downloading new software packages from the Cambium Networks site or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AX-v5.x.x.img (or higher version number)

Force 4525

For details of the Force 4525 hardware, see:

- Force 4525 integrated description
- Force 4525 part numbers
- Force 4525 interfaces
- Force 4525 specifications
- Force 4525 heater
- Force 4525 wind loading
- Force 4525 software packages

Force 4525 integrated description

The Force 4525 device is a self-contained transceiver unit that contains both radio and networking electronics. The Force 4525 uses 802.11ac technology and supports MU-MIMO.

Force 4525 is shown in Figure 64.

Figure 64: *Force 4525 integrated*

Force 4525 part numbers

Select 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
- One line cord

Table 179: Force 4525 part numbers

Cambiumdescription	Cambium partnumber
ePMP 6 GHz Force 4600C SM Radio (ROW) (no cord)	C060940C021A
ePMP 6 GHz Force 4600C SM Radio (ROW) (US cord)	C060940C121A
ePMP 6 GHz Force 4600C SM Radio (IC) (Canada/US cord)	C068940C124A
ePMP 6 GHz Force 4600C SM Radio (ROW) (EU cord)	C060940C221A
ePMP 6 GHz Force 4600C SM Radio (EU) (EU cord)	C060940C223A
ePMP 6 GHz Force 4600C SM Radio (ROW) (UK cord)	C060940C321A
ePMP 6 GHz Force 4600C SM Radio (EU) (UK cord)	C060940C323A
ePMP 6 GHz Force 4600C SM Radio (ROW) (India cord)	C060940C421A
ePMP 6 GHz Force 4600C SM Radio (India) (India Cord)	C060940C425A
ePMP 6 GHz Force 4600C SM Radio (ROW) (China cord)	C060940C521A

Cambiumdescription	Cambium partnumber
ePMP 6 GHz Force 4600C SM Radio (ROW) (Brazil cord)	C060940C621A
ePMP 6 GHz Force 4600C SM Radio (ROW) (Argentina cord)	C060940C721A
ePMP 6 GHz Force 4600C SM Radio (ROW) (ANZ cord)	C060940C821A
ePMP 6 GHz Force 4600C SM Radio (ROW) (South Africa cord)	C060940C921A
ePMP 6 GHz Force 4600C SM Radio (ROW) (No PSU)	C060940CZ21A
ePMP 6 GHz Force 4600C SM Radio (FCC) (US Cord)	C068940C122B
ePMP 6 GHz Force 4600C SM Radio (Indonesia) (EU Cord)	C060940C226A

Table 180: Force 4525 accessory part numbers

Cambiumdescription	Cambiumpartnumber
ePMP Force 4525 spares kit	XXXXXXXXXXXX

Force 4525 interfaces

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

Table 181: Force 4525 series – rear interfaces

Portname	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE)
		100/1000BASE-T Ethernet	Data
	SFP	10 Gigabit cage	Optional 10 Gigabit SFP cage for SFP module

Force 4525 specifications

The Force 4525 integrated module conforms to the specifications listed in Table 182 and Table 183.

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

Table 182: Force 4525 physical specifications

Category	Specification
Dimensions (Diameter x Depth)	256 mm x 125 mm x 46 mm (10.1 in x 4.9 in. x 1.8 in.)
Weight	1.3 kg (2.9 lbs.)

Table 183: Force 4525 environmental specifications

Category	Specification
Temperature	-30°C to 55°C (-22°F to 131°F)
Wind loading	200 km/hour (124 mph)
Environmental	IPx0

Force 4525 heater

At startup, if the Force 4525 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 start-up sequence.

The effect on device start-up time at various temperatures is defined in Table 184.

Table 184: Force 4525 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 4525 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 the 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 185 and Table 186.

Table 185: Force 4525 wind loading (Kg)

TypeofePMPdevice	Largest surfacearea(squaremeters)	Wind speed (meters per second)		
		30	40	50
Force 4525 Integrated	0.03	2.82 Kg	5.02 Kg	7.84 Kg

Table 186: Force 4525 wind loading (lb)

TypeofePMPdevice	Largest surfacearea(squarefeet)	Wind speed (miles per hour)		
		80	100	120
Force 4525 Integrated	0.28	7.53 lb	11.76 lb	16.93 lb

Force 4525 software packages

Force 4525 devices can be upgraded by downloading new software packages from the Cambium Networks site or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AX-v5.x.x.img (or higher version number)

Force 4625

For details of the Force 4625 hardware, see:

- Force 4625 integrated description
- Force 4625 part numbers
- Force 4625 interfaces
- Force 4625 specifications
- Force 4625 heater
- Force 4625 wind loading
- Force 4625 software packages

Force 4625 integrated description

The Force 4625 device is a self-contained transceiver unit that contains both radio and networking electronics. The Force 4625 uses 802.11ac technology and supports MU-MIMO. The MPE distance for FCC is 36 cm and for IC is 20 cm.

Force 4625 is shown in Figure 65.

Figure 65: *Force 4625 integrated*

Warning

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft.

Operation of the transmitters in 5.925 GHz - 7.125 GHz band is prohibited for control of communications with the unmanned aircraft systems.

Warning

Operation on oil platforms, automobiles, trains, maritime vessels, and aircraft shall be prohibited.

L'exploitation sur les plates-formes pétrolières, les automobiles, les trains, les navires maritimes et les aéronefs est interdite.

Warning

Devices shall not be used for control of or communications with unmanned aircraft systems.

Les appareils ne doivent pas être utilisés pour contrôler ou communiquer avec des systèmes d'aéronefs sans pilote.

Warning

The antenna height shall be determined by the installer or operator of the standard-power access point or fixed client device, or by automatic means. This information are stored internally in the device. Provision of accurate device information is mandatory.

La hauteur de l'antenne doit être déterminée par l'installateur ou l'opérateur du point d'accès à puissance standard ou de l'appareil client fixe, ou par des moyens automatiques. Ces informations doivent être stockées en interne dans l'appareil. La fourniture d'informations précises sur l'appareil est obligatoire.

Force 4625 part numbers

Select 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

- One line cord

Table 187: Force 4625 part numbers

Cambiumdescription	Cambium partnumber
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (no cord)	C060940M041A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (US cord)	C060940M141A
ePMP 6 GHz Force 4625 SM Bulk packaging (IC) (Canada/US cord)	C068940M144A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (EU cord)	C060940M241A
ePMP 6 GHz Force 4625 SM Bulk packaging (EU) (EU cord)	C060940M243A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (UK cord)	C060940M341A
ePMP 6 GHz Force 4625 SM Bulk packaging (EU) (UK cord)	C060940M343A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (India cord)	C060940M441A
ePMP 6 GHz Force 4625 SM Bulk packaging (India) (India Cord)	C060940M445A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (China cord)	C060940M541A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (Brazil cord)	C060940M641A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (Argentina cord)	C060940M741A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (ANZ cord)	C060940M841A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (South Africa cord)	C060940M941A
ePMP 6 GHz Force 4625 SM Bulk packaging (ROW) (No PSU)	C060940MZ41A
ePMP 6 GHz Force 4625 SM Bulk packaging (FCC) (US Cord)	C068940M142A
ePMP 6 GHz Force 4625 SM Bulk packaging (Indonesia) (EU Cord)	C060940M246A
ePMP 6GHz Force 4625 Subscriber Module	C068940P142A

Table 188: Force 4625 accessory part numbers

Cambiumdescription	Cambiumpartnumber
ePMP 5 and 6 GHz Force 4525 and 4625 Spare Dish 2-Pack	C050940M140A
ePMP Force 4000 series Spares Kit	N000900L071A

Force 4625 interfaces

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

Table 189: Force 4625 series – rear interfaces

Portname	Connector	Interface	Description
Eth	RJ45	PoE input	Power over Ethernet (PoE)
		100/1000BASE-T Ethernet	Data
	SFP	10 Gigabit cage	Optional 10 Gigabit SFP cage for SFP module

Force 4625 specifications

The Force 4625 integrated module conforms to the specifications listed in Table 190 and Table 191.

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

Table 190: Force 4625 physical specifications

Category	Specification
Dimensions (Diameter x Depth)	256 mm x 125 mm x 46 mm (10.1 in x 4.9 in. x 1.8 in.)
Weight	1.3 kg (2.9 lbs.)

Table 191: Force 4625 environmental specifications

Category	Specification
Temperature	-30°C to 55°C (-22°F to 131°F)
Wind loading	200 km/hour (124 mph)
Environmental	IPx0

Force 4625 heater

At startup, if the Force 4625 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 start-up sequence.

The effect on device startup time at various temperatures is defined in Table 192.

Table 192: Force 4625 startup times based on ambient temperature

InitialTemperature	Startuptime(frompowerontooperational)
-22°F (-30°C) H	20 minutes
-4°F (-20°C)	6 minutes
14°F (-10°C)	2 minutes, 30 seconds

Force 4625 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 the 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 193 and Table 194.

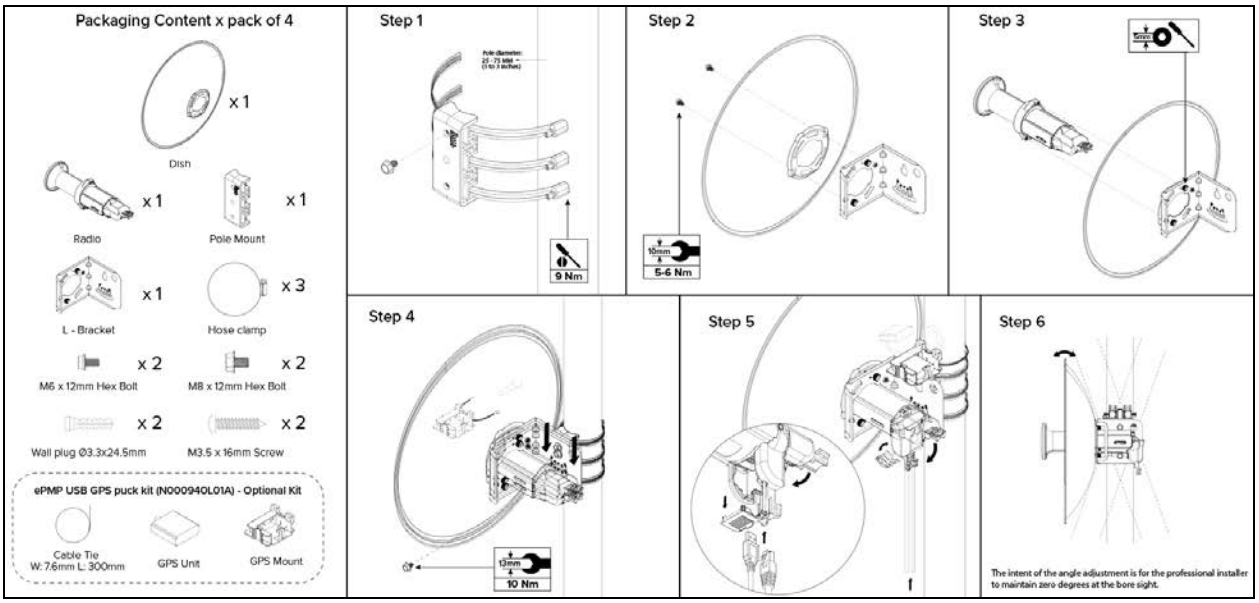
Table 193: Force 4625 wind loading (Kg)

TypeofePMPdevice	Largest surfacearea(squaremeters)	Wind speed (meters per second)		
		30	40	50
Force 4625 Integrated	0.03	2.82 Kg	5.02 Kg	7.84 Kg

Table 194: Force 4625 wind loading (lb)

TypeofePMPdevice	Largest surfacearea(squarefeet)	Wind speed (miles per hour)		
		80	100	120
Force 4625 Integrated	0.28	7.53 lb	11.76 lb	16.93 lb

Force 4625 mounting instructions



Force 4625 software packages

Force 4625 devices can be upgraded by downloading new software packages from the Cambium Networks site or by using cnMaestro. The software packages applicable to ePMP integrated radios are named:

- ePMP-AX-v5.x.x.img (or higher version number)

Power supply

For details of the ePMP power supply units, see:

- Power supply description
- Power supply part numbers
- Power supply interfaces
- Power supply specifications
- Power supply location considerations

Power supply description

The power supply unit that is connected to the ePMP modules is rated for indoor use. The ePMP modules are installed outdoors and terminated to network equipment using Cat5e cables with RJ45 connectors. The Cat5e cables are plugged into an AC or DC power supply to inject Power over Ethernet (PoE) into the module. The Cat5e cables connected to the power supply transitioning from indoors to outdoors must be rated for outdoor use.

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.

Power supply part numbers

Each module requires one power supply and one power supply line cord (line cord included with radio device, refer to, Table 195.

Table 195: Power supply part numbers

Cambium description	Cambium part number	Device Compatibility
ePMP Power Supply for GPS Radio - no cord (spare)	N000900L001	ePMP MP 3000 Access Point
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 195. This product is intended to be supplied by a UL Listed and IEC certified Power Supply Unit marked "LPS" or "PS2" and providing power over the Ethernet (PoE) supply.

Power supply interfaces

The power supply interfaces are illustrated in Figure 66 and described in Table 196 and Table 197.

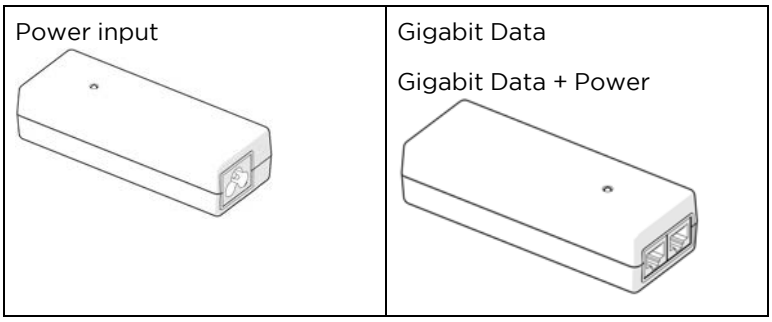


Figure 66: *Power supply interfaces*

Table 196: 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. **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 197: 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 198: 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 199, Table 200, and Table 201.

Table 199: 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 200: Power supply environmental specifications

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

Table 201: 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 considerations

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

- The power supply is rated for indoor use and can be mounted on a wall or other flat surface.
- The power supply must be kept dry, with no possibility of condensation, flooding, or rising dampness.
- The power supply can be accessed to view status indicators.
- The power supply can be connected to the ePMP module drop cable and network terminating equipment.
- The power supply can be connected to a mains or DC power supply that meets the requirements defined in Table 201.

Ethernet cabling

For more information on the Ethernet cabling components of an ePMP installation, see:

- Ethernet standards and cable lengths
- Outdoor Cat5e cable

Ethernet standards and cable lengths

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

Attention

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

For each power supply, the maximum permitted drop cable length is specified in Table 202.

Table 202: 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) The maximum length of Ethernet cable from the device to the 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. 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.

Industrial-grade cable by Cambium Networks is well suited for high-quality durable installations of subscriber modules, APs, and enterprise point-to-point links and in tactical non-permanent deployments of infrastructure.

Table 126 Cambium Industrial Cable part numbers

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

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.

Surge suppression unit

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

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

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

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.

Figure 67: *Gigabit Ethernet Surge Suppressor*

Table 127 Surge suppressor 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. Refer to Table 127 for more details.

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.

Figure 68: *cnPulse sync generator*

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 3000, 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

Note

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

System Planning

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

The following topics are described in this section:

- Planning of the ePMP links to conform to the regulatory restrictions that apply in the country of operation is explained in Radio spectrum planning
- Factors to be considered when planning links such as range, path loss, and throughput are described in Link planning
- The grounding and lightning protection requirements of an ePMP installation are described in Grounding and lightning protection
- Factors to be considered when planning ePMP data networks are described in Data network planning

Regulatory Information

This section describes planning of the 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 203. The wireless specifications that are specific to each frequency variant are listed in Table 204.

Table 203: 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.
Maximum transmit power	ePMP 3000 Access Point: 33 dBm Force 300-25: 29 dBm Force 300-19(R): 28dBm

Item	Specification
	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 204: 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 Dual-Horn antenna – 13 dBi Omni antenna – 13 dBi
Antenna 3dB Beamwidth	Integrated Dish: 6-10° azimuth, 6-10° elevation Integrated Patch: 15° azimuth, 30° elevation Sector antenna: 70° azimuth, 6° elevation Dual-Horn antenna: 45° azimuth/elevation Omni antenna: 360° azimuth, 7° 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.

Conforming to the limits

Ensure the link is configured to conform to the 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 prevent the operation automatically 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 can be obtained from https://support.cambiumnetworks.com/licensekeys/epmp.

Available spectrum

The available spectrum for the operation depends on the region. When configured with the appropriate country code, the unit allows operation on those channels only 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 does 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.

Channel bandwidth

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

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

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

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 is granted for ePMP are listed under Table 205.

Table 205: EMC emissions compliance

Region	Specification (Type Approvals)
USA	FCC CFR 47 Part 15 class B
Canada	RSS210, Issue 8 RSS247, Issue 1 (May 2015)

Region	Specification (Type Approvals)
Europe	ETSI EN301 489-4

Compliance with safety standards

This section lists the safety specifications against which the ePMP is tested and certified. It also describes keeping the RF exposure within safe limits.

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

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

Path loss

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

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

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

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 are obtained, taking account of propagation and interference. When the link is 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 206.

Table 206: 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
Interface	10/100/1000BASE-T (RJ-45)
Maximum Ethernet Frame Size	1700 bytes
Service classes for bridged traffic	3 classes

Note

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

Over the air, throughput is 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 is 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 the amount of quality of service is configured in ePMP to minimize the 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 the high-priority transmissions are complete.

Using the Device Management Interface

This section describes all configuration and alignment tasks that are performed while deploying the ePMP system.

Perform the following tasks while configuring the ePMP devices:

- Preparing for configuration
- Connecting to the unit
- Using the web interface
- Using the installation wizard – Access Point
- Using the installation wizard – Subscriber Module
- Using the menu options

Preparing for configuration

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

Safety precautions

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

Warning

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

Observe the following guidelines:

- Never work in front of the antenna when the device is powered on.
- Always switch off 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, refer to Compliance with safety standards section.

Connecting to the unit

To connect the unit to management PC, perform the following procedures:

- Configuring the management PC
- Connecting to the a PC and powering up

Configuring the management PC

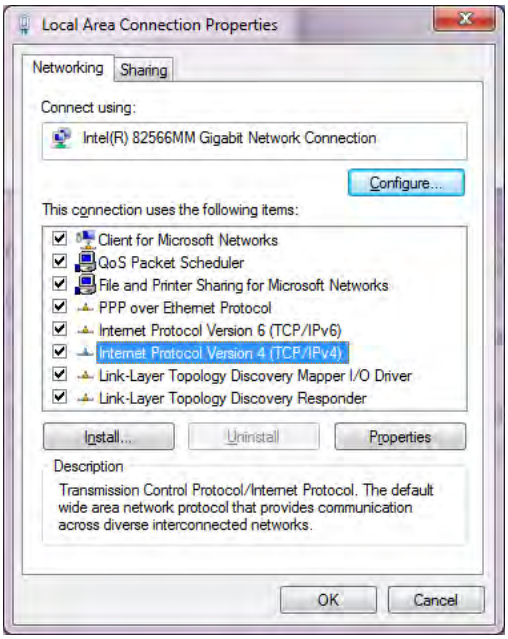
Perform the following steps to configure the local management PC to communicate with the ePMP module:

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

   For Windows 7, navigate to **Control Panel > Network and Internet > Network Connections > Local Area Connection**.

2. Select the **Internet Protocol (TCP/IP)** option.

3. Click **Properties**.



4. Enter an IP address that is valid for the 169.254.1.x network, avoiding 169.254.1.1. For example, 169.254.1.100.

5. Enter a subnet mask of **255.255.255.0**.

   Leave the default gateway blank.

6. Click **OK** and then click **Close**.

Connecting to a PC and powering up

Perform the following steps to connect a management PC directly to the ePMP for configuration and alignment purposes and to power up the ePMP device.

1. Verify that the device and power supply are connected correctly (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 main or battery power to the power supply. The Green power LED must blink continuously.

Note

If the power and Ethernet LEDs do not blink continuously, refer to Testing hardware section to troubleshoot.

Using the web interface

This section describes the usage of ePMP web interfaces.

- Logging into the web interface

Logging into the web interface

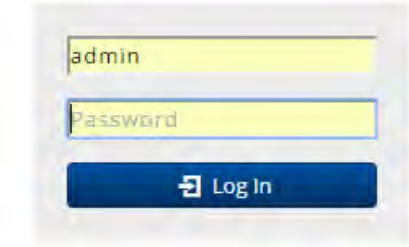
Perform the following procedure to login into the web interface as a system administrator.

Equipment and tools

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

Procedure

1. Verify that the device and power supply are connected correctly (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. Configure the host machine with an IP address in the 169.254.1.x subnet (excluding 169.254.1.1).
4. Connect the power supply to power mains.
5. From the browser, navigate to the device's default IP address **169.254.1.1**.



6. Log in with **admin** username and **admin** password.

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.

Attention

All the new ePMP devices contain default username and password configurations. It is recommended to change the password configurations immediately. These passwords is configured in the management UI section **Configuration > System > Account Management**.

Using the installation wizard – Access Point

ePMP device provides a guided configuration mechanism for configuring key parameters for the link operation.

This setup can be accessed from the **Installation** page by clicking on the Start Setup button.

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

Step 1: Main system parameters

Figure 69 shows the Main system parameters page.

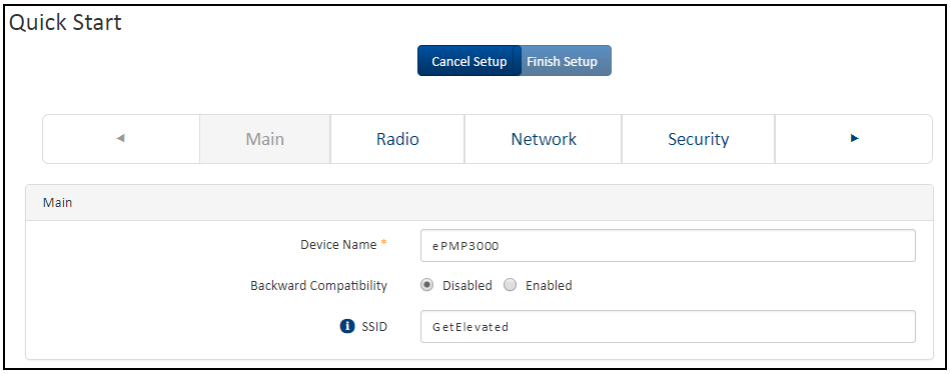


Figure 69: *Quick Start page*

Attribute	Description
Main	
Device Name	The configured identifier used in NMS such as cnMaestro.
Backward Compatibility	**Enabled**: 802.11n ePMP subscribers can 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 AP's beacon. (Access Point Mode). SSID must be the same at both ends and different from the site name.

Step 2: Radio parameters

Figure 70 shows the Radio parameters page.

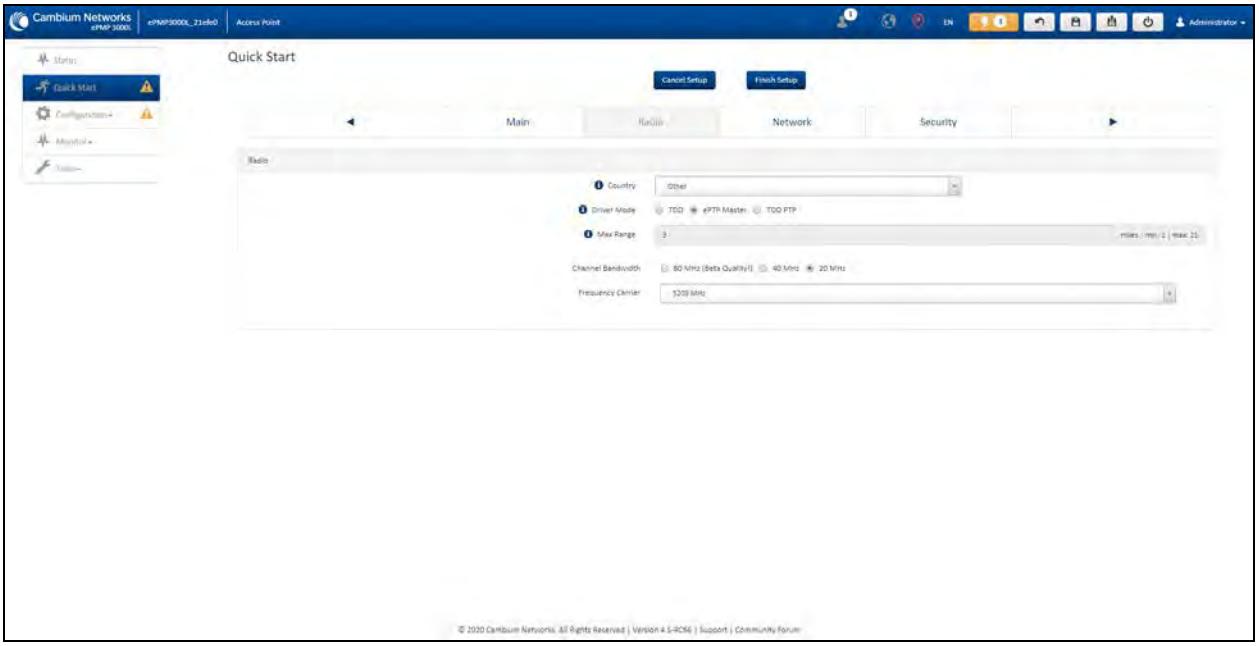


Figure 70: *Radio parameters page*

Attribute	Description
Radio	
Country	Defines the country code that is used by the device. The country code of the Subscriber Module follows the country code of the associated AP 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.
Driver Mode	**TDD**: The device is operating in point-to-multipoint (PMP) mode using TDD scheduling. The AP can GPS synchronize in this mode. **ePTP Master**: The AP is operating as a Master in point-to-point mode. The AP does not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode. **TDD PTP**: The AP is operating in point-to-point (PTP) mode using TDD scheduling. The AP can GPS synchronize in this mode.
Downlink/Uplink Ratio	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.

Attribute	Description
Max Range	This parameter represents the cell coverage radius. Subscriber Modules outside the configured radius does not able to connect. It is recommended to configure Max Range to match the actual physical distance of the farthest subscriber.
Channel Bandwidth	Configure the channel size used by the radio for RF transmission.
Frequency Carrier	Configure the frequency carrier for RF transmission. This list is dynamically adjusted to the regional restrictions based on the setting of the **Country** parameter. Ensure that a thorough spectrum analysis is completed before configuring this parameter.

Step 3: Network parameters

Figure 71 shows the Network parameters page.

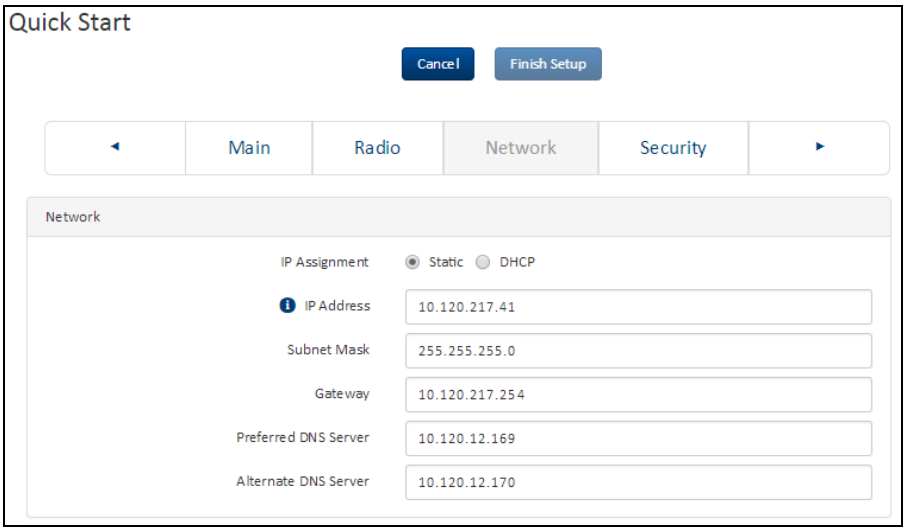


Figure 71: *Network parameters page*

Attribute	Description
Network	
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 (AP) or 192.168.0.2 (SM).

Attribute	Description
Subnet Mask	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 will belong to subnet **192.168.2.X**.
Gateway	Configure the IP address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Preferred DNS Server	Configure the primary IP address of the server used for DNS resolution.
Alternate DNS Server	Configure the secondary IP address of the server used for DNS resolution.

Step 4: Security parameters

Figure 72 shows the Security parameters page.

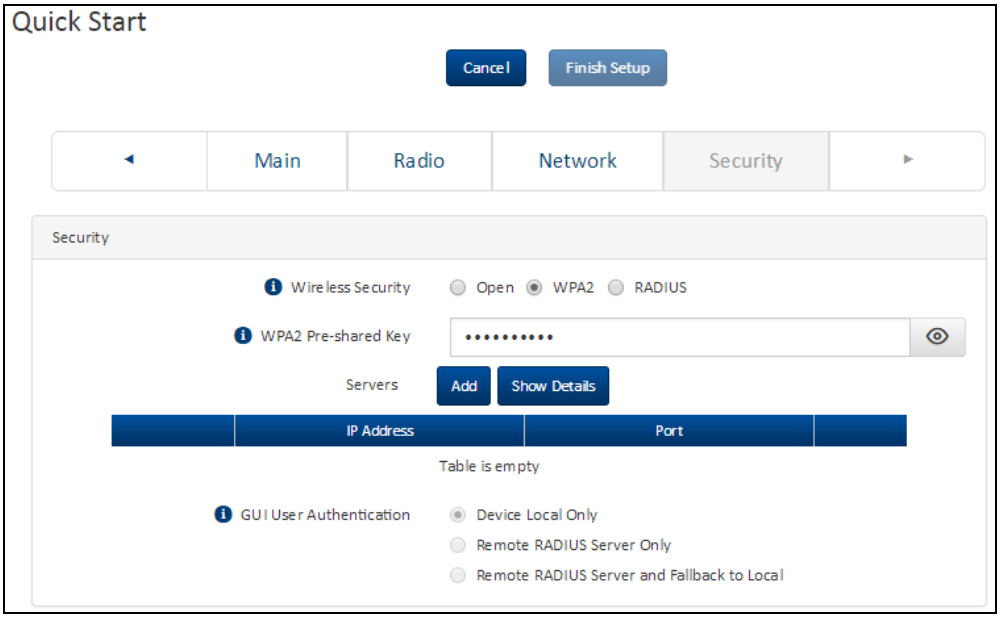


Figure 72: *Security parameters page*

Attribute	Description
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 AP and Subscriber Module. **RADIUS**: Enables Subscriber Module authentication through a pre-configured Radius server.

Attribute	Description
WPA2 Pre-shared Key	Configure this key on the AP, 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 three 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 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 the guided configuration mechanism for configuring key parameters for link operation.

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

button.

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

Step 1: Main system parameters

Figure 73 shows the Main system parameters page.

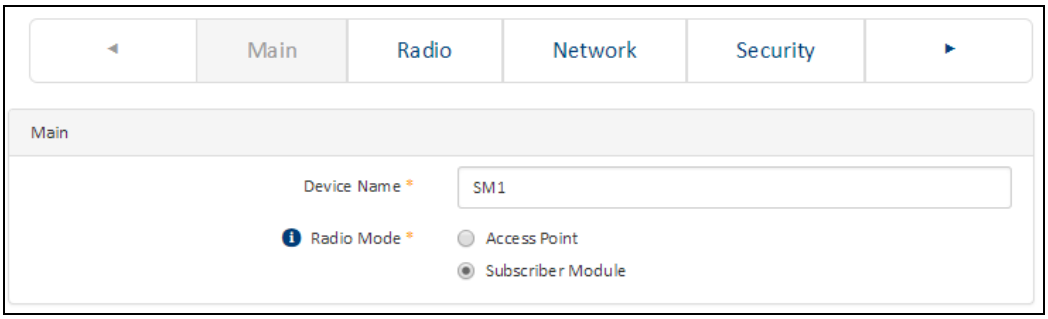


Figure 73: *Main system parameters page*

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

Step 2: Radio parameters

Figure 74 shows the Radio parameters page.

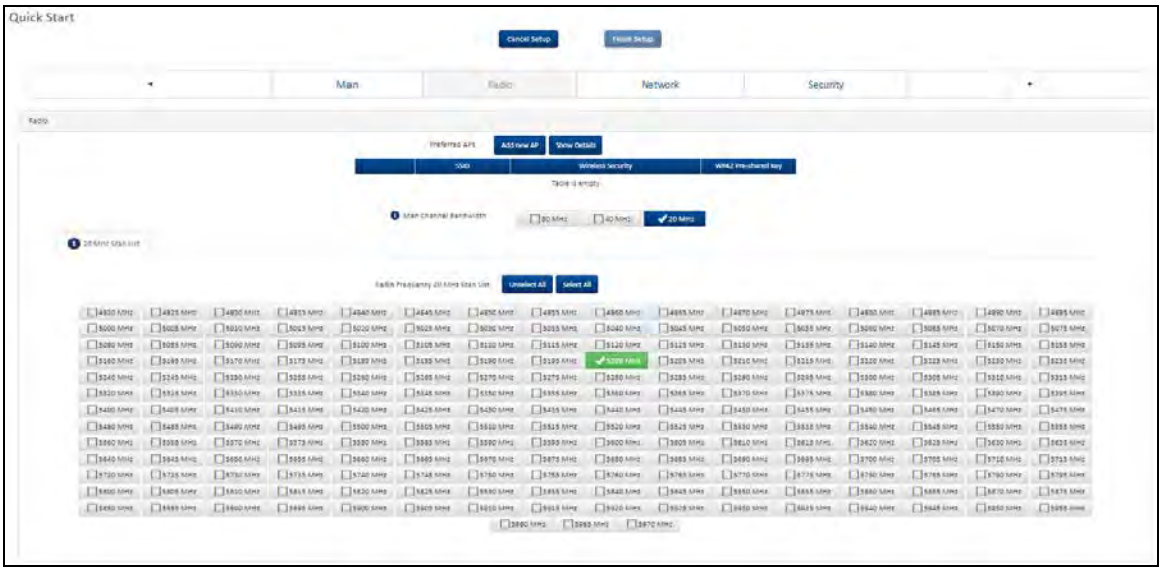


Figure 74: *Radio parameters page*

Attribute	Description
Radio	
Preferred APs	
SSID	The **Preferred Access Points SSID** defines the AP SSID to which the Subscriber Module (SM) device attempts the registration.
Wireless Security	**Open:** The SM device attempts the registration to preferred APs SSID with no security mechanism. **WPA2**: The WPA2 mechanism provides AES radio link encryption and SM network entry authentication. When enabled, the SM must register using the Authentication Pre-shared Key configured on the AP and SM.
WPA2 Pre-shared Key	The **Preferred Access Points WPA2 Pre-shared Key** must be configured on the SM device to match the pre-shared key configured on the Access Point for registration with WPA2 security.

Attribute	Description
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 is completed before configuring this parameter.

Step 3: Network parameters

Figure 75 shows the Network parameters page.

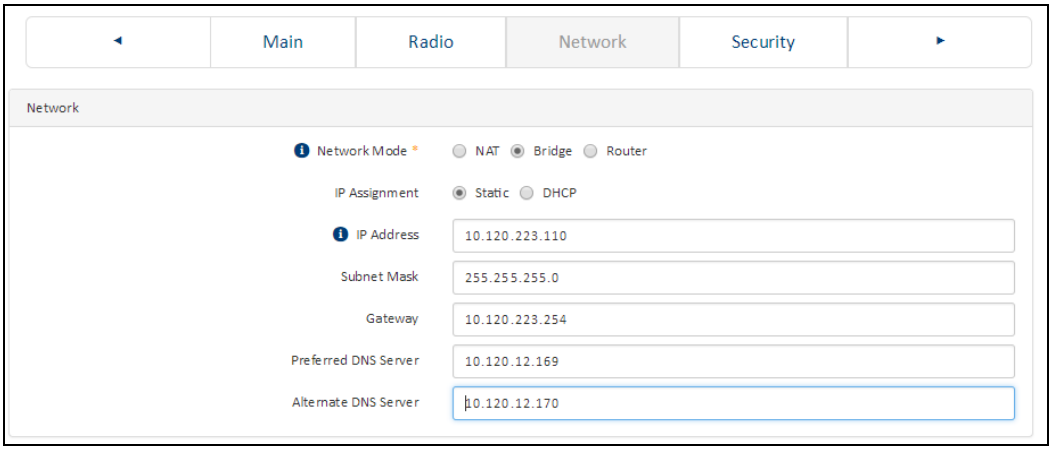


Figure 75: *Network parameters page*

Attribute	Description
Network	
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. **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.
IP Address	Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.

Attribute	Description
	If IP Address Assignment is set to DHCP and the device is unable to retrieve IP address information through DHCP, the device management IP is set to fallback IP 192.168.0.1 (AP) or 192.168.0.2 (SM).
Subnet Mask	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 belongs to subnet **192.168.2.X**.
Gateway	Configure the IP address of the device on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks.
Preferred DNS Server	Configure the primary IP address of the server used for DNS resolution.
Alternate DNS Server	Configure the secondary IP address of the server used for DNS resolution.

Step 4: Security parameters

Figure 76 shows the Security parameters page.

Figure 76: *Security parameters page*

Attribute	Description
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 the web pages. Some of the menu options are only displayed for specific system configurations. Refer to, Table 207 to locate information about each web page.

Table 207: Menu options and web pages

Main menu	Menu option	Web page information
Status		Status page
Installation		Installation page
Configuration		Configuration menu
	Radio	Configuration > Radio page
	System	Configuration > System page
	Network	Configuration > Network page
	Security	Configuration > Security page
Monitor		Monitor menu
	Performance	Monitor > Performance page
	System	Monitor > System page
	Wireless	Monitor > Wireless page
	Throughput Chart	Monitor > Throughput Chart page
	GPS	Monitor > GPS page (Access Point mode)
	Network	Monitor > Network page
	System Log	Monitor > System Log page
Tools		Tools menu
	Software Upgrade	Tools > Software Upgrade page
	Backup / Restore	Tools > Backup/Restore page
	License Management	Tools > License Management page (Access Point Mode)
	Spectrum Analyzer	Tools > Spectrum Analyzer page
	eAlign	Tools > eAlign page
	Wireless Link Test	Tools > Wireless Link Test page
	Watchdog	Tools > Watchdog page
	Ping	Tools > Ping page
	Traceroute	Tools > Traceroute page

Status page

The status page describes the status information of the QoE device. Figure 77 shows the Status page.

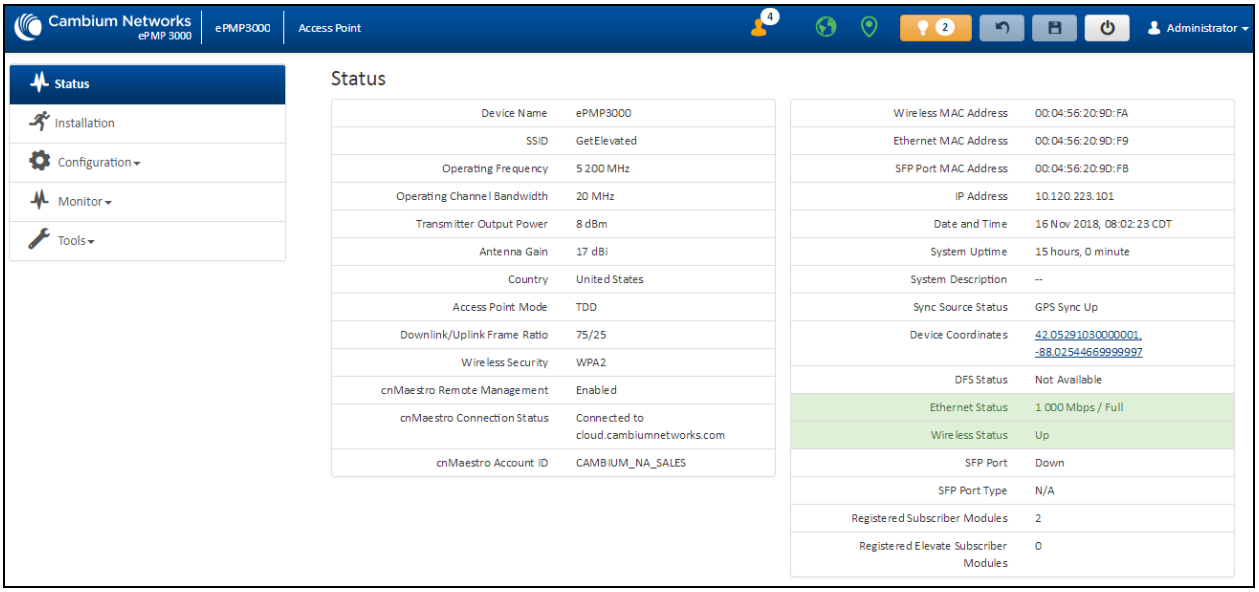


Figure 77: *Status page*

Table 132 Status page attributes

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

Attribute	Description
Access Point Mode	**TDD**: The Access Point is operating in point-to-multipoint (PMP) mode using TDD scheduling. The AP can GPS synchronize in this mode (except when in Flexible mode). **ePTP Master**: The Access Point is operating as a Master in point-to-point mode. The AP does not support GPS Synchronization in this mode but can provide **significantly lower latency** than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode. **PTP**: The Access Point is operating in point-to-point (PTP) mode using TDD scheduling. The AP can GPS synchronize in this mode (except when in Flexible mode).
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	Currently 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 concerning the Cambium Cloud Server. When Enabled under **Configuration > System**, the device will be managed by the Cambium Remote Management System, which allows all Cambium devices to be managed from the Cambium Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Cloud Server.
Wireless MAC Address	The MAC address of the device wireless interface.
Ethernet MAC Address	The MAC address of the device Ethernet (LAN) interface.
SFP Port MAC Address	The MAC address of the device SFP interface.
IP Address	The currently configured device IP address (LAN) is used for management access.
IPv6 Link Local Address	A link-local address is required for the IPv6-enabled interface (applications may rely on the link-local address even when there is no IPv6 routing). The IPv6 link-local address is comparable to the auto-configured IPv4 address 169.254.0.0/16.
IPv6 Address	The IPv6 address for device management.
Date and Time	The current date and time on the device, subject to the configuration of the parameter **Time Zone.**
System Uptime	The total uptime of the radio since the last reset.

Attribute	Description
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**: Before transmitting, the device must check the configured **Frequency Carrier** for radar pulses for 60 seconds). If no radar pulses are detected, the device transitions to state **In-Service Monitoring.** **In-Service Monitoring**: Radio is transmitting and receiving normally while monitoring for radar pulses that 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 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. **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.
Registered Elevate Subscriber Modules	The total number of ePMP Elevate (third-party software solution) subscribers registered to the AP.

Installation page

For more information on the installation page, refer to Using the installation wizard – Access Point and Using the installation wizard – Subscriber Module sections.

Configuration menu

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

Configuration > Radio page

Figure 78 and Figure 79 shows the Radio pages (AP mode and SM mode).

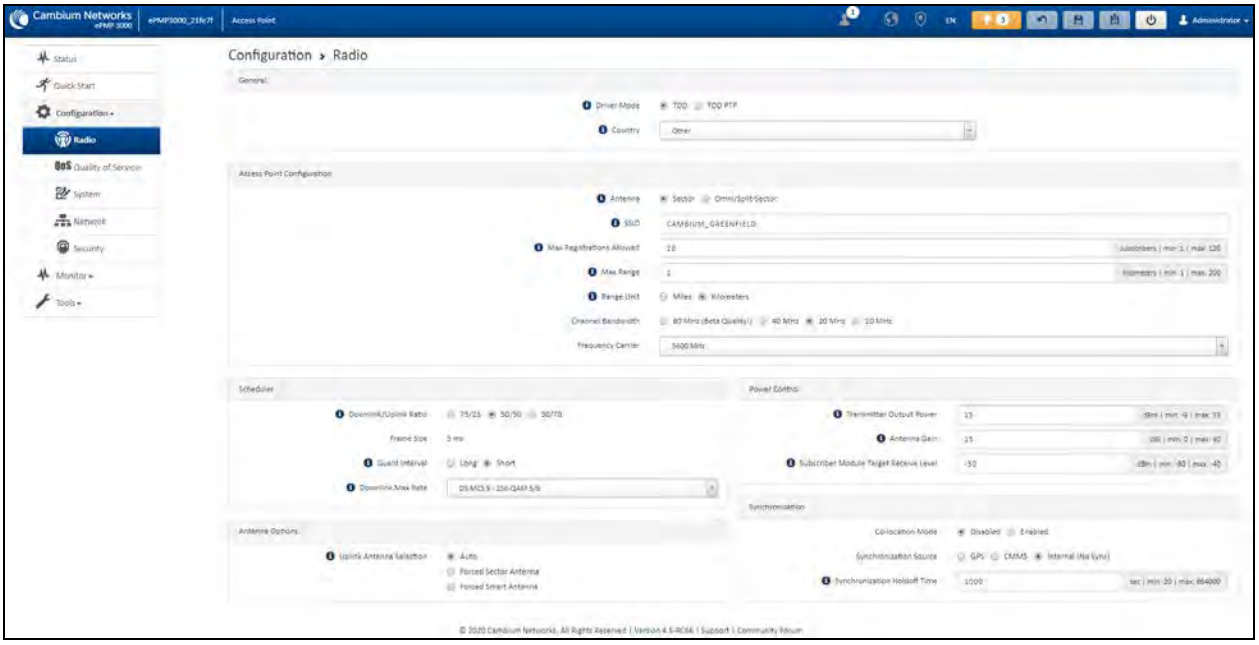


Figure 78: *Configuration > Radio page (AP mode)*

Note

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

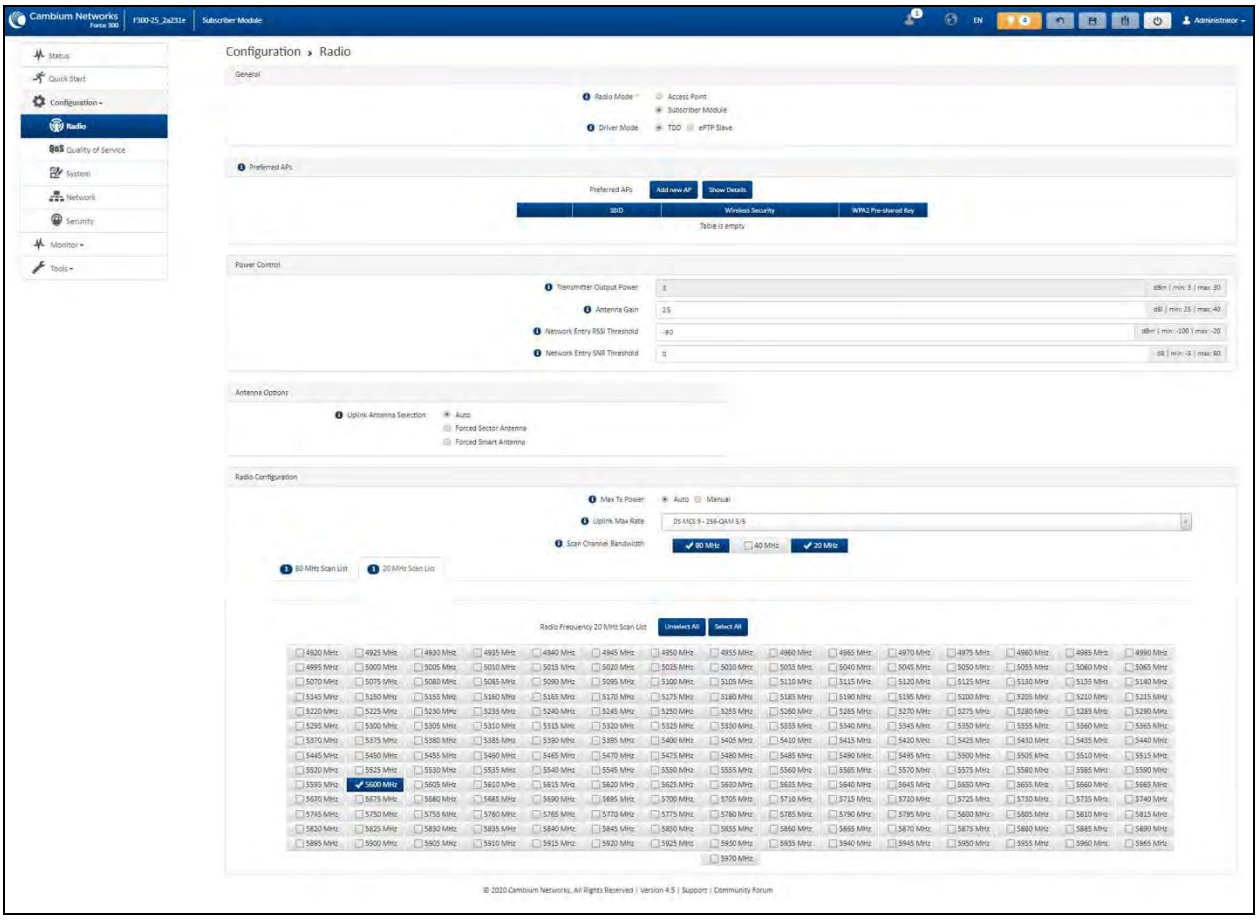
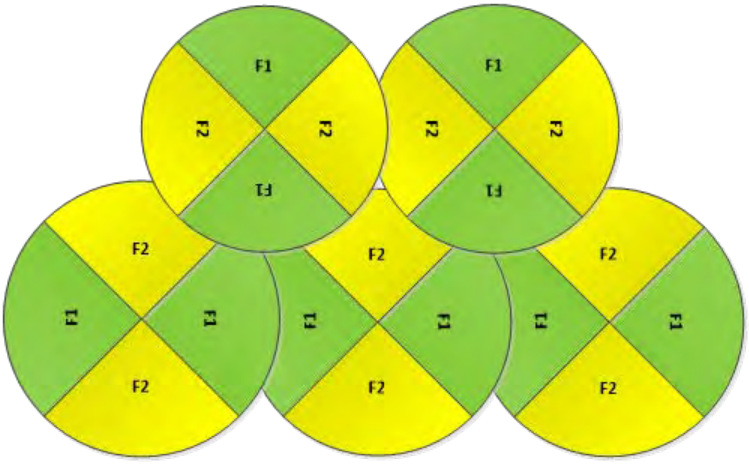


Figure 79: *Configuration > Radio page (SM mode)*

Table 133 Configuration > Radio page attributes

Attribute	Description
General	
Driver Mode	**TDD**: The device is operating in Point-to-Multipoint (PMP) mode using TDD scheduling. The AP can GPS synchronize in this mode. **ePTP Slave**: The SM is operating as a Slave in point-to-point mode. The AP and the system do not support GPS Synchronization in this mode but can provide significantly lower latency than other modes. QoS (MIR and traffic priority) capability and Link Quality/Capacity indicators are not available in this mode. **TDD PTP**: The Access Point is operating in point-to-point (PTP) mode using TDD scheduling. The AP can GPS synchronize in this mode.
Radio Mode	**Access Point**: The unit controls the point-to-point link and its maintenance. On start-up, the Access Point transmits until a link with the Subscriber Module is made.

Attribute	Description
	Subscriber Module: The unit listens for its peer and only transmits when the peer has been identified.
Backward Compatibility (Access Point Mode)	**Enabled**: 802.11n ePMP subscribers can 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).
Access Point Configuration (AP mode)	
Antenna (Access Point Mode)	**Sector:** Panel, 90° or Dual-Horn, 60° **Omni:** KP-5QSOMNI-13
SSID (Access Point Mode)	SSID is a unique identifier for a wireless LAN which is specified in the AP's beacon. (AP mode). SSID must be the same at both ends and different from the site name.
Max Registrations Allowed (Access Point Mode)	Based on a 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. That is **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.
Max Range (Access Point Mode)	This parameter represents the cell coverage radius. Subscriber Modules outside the configured radius does not able to connect. It is recommended to configure Max Range to match the actual physical distance of the farthest subscriber.

Attribute	Description
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 before 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 79. Note that CMM3 and CMM4 devices cannot be used as synchronization sources for ePMP 3000, the parameter setting suggestions below serve as a guideline for mixed 802.11n and 802.11ac networks.  Figure 80: *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. 0B0BThe 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 • CMM4 • CMM5

Attribute	Description
	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 has 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. • 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.**

Attribute	Description
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 is being uses by the device.
Subscriber Module Target Receive Level (Access Point Mode)	Defines the desired received power level at the AP from the registered Subscriber Module. APs use this parameter to control the transmission power of the Subscriber Module to reduce system self-interference.
Network Entry RSSI Threshold (Subscriber Module Mode)	This defines the Downlink RSSI threshold below which a Subscriber Module does 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 does not register to an Access Point.
Synchronization (AP mode)	
Co-location Mode (Access Point Mode)	**Disabled:** The ePMP device can synchronize only with other ePMP APs. **Enabled:** The ePMP device can be configured to synchronize with PMP 100 or PMP 450 series of radios in addition to other ePMP APs. Refer to 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 through 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 through the AP's Ethernet port through a connected Cambium Cluster Management Module 5 (CMM5). Co-located or in-range APs receiving synchronization through GPS or CMMl transmits and receive at the same time, thereby reducing self-interference. For more information on CMM configuration, refer to *PMP Synchronization Solutions User Guide*. If CMM is 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** does not transmit and receive in sync with other co-located or in-range APs, which introduces self-interference into the system.

Attribute	Description
Synchronization Holdoff Time (Access Point Mode)	The **Synchronization Holdoff Time** is designed to gracefully handle fluctuations/losses in the GPS synchronization signaling. After the AP has received a reliable synchronization pulse for at least 60 seconds, if there is a loss of synchronization signal, the **Synchronization Holdoff** timer is started. During the holdoff interval, all SM registrations are maintained. If a valid GPS synchronization pulse is regained during the holdoff interval, then the AP continues to operate normally. If a valid synchronization pulse is not regained from the GPS source during the holdoff interval, then the AP ceases radio transmission. The default is **30 seconds**.
Preferred Access Points (SM 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 SM device sequentially attempts registration. For each AP configured, if authentication is required, enter the **Wireless Security** type and **WPA2 Pre-shared Key** associated with the configured **SSID**.
Scheduler (AP 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 is used for downlink resources, and the amount of the total radio link's aggregate throughput that is 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 channel efficiency.
Downlink Max Rate (AP mode)	Specifies the maximum downlink MCS value that the Rate Adapt algorithm chooses 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.  **Note** This setting is not available if the AP is set to ePTP Master mode.
Radio Configuration	
Maximum Tx Power (SM mode)	**Auto**: The AP can control, using ATPC (Automatic Transmit Power Control), the TX power of the SM up to the maximum capability of the SM's transmitter (based on regulatory limits). **Manual**: The AP can control the TX power of the SM up to the value configured in the **Transmitter Power** field.

Attribute	Description
Transmitter Output Power (SM 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 Maximum Rate (SM mode)	Specifies the maximum uplink MCS value that the Rate Adapt algorithm chooses 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.  **Note** This setting is not available if the SM is set to ePTP Slave mode.
Scan Channel Bandwidth (Subscriber Module Mode)	The selected scan channel bandwidths are scanned by the SM. Any combination can 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 contains 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 the channels are scanned.

Configuration > Quality of Service (QoS)

The AP Quality of Service (QoS) page

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

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

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

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

Warning

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

The ePMP platform also supports radio data rate-limiting (Maximum Information Rate, or MIR) based on the configuration of the MIR table. Operators may add up to 16 MIR profiles on the AP, each with unique limits for uplink and downlink data rates. The SM field **MIR Profile Setting** is used to configure the appropriate MIR profile for limiting the SM's data rate. Figure 81 shows the Quality of Service page.

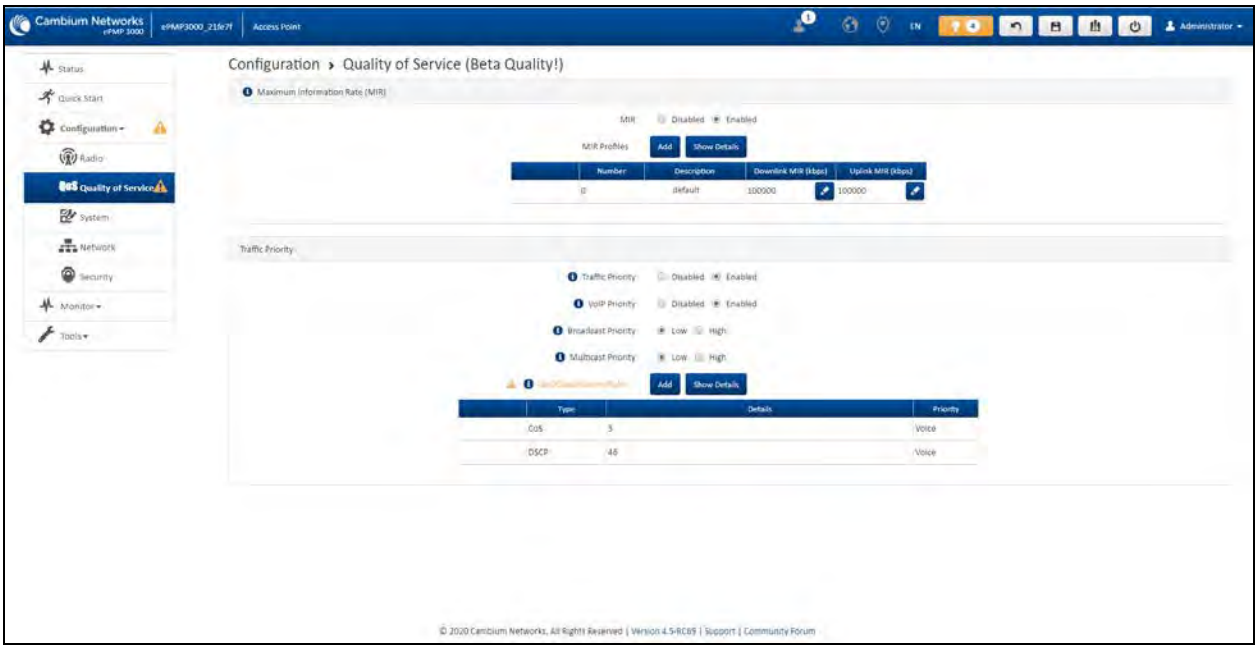


Figure 81: *Configuration > AP Quality of Service page*

Table 208: AP Radio Configuration attributes

Attribute	Description
Maximum Information Rate (MIR)	
MIR	**Disabled:** When disabled, RF transmission is only limited by the capacity of the link (and any active QoS classification rules). **Enabled:** When enabled, all downlink and uplink traffic is limited based on the profiles configured in the MIR table.
MIR Profiles	The MIR (Maximum Information Rate) table is comprised of up to sixteen profiles which, after configured, may be set on the SM to employ a certain service level or data rate.
Number	Assign a profile number to each row in the AP MIR table. This profile number is then set on each SM to limit data transfer rates based on the operator's configuration of the MIR table and its profiles.
Description	Assign a logical description for each service level. For example, a tiered service-level provider may deploy service levels **Gold**, **Silver** and **Bronze** or **20 Mbps**, **10 Mbps** and **5 Mbps** to offer a clear description.
Downlink MIR (kbps)	Specify the downlink rate at which the AP is allowed to transmit for this configured profile.

Attribute	Description
Uplink MIR (kbps)	Specify the uplink rate at which the AP is allowed to transmit for this configured profile.
Traffic Priority	
Traffic Priority	**Disabled**: No traffic prioritization is performed. All traffic is treated with equal priority (low priority). **Enabled:** Traffic prioritization is enabled, and specific types of traffic can be prioritized using the fields below.
VoIP Priority	**Enabled**: When enabled, two entries are automatically added to the first and second rows of the QoS Classification Rules table, one with **Rule Type CoS** (5) and one with **Rule Type DSCP** (46). The addition of these rules ensures that VoIP traffic passed over the radio downlink is given the highest priority. The **CoS** and **DSCP** values may be modified to accommodate non-standard VoIP equipment. **Disabled**: When disabled, VoIP traffic is scheduled normally along with all other user data.
Broadcast Priority	**Low Priority**: All broadcast traffic sent over the downlink is prioritized as low priority and is delivered to the SM after scheduled high priority and VoIP traffic. **High Priority**: All broadcast traffic sent over the downlink is prioritized as a high priority and is scheduled for delivery to SMs before low priority traffic but after VoIP traffic.
Multicast Priority	**Low Priority**: All multicast traffic sent over the downlink is prioritized as low priority and will be delivered to the SM after scheduled high priority and VoIP traffic. **High Priority**: All multicast traffic sent over the downlink is prioritized as a high priority and is scheduled for delivery to SMs before low priority traffic but after VoIP traffic.
QoS Classification Rules	The QoS Classification Rules table contains all of the rules enforced by the device when passing traffic over the radio downlink. Traffic passed through the device is matched against each rule in the table; when a match is made the traffic is sent over the radio link using the priority defined in **Traffic Priority** column.
Type	**CoS**: Class of Service; traffic prioritization is based on the 3-bit header present in the 802.1Q VLAN-tagged Ethernet frame header in the packet entering the AP's Ethernet port. **VLAN ID:** Traffic prioritization is based on the VLAN ID of the packet entering the AP's Ethernet port. **EtherType:** Traffic prioritization is based on the two-octet Ethertype field in the Ethernet frame entering the AP's Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame. **IP:** Traffic prioritization is based on the source and (or) destination IP address of the packet entering the AP's Ethernet port. A subnet mask may be included to define a range of IP addresses to match.

Attribute	Description
	MAC: Traffic prioritization is based on the source and (or) destination MAC address of the packet entering the AP's Ethernet port. A mask may be included to define a range of MAC addresses to match. The mask is made up of a hex representation of a series of 1s to start the mask and 0s that end the mask. A 1 may not follow a 0. Thus FF:FF:FF:FF:00:00 is allowed, but FF:00:FF:FF:FF:FF is not. The MAC address is combined with the mask to define the range of allowed MAC addresses.
Details	Represents the details of the Class of Service (CoS) present in the packet entering the AP's Ethernet port.
Priority	Represents the QoS classification rule priority.

The SM Quality of Service page

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

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

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

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

Warning

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

The ePMP platform also supports radio data rate-limiting (Maximum Information Rate (MIR)) based on the configuration of the MIR table. Operators may add up to 16 MIR profiles on the AP, each with unique limits for uplink and downlink data rates. The SM field **MIR Profile Setting** is used to configure the appropriate MIR profile for limiting the SM's data rate. Figure 82 shows the Quality of Service page.

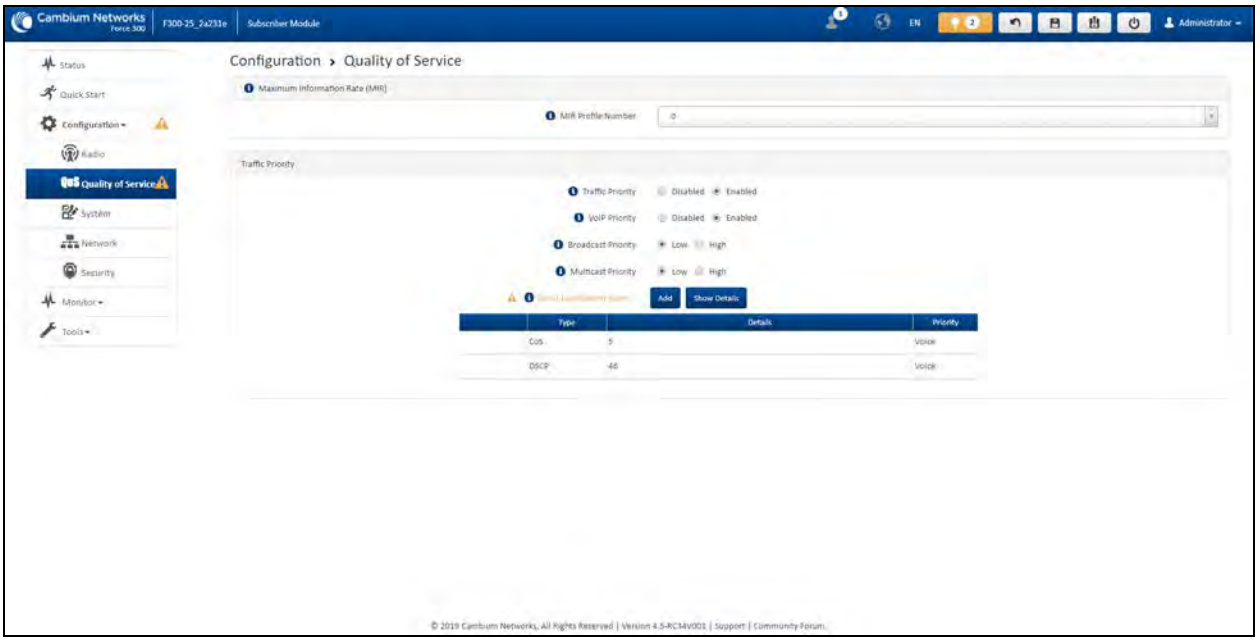


Figure 82: *Configuration > SM Quality of Service page*

Table 135 SM QoS attributes

Attribute	Description
Maximum Information Rate (MIR)	
MIR Profile Number	Configure the desired MIR (Maximum Information Rate) profile for SM operation. This profile must be configured on the AP else the default profile (0) is used.
Traffic Priority	**Enabled**: The QoS Classification Rules table is editable and is utilized by the device to classify traffic. **Disabled**: The QoS Classification Rules table is greyed out and all traffic is sent at one priority level.
VoIP Priority	**Enabled**: When enabled, two entries are automatically added to the first and second rows of the QoS Classification Rules table, one with **Rule Type CoS** (5) and one with **Rule Type DSCP** (46). The addition of these rules ensures that VoIP traffic passed over the radio downlink is given the highest priority. The **CoS** and **DSCP** values may be modified to accommodate non-standard VoIP equipment.
Broadcast Priority	**Low Priority**: All Broadcast traffic sent over the uplink is prioritized as low priority and is delivered to the AP after scheduled high priority and VoIP traffic. **High Priority**: All Broadcast traffic sent over the uplink is prioritized as a high priority and is scheduled for delivery to the AP before low priority traffic but after VoIP traffic.
Multicast Priority	**Low Priority**: All Multicast traffic sent over the uplink is prioritized as low priority and is delivered to the AP after scheduled high priority and VoIP traffic. **High Priority**: All Multicast traffic sent over the uplink is prioritized as a high priority and is scheduled for delivery to the AP before low priority traffic but after VoIP traffic.

Attribute	Description
Subscriber Module Priority	**Normal**: SM gives priority to the packets as defined in the rules which can be **Low**, **High**, or **VoIP**. **Normal** priority allows data to be added to the appropriate **High**, **Low**, and **VoIP** queues based on the QoS rules. This is the default setting. If no rule is defined for a packet, then the packet priority is **Low**. **High**: SM places all data other than VoIP in the **High** queue. It is given higher priority than SMs configured with **Low** and **Normal** when there is contention for bandwidth under the AP. **Low**: **Low** priority places all data that is not VoIP in the **Low** priority queue. It will be given lower priority than SMs configured with **High** when there is contention for bandwidth under the same AP. **VoIP** queue is the highest priority queue followed by the **High** queue and then by the **Low** queue. Higher priority queues have preference over lower priority queues, but does not suffer them.
QoS Classification Rules	The QoS Classification Rules table contains all of the rules enforced by the device when passing traffic over the radio downlink. Traffic passed through the device is matched against each rule in the table; when a match is made the traffic is sent over the radio link using the priority defined in column **Traffic Priority**.
Type	**DSCP**: Differentiated Services Code Point; traffic prioritization is based on the 6-bit differentiated services field in the IP header present in the packet entering the Ethernet port. **CoS**: Class of Service; traffic prioritization is based on the 3-bit header present in the 802.1Q VLAN-tagged Ethernet frame header in the packet entering the SM's Ethernet port. **VLAN ID:** Traffic prioritization is based on the VLAN ID of the packet entering the SM's Ethernet port. **EtherType:** Traffic prioritization is based on a 2 octet Ethertype field in the Ethernet frame entering the SM's Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame. **IP:** Traffic prioritization is based on the source and/or destination IP addresses of the packet entering the SM's Ethernet port. A subnet mask may be included to define a range of IP addresses to match. **MAC:** Traffic prioritization is based on the source and/or destination MAC addresses of the packet entering the SM's Ethernet port. A mask may be included to define a range of MAC addresses to match. The mask is made up of a hex representation of a series of 1s to start the mask and 0s that end the mask. A 1 may not follow a 0. Thus, FF:FF:FF:FF:00:00 is allowed, but FF:00:FF:FF:FF:FF is not. The MAC address is combined with the mask to define the range of allowed MAC addresses.
Details	The **Rule Details** column is used to further configure each classification rule specified in column **Rule Type**.
Priority	**High**: Traffic entering the SM's Ethernet port is prioritized as **high priority** for sending over the radio link (traffic will be sent after VOIP-classified traffic but before Low-classified traffic).

Attribute	Description
	Low: Traffic entering the SM's Ethernet port is prioritized as **low priority** for sending over the radio link (traffic will be sent after VOIP-classified and High-classified traffic is sent).

Configuration > System page

Figure 83 shows the System page.

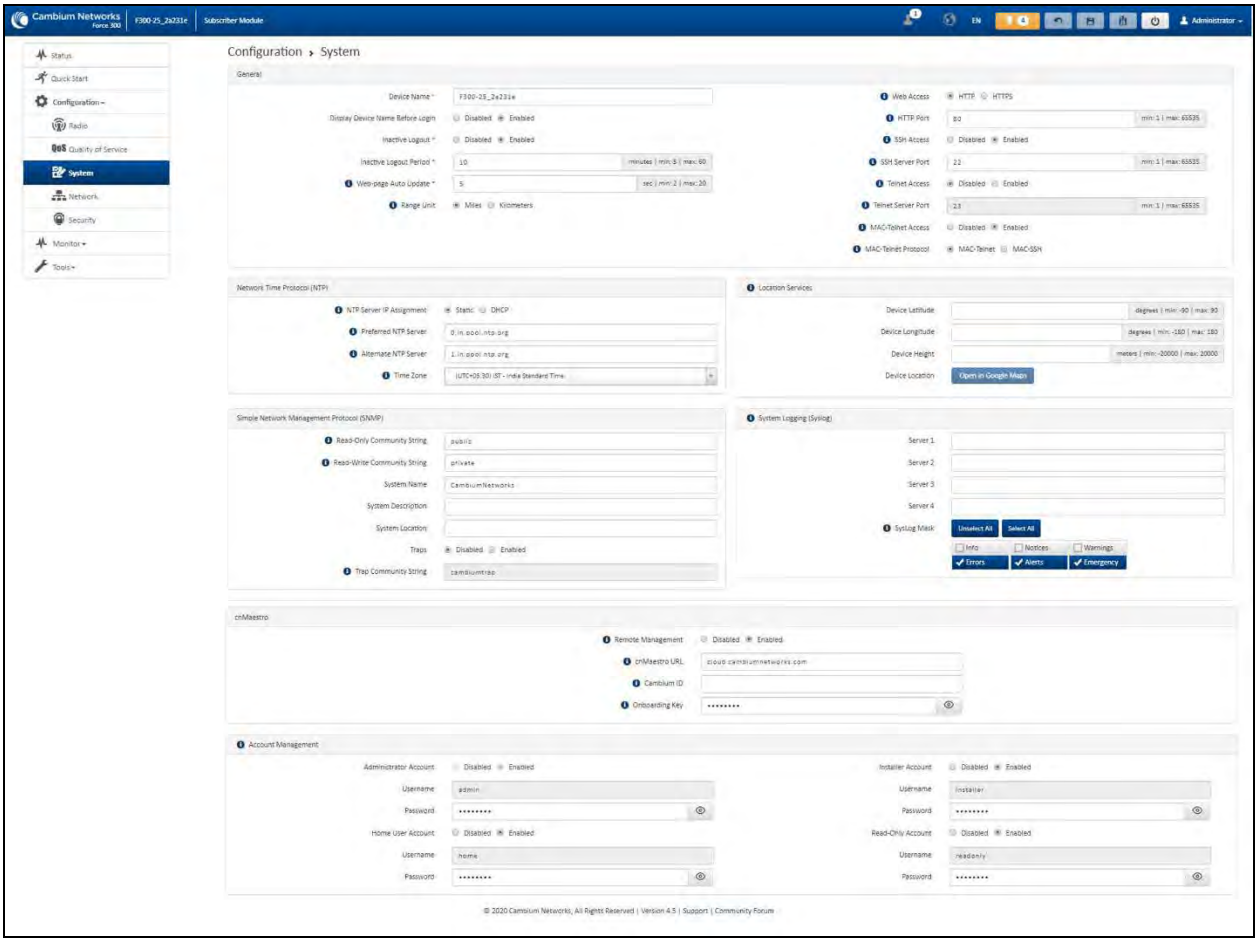


Figure 83: *Configuration > System page parameters*

Table 136 Configuration > System page attributes

Attribute	Description
General	
Device Name	The configured identifier is 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.

Attribute	Description
	Enabled: The configured **Device Name** is displayed upper-left on the device login screen.
Inactive Logout	**Disabled**: The device does not automatically log out users after a period of inactivity. **Enabled**: After the period configured in the **Inactive Logout Period** has elapsed, the device automatically log out the user.
Inactive Logout Period	Represents the amount of time for which a user remains logged in. After this period has elapsed, the user 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 is 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 web management interface of the device is accessed through HTTP. **HTTPS:** The web management interface of the device may only be accessed through 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 Networks 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 through Telnet is not allowed **Enabled:** Command Line Interface access through 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 through a network DHCP server.
Preferred NTP Server	Configure the primary NTP server IP addresses from which the device retrieves time and date information.
Alternate NTP Server	Configure alternate or secondary NTP server IP addresses from which the device retrieves time and date information.

Attribute	Description
Time Zone	The Time Zone option may be used to offset the received NTP time to match the operator's local time zone.
Location Services	
On-board GPS Latitude	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. **Enabled**: SNMP traps for system events are sent to the servers configured in table **Trap Servers**.

Attribute	Description
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. That is, 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 for the appropriate installation. Excessive logging can cause the device log file to fill and starts overwriting the previous entries.
cnMaestro	
Remote Management	When **Enabled**, the device is managed by cnMaestro - the Cambium Networks Remote Management System, allows all Cambium Networks 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 uses for onboarding on to cnMaestro.
Onboarding Key	Configure the password/key associated with the **Cambium-ID** that the device uses for onboarding 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 is 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.

Attribute	Description
	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 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 is 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 permission to view only the **Monitor** page. **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 84 shows the Network page (AP mode).

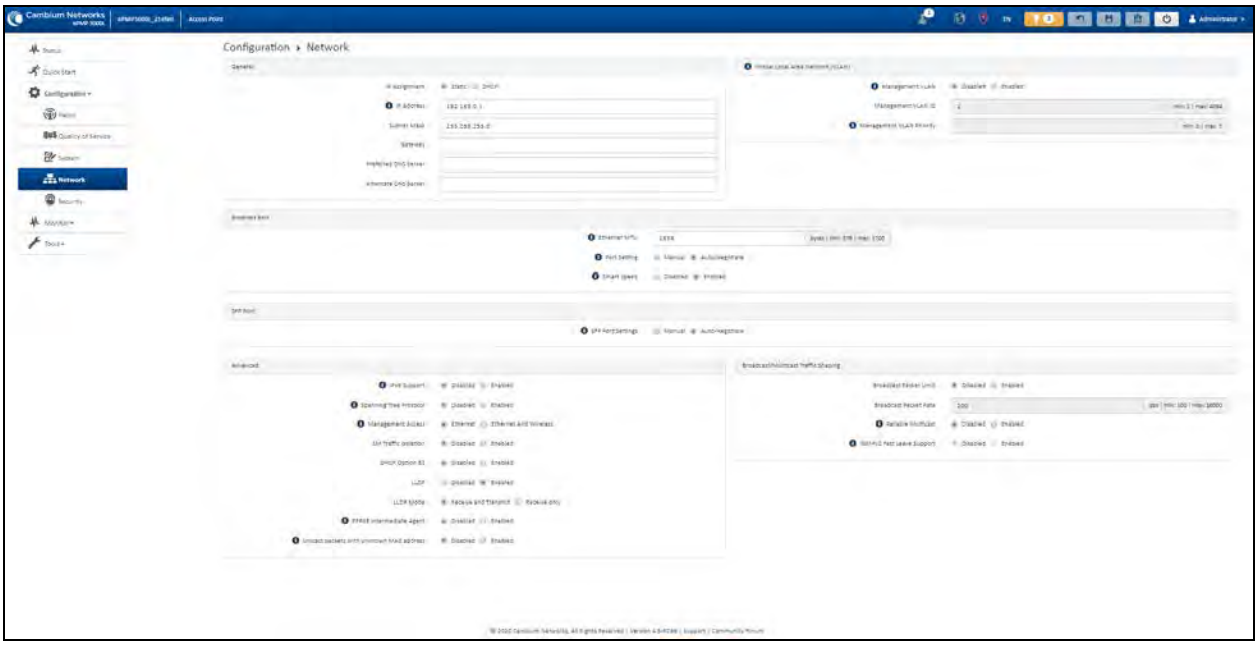


Figure 84: *Configuration > Network page (AP mode)*

Figure 85 shows the Network page (SM mode, Bridge Network mode).

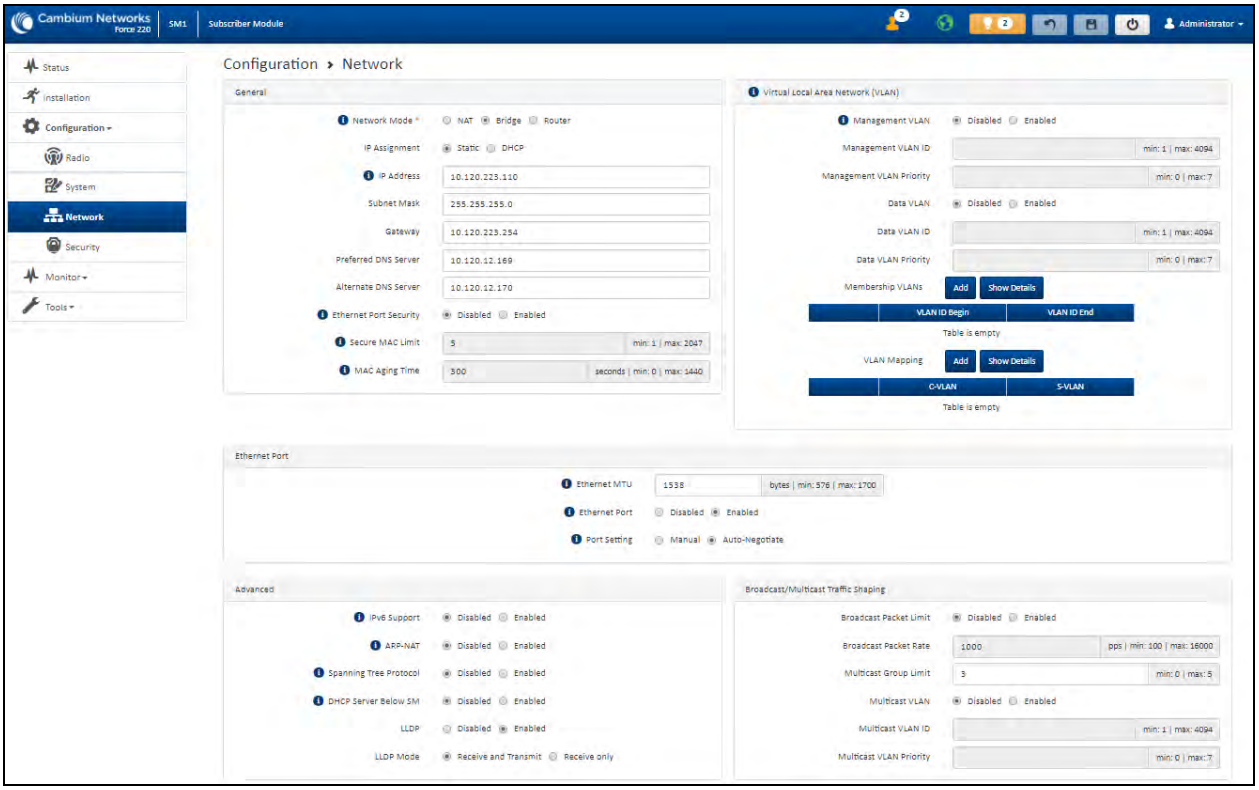


Figure 85: *Configuration > Network page (SM mode, Bridge Network mode)*

Figure 86 shows the Configuration > Network page (SM mode, NAT Network mode) .

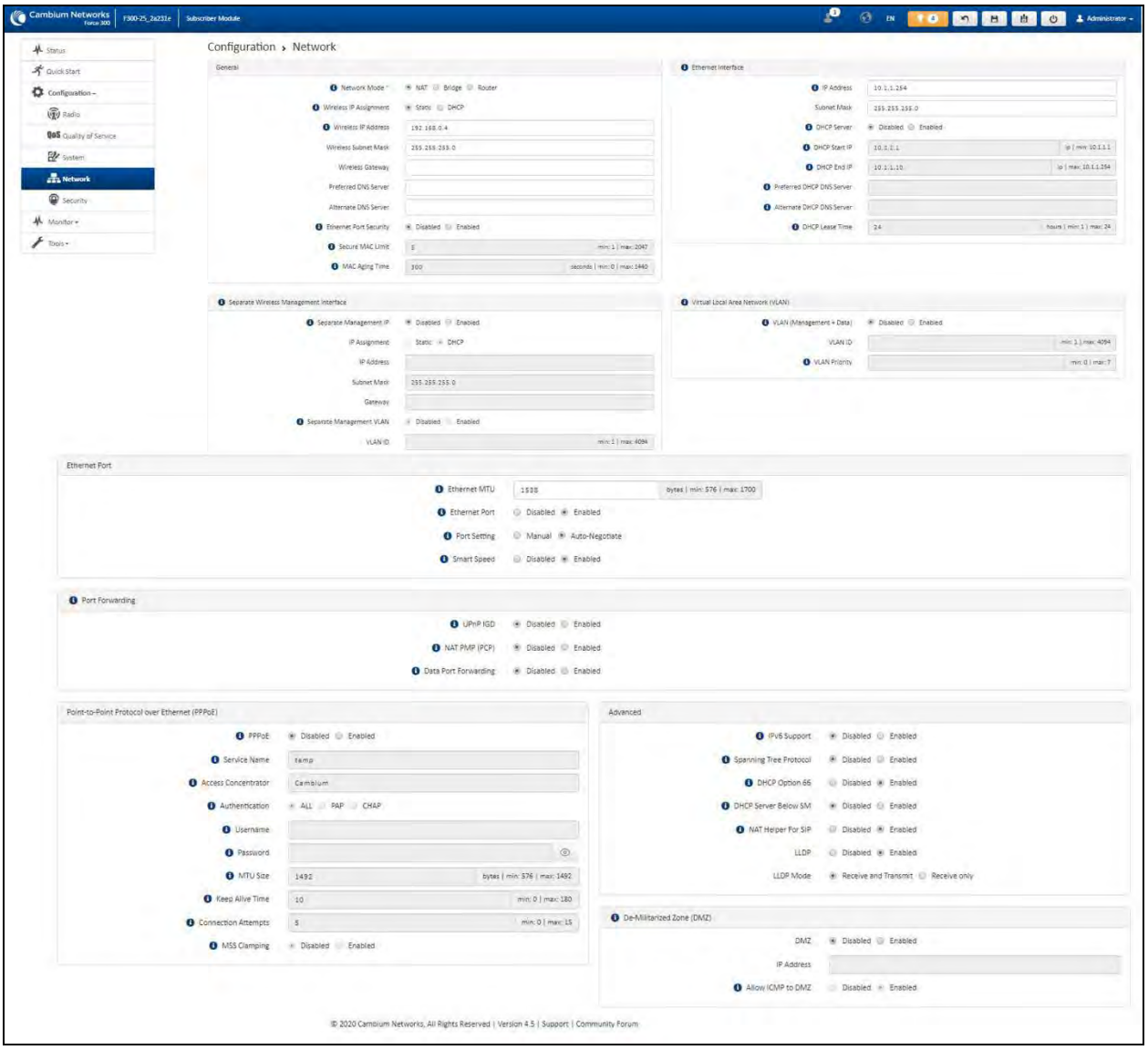


Figure 86: *Configuration > Network page (SM mode, NAT Network mode)*

Figure 87 shows the Configuration > Network page (SM mode, Router mode).

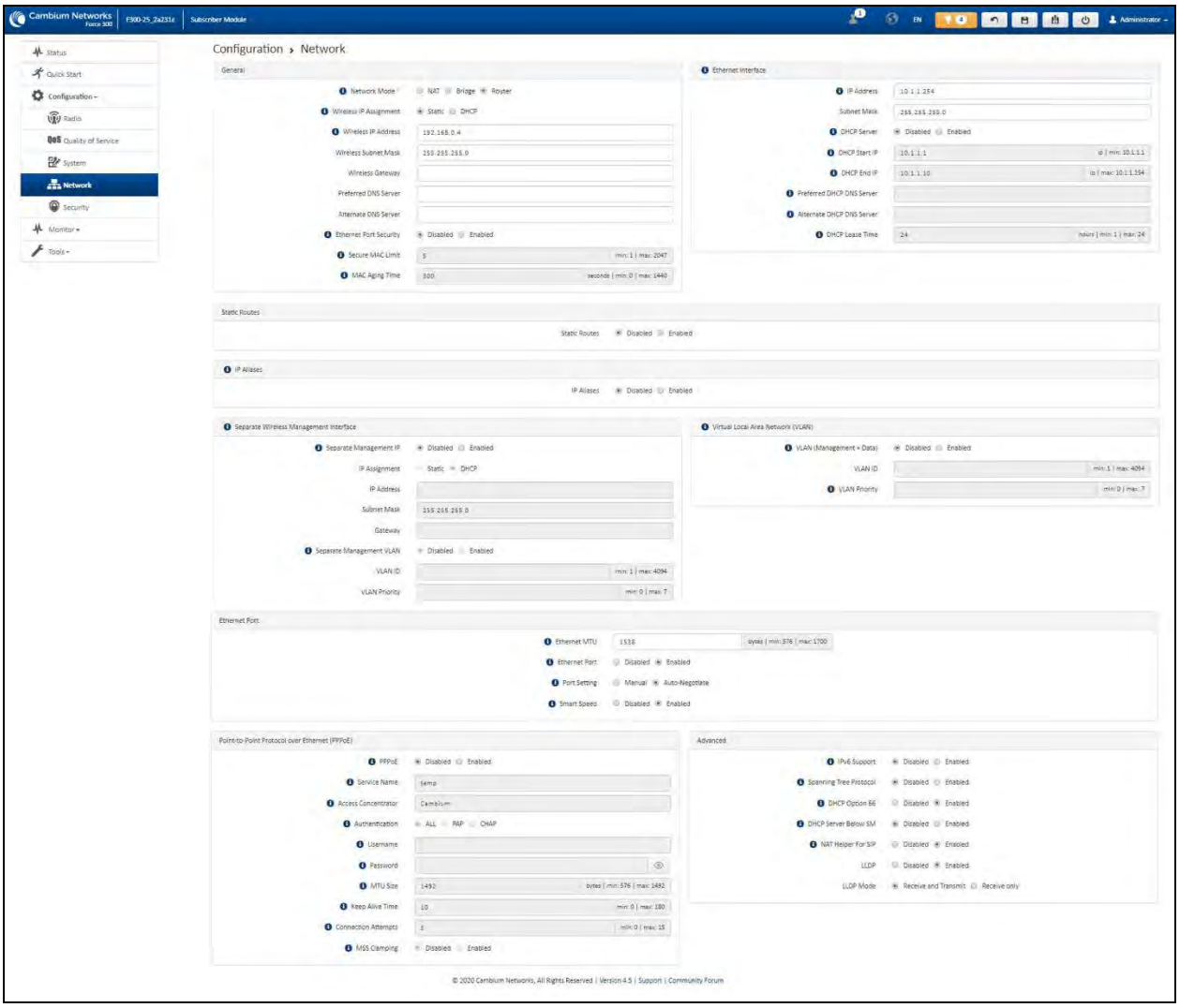


Figure 87: *Configuration > Network page (SM mode, Router mode)*

Table 137 Configuration > Network page attributes

Attribute	Description
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. **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.

Attribute	Description
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 through 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 through 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 through 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.
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.

Attribute	Description
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 SM 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 SM Ethernet port.
Secure MAC Limit (SM mode)	Configure the number of simultaneous secure MAC addresses that is allowed at the Ethernet interface of the SM
MAC Aging Time (SM 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 is 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 (SM 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 (SM 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 belongs to subnet 192.168.2.X.
DHCP Server (SM 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 is 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 (SM NAT mode, Router mode)	Configure the first address which is issued to a DHCP client. Upon additional DHCP requests, the DHCP Start IP is incremented until the local DHCP End IP is reached.
DHCP End IP (SM 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 (SM NAT mode, Router mode)	Configure the primary DNS Server IP address which is used to configure DHCP clients (if local DHCP Server is set to **Enabled**).
Alternate DHCP DNS Server (SM NAT Mode, Router mode)	Configure the secondary DNS Server IP address which is used to configure DHCP clients (if local DHCP Server is set to **Enabled**).
DHCP Lease Time (SM 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 addresses through DHCP request.

Attribute	Description
PPPoE	**Point-to-Point Protocol over Ethernet**: Used for encapsulating PPP frames inside Ethernet frames.
Service Name	Optional entry to set a specific service name to connect to for the PPPoE session. If this is left blank the SM accepts the first service option that comes back from the Access Concentrator specified below, if any. This is limited to 32 characters.
Access Concentrator	An optional entry to set a specific Access Concentrator to connect to for the PPPoE session. If this is blank, the SM accepts the first Access Concentrator which matches the service name (if specified). This is limited to 32 characters.
Static Routes (Subscriber Module Router Mode)	
Static Routes (SM Router mode)	When **Enabled**, it allows the operator to create static routes that 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 equipment has been configured to statically or dynamically route packets to the proper destination. Otherwise, network communication fails. Network Address Translation (NAT) is not performed when the SM is in Router mode.
Target Network IP (SM Router mode)	Configure the target subnet/network's IP address to which the SM should route the packets.
Subnet Mask (SM Router mode)	Configure the subnet mask for the **Target Network IP** address.
Gateway (SM Router mode)	Configure the gateway to which packets that match the **Target Network IP Address** and **Subnet Mask** are sent.
Description (SM Router mode)	Provide a description to easily identify the static route and its purpose.

Attribute	Description
IP Aliases (Subscriber Module Router Mode)	
IP Aliases (SM 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 (SM Router mode)	Configure the IP address for the alias.
Subnet Mask (SM Router mode)	Configure the subnet mask for the alias.
Description (SM Router mode)	Provide a description to easily identify the IP alias and its purpose/connected network.
Separate Wireless Management Interface (SM NAT mode, Router mode)	
Separate Management IP (SM 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 (SM 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 through a network DHCP server.
IP Address (SM NAT mode, Router mode)	Configure the IP address that is used to access the SM's management interface when in NAT mode. The Wireless IP (public IP) does not allow management access.
Subnet Mask (SM 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 belongs to the subnet 192.168.2.X.
Gateway (SM 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 (SM 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 applies to management data. **Disabled**: When disabled, the SM does not have a unique management VLAN.

Attribute	Description
VLAN ID (SM NAT mode, Router mode)	Configure this parameter to include the device's management traffic on a separate VLAN network.
VLAN Priority (SM 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 the management data of the device. 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 (AP 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) (SM mode)	**Enabled:** The device management interface can be assigned to a Management VLAN to separate management traffic (remote module management through 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.

Attribute	Description
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 the 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 VLAN ID (AP mode) (SM Bridge mode)	Configure this parameter to include the device's management traffic on a separate VLAN network. For example, if Management VLAN ID is set to 2, UI access is allowed only from frames tagged with VLAN ID 2. This parameter takes effect only if the MGMT VLAN parameter is enabled.
Management VLAN Priority (AP mode) (SM 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 the 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 (SM mode) (Bridge mode)	**Enabled**: A VLAN tag is 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 SM device WAN port before sending to the SM device LAN port. **Disabled**: When disabled, no changes are made to untagged traffic passing through the SM device.
Data VLAN ID (SM 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 SM device LAN port.
Data VLAN Priority (SM 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 SM device. The default value is 0.

Attribute	Description
Membership VLAN (SM 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 to the other interface. When the SM receives a packet tagged with a VLAN ID that is not present in the **Membership VLAN Table**, the frame is dropped (assuming there is at least one VLAN ID present in the Membership VLAN table or configured as a Data VLAN).
VLAN Mapping (SM Bridge mode)	Configure the **VLAN Mapping Table** to map the C-VLAN of traffic ingressing the Ethernet (LAN) port of the SM to an S-VLAN before being forwarded to the air interface on the UL. In the DL direction, the SM will automatically un-map the S-VLAN to the C-VLAN before forwarding the tagged packets to the Ethernet (LAN) interface of the SM.
C-VLAN (SM 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 (SM Bridge mode)	Configure the S-VLAN ID to which the tagged traffic needs to be mapped. 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 (SM 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**: • If 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 select **Auto-Negotiate**. • If the other end of the Ethernet connection does not support auto-negotiation, then select **Manual** 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.

Attribute	Description
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 (SM mode) (NAT 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 APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise-class devices. With UPnP IGD and PCP protocols, ePMP supports 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) (SM 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 (SM mode) (NAT mode)	The Data Port Forwarding Table is used to define which range of wireless ports are forwarded to a LAN (SM local network) IP address below the SM.
Protocol (SM mode) (NAT mode)	**UDP**: Packet forwarding decisions are based on UDP packets. **TCP**: Packet forwarding decisions are based on TCP packets.
Port Begin (SM mode) (NAT mode)	Configure the beginning of the range of wireless ports to match for forwarding to LAN IP.
Port End (SM mode) (NAT mode)	Configure the end of the range of wireless ports to match for forwarding to LAN IP.
Forwaring IP (SM 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 (SM 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.
Point-to-Point Protocol over Ethernet (PPPoE) (SM mode) (NAT mode, Router mode)	
PPPoE (SM mode) (NAT mode, Router mode)	Point-to-Point Protocol over Ethernet: Used for encapsulating PPP frames inside Ethernet frames.

Attribute	Description
Service Name (SM 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 (SM 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 (SM mode) (NAT mode, Router mode)	**ALL:** This means that CHAP authentication is attempted first, then PAP authentication. The same password is used for both types. **CHAP:** This means that CHAP authentication is attempted. **PAP:** This means that PAP authentication is attempted.
Username (SM mode) (NAT mode, Router mode)	This is the CHAP/PAP username that is used. This is limited to 32 characters.
Password (SM mode) (NAT mode, Router mode)	This is the CHAP/PAP password that is used. This is limited to 32 characters.
MTU Size (SM mode) (NAT mode, Router 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 is able to enter an MTU value up to 1492. However, if the MTU determined in LCP negotiations is less than this user-specified value, the SM uses the smaller value as its MTU for the PPPoE link.
Keep Alive Time (SM 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 sends 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 four more times (for a total of five times) before tearing down the PPPoE session. Setting this to 12 means the keep-alive message is sent every 12 seconds and when there is no acknowledgment, the client tries for a total of 12 times every 12 seconds before tearing down the PPPoE session.
MSS Clamping (SM 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.

Attribute	Description
	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 (AP 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 are 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 (SM mode)	**Disabled**: This blocks DHCP servers connected to the SM device LAN side from handing out IP addresses to DHCP clients above the SM device (wireless side). **Enabled**: This allows DHCP servers connected to the SM device LAN side to assign IP addresses to DHCP clients above the SM device (wireless side). This configuration is typical in PTP links.
Management Access (AP mode)	**Ethernet**: Only allow access to the AP's web management interface through a local Ethernet (LAN) connection. In this configuration, the AP's web management interface may not be accessed from over the air (from a device situated below the SM). **Ethernet and Wireless**: Allow access to the AP's web management interface through a local Ethernet (LAN) connection and from over the air (from a device situated below the SM). APs configured with Management Access Interface set to Ethernet and Ethernet and Wireless are susceptible to unauthorized access.
SM Traffic Isolation (AP mode)	**Disabled**: This is the default mode. When SM isolation is disabled, an SM can communicate with another SM, when both the SMs are associated with the same Access Point (AP). **Enabled**: When the 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 AP. This feature essentially enables the AP to drop the packets to avoid peer-to-peer traffic scenarios.
DHCP Option 82 (AP 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.

Attribute	Description
	Enabled: The device inserts **remote-id** (option ID 0x02) to be the SM MAC address and the **circuit-id** (ID 0x01) to be the AP's MAC address. Those two fields are used to identify the remote device and connection from which the DHCP request was received.
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.
PPPoE Intermediate Agent	When enabled, during the PPPoE Discovery phase the AP inserts access loop identification into the PPPoE PADR packets. This mechanism helps the service provider to distinguish between end hosts connected via Ethernet as an access device (typically, home routers situated below an ePMP subscriber device). On the AP, PPPoE Intermediate Agent enables subscriber line identification by tagging Ethernet frames of corresponding users with Vendor-Specific PPPoE Tags **Circuit ID** (defining AP name, frame, slot, port, and VLAN ID information) and **Remote ID** (defining user phone number).
Broadcast / Multicast Traffic Shaping (SM mode) (Bridge mode)	
Broadcast Packet Limit (SM 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 allowed into the ingress of the radio's Ethernet port.
Broadcast Packet Rate (SM mode) (Bridge mode)	Set the packets per second value to limit the amount of broadcast traffic 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**.
Reliable Multicast	**Enabled**: This feature allows ePMP to support IGMP capable devices. Once a multicast group is identified, the AP allows multicast traffic to be sent only to the SMs within the multicast group. The SMs support up to 5 unique multicast groups. Also, when this option is enabled, the multicast traffic is sent to the SMs using the current Downlink MCS rate.

Attribute	Description
	Disabled: ePMP supports IGMP capable devices but the multicast traffic is sent using MCS 1 on the downlink to all SMs, regardless of the multicast group.
Multicast Group Limit (SM mode) (Bridge mode)	Configure the maximum number of simultaneous multicast groups that the SM allows from devices below it. The default is **3**.
Multicast VLAN (SM mode) (Bridge mode)	**Enabled:** A VLAN tag is 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 (SM 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 (SM 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 the device's **multicast** data. This parameter only takes effect if the **Multicast VLAN** parameter is enabled. Configure this parameter to set the value of the Priority code point field in the 802.1q tag for traffic on the **Multicast VLAN** originating from the SM. The default value is 0.
De-Militarized Zone (Subscriber Module NAT Mode)	
DMZ (SM 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 (SM 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 (SM 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 is enabled.

Configuration > Security page

The **Security** page is used to configure system security features including authentication and Layer2/Layer3 Firewall rules. Figure 88 and Figure 89 shows the Security page (AP mode) and Security page (SM mode).

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 drops 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.

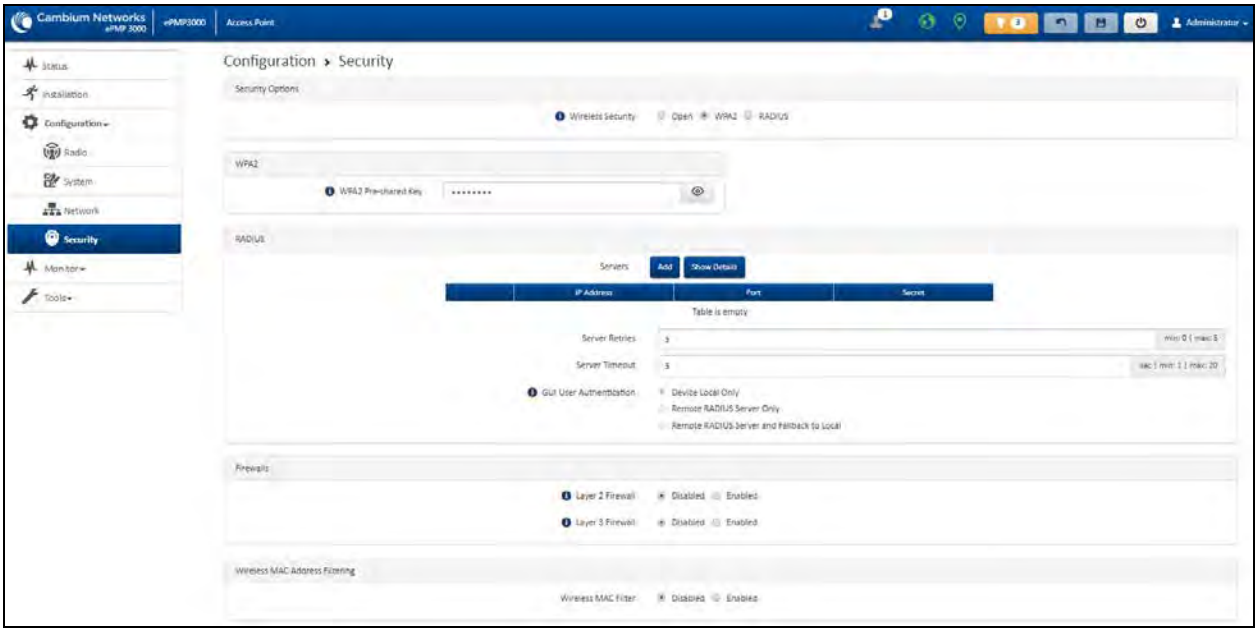


Figure 88: *Configuration > Security page (AP mode)*

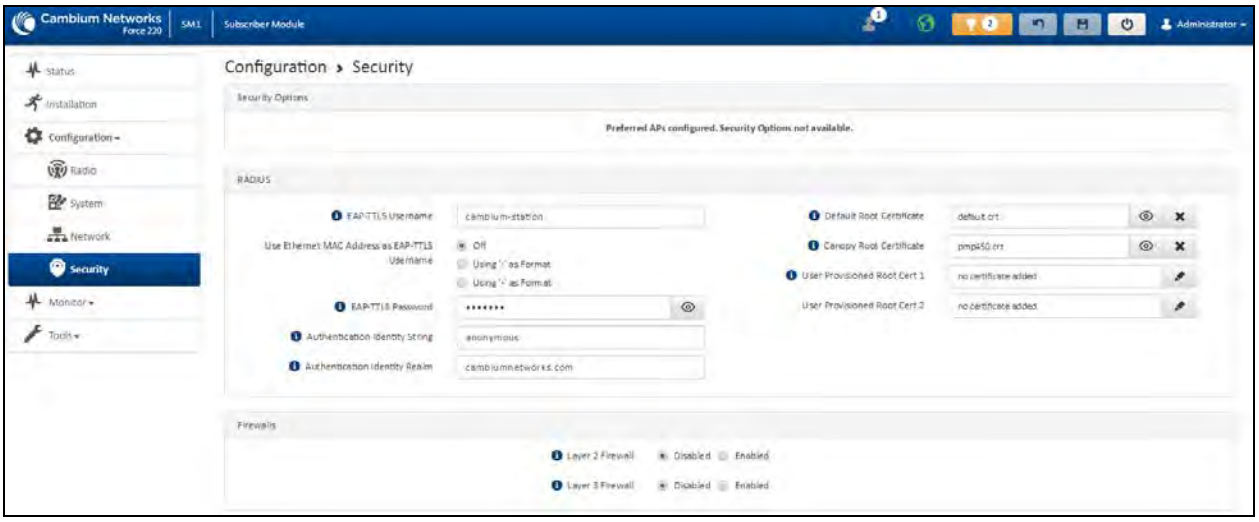


Figure 89: *Configuration > Security page (SM mode)*

Table 209: Configuration > Security page attributes

Attribute	Description
Security Options	
Wireless Security (AP mode)	For AP mode devices, select the security mode enforced upon network entry. For SM mode devices, select the security mode utilized upon network entry attempts. **Open:** All SM devices requesting network entry are allowed registration. **WPA2:** The WPA2 mechanism provides AES radio link encryption and SM network entry authentication. When enabled, the SM must register using the authentication pre-shared key configured on the AP and SM. **RADIUS**: Enables SM authentication through a pre-configured Radius server.
WPA2	
WPA2 Pre-shared Key	Configure this key on the AP, then configure the SM with this key to complete the authentication configuration. This key must be between 8 to 128 symbols.
RADIUS (AP mode)	
Servers (AP mode)	For more Radio servers, click **Add**. Up to three 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 (AP mode)	The number of times the radio retries authentication with the configured Radius server before it fails authentication of the SM.
Server Timeout (AP mode)	Timeout between each retry with the configured RADIUS server before it fails authentication of the SM.
GUI User Authentication (AP 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 UI authentication of the device is performed using a RADIUS server. **Remote RADIUS Server and Fallback to Local:** The UI authentication of the device 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**.
EAP-TTLS Username (SM mode)	Configure the EAP-TTLS Username to match the credentials on the RADIUS server being used for the network.

Attribute	Description
Use Ethernet MAC Address at EAP-TTLS Username (SM mode)	The device MAC Address can be used as the EAP-TTLS Username in either ":" or "-" delimited format.
EAP-TTLS Password (SM mode)	Configure the EAP-TTLS Password to match the credentials on the RADIUS server being used for the network.
Authentication Identity String (SM 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 (SM 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 (SM mode)	Default EAP-TTLS root certificate that must match the certificate on the RADIUS server.
Canopy Root Certificate (SM 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 (SM mode)	Import a user certificate if a certificate different from the default certificates is needed.
User Provisioned Root Cert 2 (SM mode)	Import a second user certificate if a certificate different from the default or 1st user provisioned certificate is needed.
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)	

Attribute	Description
Wireless MAC Filter (AP 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 (AP 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 (AP mode)	Configure the SM's MAC addresses that are permitted or prevented from registering to the AP.
MAC Address (AP mode)	MAC Address of the SM.
Description (AP mode)	Friendly description to identify the SM.

Monitor menu

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

Monitor > Performance page

Figure 90 shows the Performance page.

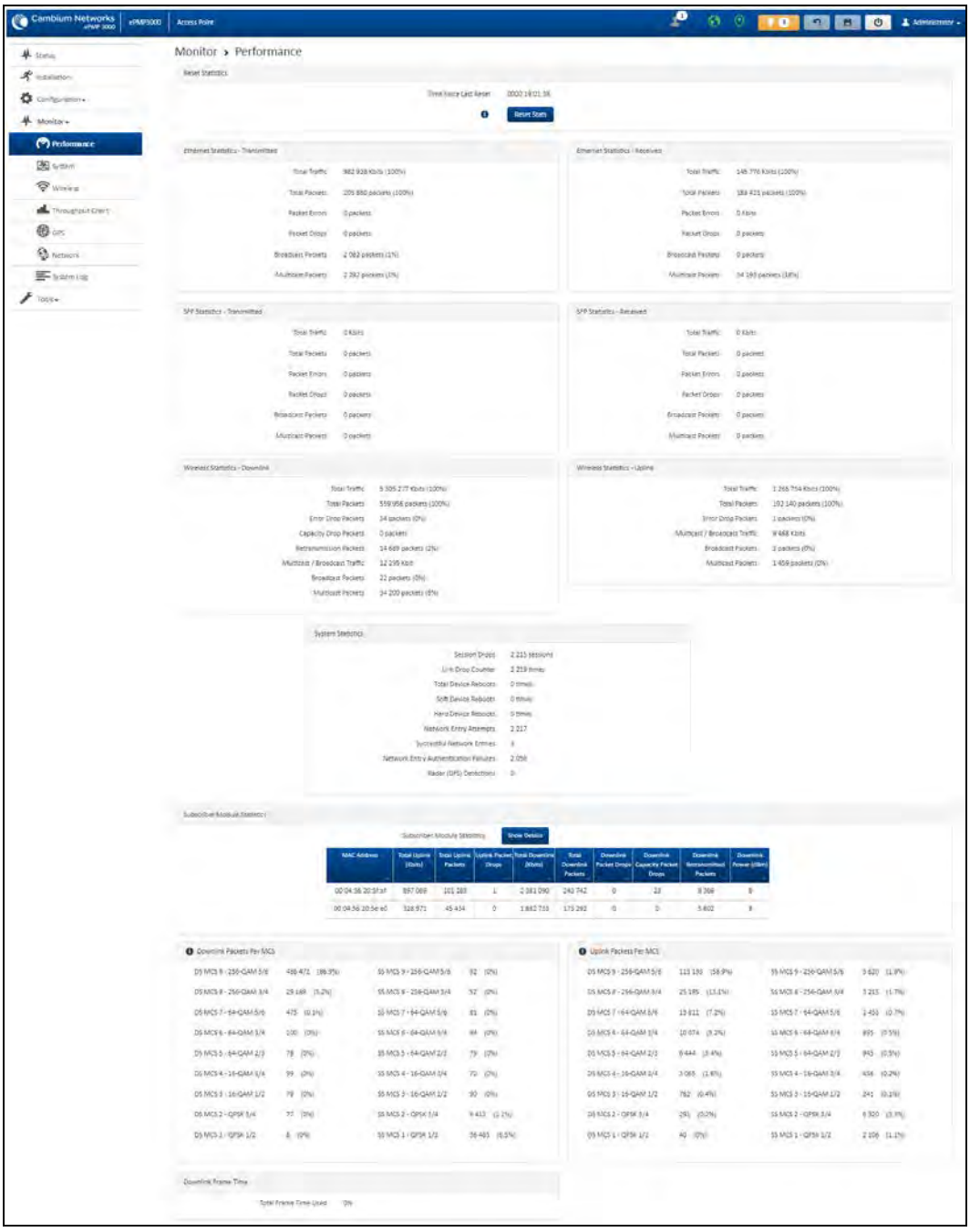


Figure 90: *Monitor > Performance page*

Table 139 Monitor > Performance page attributes

Attribute	Description
Reset Statistics	
Time Since Last Reset	Time since the stats were last reset.

Attribute	Description
Ethernet Statistics – Transmitted	
Total Traffic	The total amount of traffic in KB 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 before sending out from the device's Ethernet interface due to Ethernet setup or filtering issues.
Broadcast Packets	The total number of broadcast packets sent through the device Ethernet interface.
Multicast Packets	The total number of multicast packets sent through the device Ethernet interface.
Ethernet Statistics – Received	
Total Traffic	The total amount of traffic in KB 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 before sending out from the device's wireless interface due to Ethernet setup or filtering issues.
Broadcast Packets	The total number of broadcast packets received through the device Ethernet interface.
Multicast Packets	The total number of multicast packets received through the device Ethernet interface.
SFP Statistics – Transmitted	
Total Traffic	The total amount of traffic in KB 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 before sending out from the device's SFP interface due to setup or filtering issues.
Broadcast Packets	The total number of broadcast packets sent through the device SFP interface.
Multicast Packets	The total number of multicast packets sent through the device SFP interface.
SFP Statistics - Received	
Total Traffic	The total amount of traffic in KB received by the device SFP interface.
Total Packets	The total number of packets received by the device SFP interface.

Attribute	Description
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 before sending out of the device wireless interface due to SFP setup or filtering issues.
Broadcast Packets	The total number of broadcast packets received through the device SFP interface.
Multicast Packets	The total number of multicast packets received through 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 (AP 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 (AP mode)	The total number of packets re-transmitted after transmitting out of the device's 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 KB.
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 through the device wireless interface in KB.
Total Packets	The total number of packets received through the device wireless interface.
Error Drop Packets	The total number of packets dropped before sending out of the device Ethernet interface due to RF errors (packet integrity error and other RF-related packet error).
Capacity Drop Packets (SM 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 KB.

Attribute	Description
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) (SM 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) (SM 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 AP.
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**.
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 (AP mode)	The total number of Network Entry Attempts by Subscriber Module devices.
Successful Network Entries (AP mode)	The total number of successful network entry attempts.
Network Entry Authentication Failures (AP mode)	The total number of failed Network Entry Attempts by SM devices.

Attribute	Description
Radar (DFS) Detections	
Subscriber Module Statistics (AP mode)	
MAC Address	MAC Address of the Subscriber Module connected to the AP.
Total Uplink (KB)	The total amount of traffic received through the AP wireless interface from the Subscriber Module in KB.
Total Uplink Packets	The total number of packets received through the AP wireless interface from this SM.
Uplink Packet Drops	The total number of packets dropped before sending out of the AP Ethernet interface due to RF errors (packet integrity error and other RF-related packet error) from the SM.
Total Downlink (KB)	The total amount of traffic transmitted out of the AP wireless interface in KB.
Total Downlink Packets	The total number of packets transmitted out of the AP wireless interface.
Downlink Packet Drops	The total number of packets dropped after transmitting out of the AP wireless interface due to RF errors (No acknowledgment and other RF-related packet errors).
Downlink Capacity Packet Drops	The total number of packets dropped after transmitting out of the AP 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 AP Wireless interface due to the packets not being received by the SM.
Downlink Power (dBm)	The transmit power of the AP for the downlink packets to the SM.
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 (AP mode)	Percentage of frame time used in the uplink.

Monitor > System page

Figure 91 shows the System page.

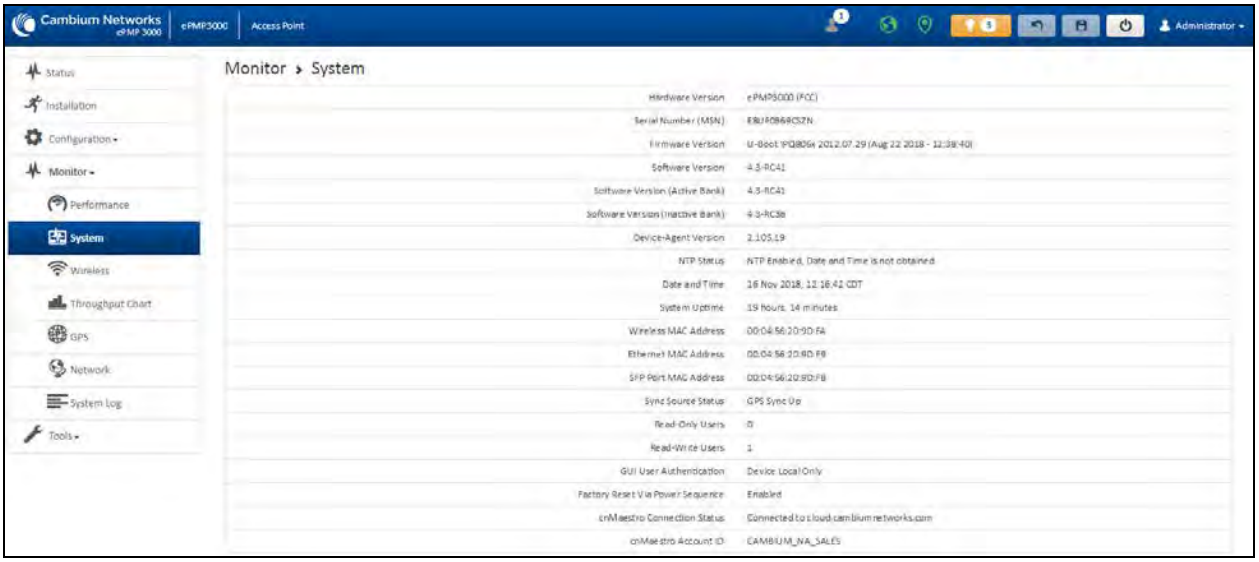


Figure 91: *Monitor > System page*

Table 140 Monitor > System page attributes

Attribute	Description
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 is used upon failure of the active bank. Two software upgrades in sequence updates 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 displays the time configured from the factory.
System Uptime	The total system uptime since the last device reset.

Attribute	Description
Wireless MAC Address	The hardware address of the device's 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.
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. **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 for the Cambium Cloud Server. When Enabled under **Configuration**> **System**, the device is managed by the Cambium Networks Remote Management System, which allows all Cambium devices to be managed from the Cambium Networks Cloud Server.
cnMaestro Account ID	The ID that the device is currently using to be managed by the Cambium Networks Cloud Server.

Monitor > Wireless page

Figure 92 and Figure 93 shows Wireless page (AP mode) and Wireless page (SM mode).

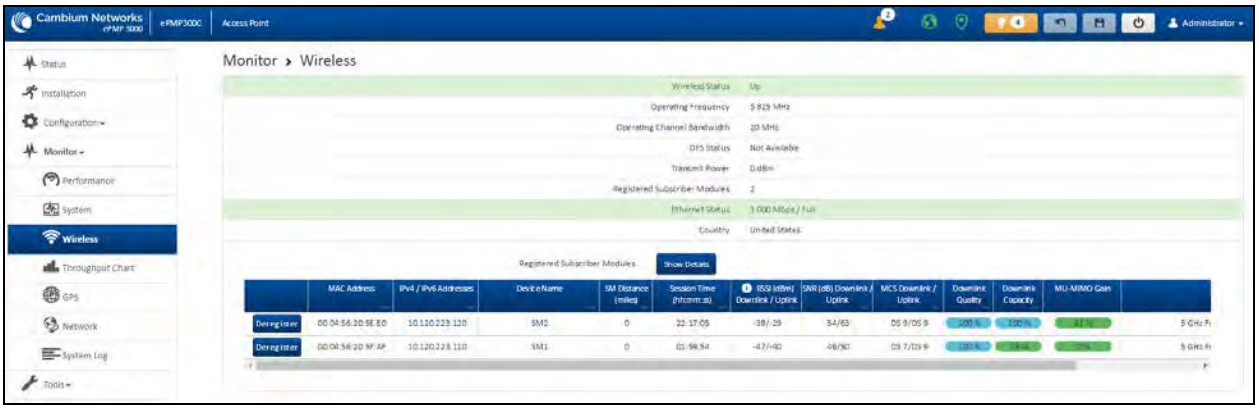


Figure 92: *Monitor > Wireless page (AP Mode)*

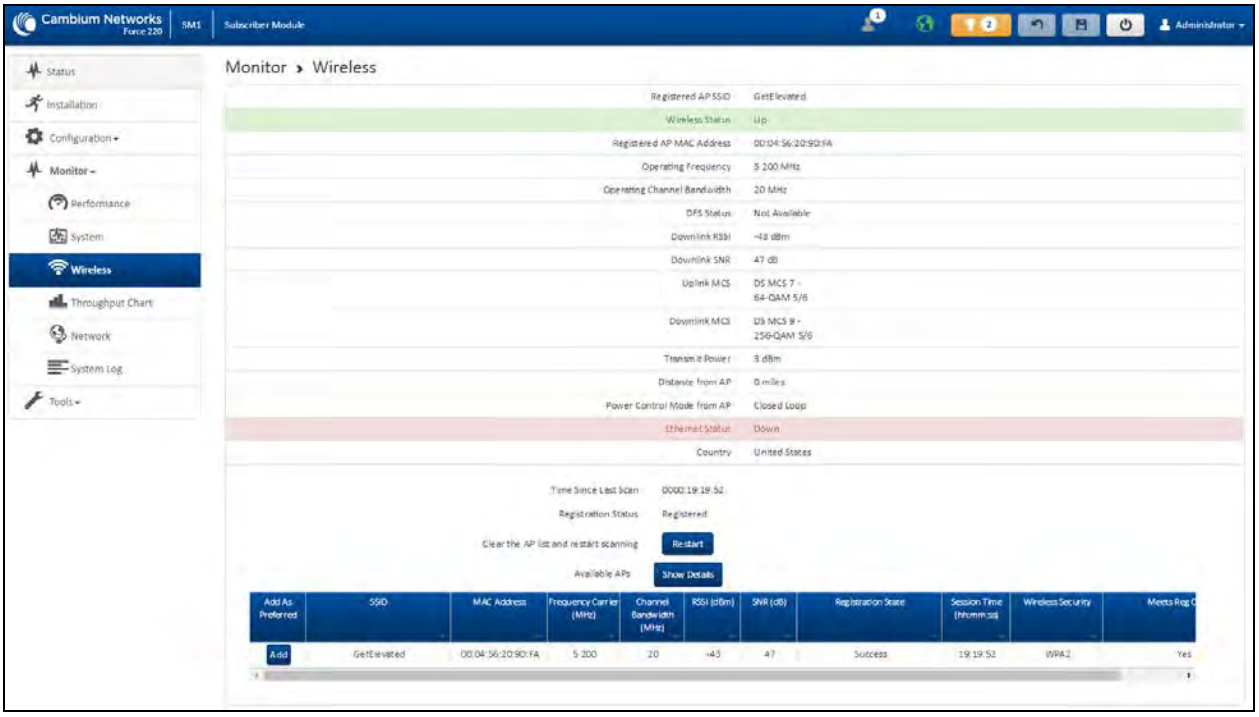


Figure 93: *Monitor > Wireless page (SM Mode)*

Table 141 Monitor > Wireless page attributes

Attribute	Description
Registered Access Point SSID (SM mode only	SSID of the AP to which the SM is registered.
Wireless Status (AP mode)	**Up**: The wireless interface of the device is functioning and sending beacons. **Down**: The wireless interface of the device has encountered an error disallowing full operation. Reset the device to re-initiate the wireless interface.
Wireless Status (SM mode)	**Up**: The device wireless interface is functioning and the device has completed network entry. **Down**: The device's wireless interface has encountered an error disallowing full operation. Evaluate radio and security configuration on the AP and SM device to determine the network entry failure.
Registered AP MAC Address (SM mode)	Wireless MAC address of the AP to which the SM is registered.
Range (SM mode)	The calculated distance from the AP, determined by radio signal propagation delay.
Operating Frequency	The current frequency at which the device is operating.

Attribute	Description
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**: Before transmitting, the device must check the configured **Frequency Carrier** for radar pulses for 60 seconds). If no radar pulses are detected, the device transitions to state **In-Service Monitoring.** **In-Service Monitoring**: Radio is transmitting and receiving normally while monitoring for radar pulses that 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 SNR (SM mode)	The Signal-to-Noise Ratio of the signal being received from the AP.
Transmitter Power	The current power level at which the device is transmitting.
Uplink MCS (AP mode)	Specifies the current MCS utilized for uplink transmission.
Registered Subscriber Modules (AP mode)	The count of registered AP.
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 (AP 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 **Deregister** to disassociate the SM device from the AP.
MAC Address (AP Mode)	The MAC address of the SM wireless interface.

Attribute	Description
IPv4 / IPv6 Addresses (AP mode)	The IP address of the SM wireless interface.
Device Name (AP mode)	The configured device name of the SM wireless interface.
SM Distance (miles)	Indicates the calculated distance of the SM from the AP.
Session Time (hh:mm:ss) (AP mode)	The time duration for which the SM has been registered and in session with the AP.
RSSI (dBm) Downlink / Uplink	Indicates the estimated RSSI of the AP at the SM (first value) and the RSSI of the SM 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 (AP mode)	Current MCS at which the downlink (first value) and uplink (second value) are operating.
Downlink Quality (AP mode)	The downlink quality is based on the current MCS and PER (Packet Error Rate) for this SM.
Downlink Capacity (AP mode)	The downlink capacity is based on the current DL MCS for the highest supported MCS (MCS15). The downlink capacity is based on the current DL MCS for 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 SM.
Add As Preferred (SM mode)	Click **Add** to add the AP to the **Preferred Access Points List** under **Configuration** > **Radio**.
SSID (SM mode)	The SSID of the visible AP.
MAC Address (SM mode)	The MAC address of the visible AP.
Frequency Carrier (MHz) (SM mode)	The current operating frequency of the visible AP.
Channel Bandwidth (MHz) (SM mode)	The current operating channel bandwidth of the visible AP.
RSSI (dBm) (SM mode)	The current measured Received Signal Strength Indicator at the AP.
SNR (dB) (SM mode)	The current measured Signal-to-Noise Ratio (SNR) of the SM to AP link.
Registration State (SM mode)	The indication of the result of the Subscriber Module device network entry attempt:

Attribute	Description
	• **Successful**: The SM registration is successful. • **Failed - Out of Range**: The SM is out of the Access Point's configured maximum range (**Max Range** parameter). • **Failed- Capacity limit reached at Access Point**: The AP is no longer allowing SM network entry due to capacity reached. • **Failed - No Allocation on Access Point**: The SM to AP handshaking failed due to a misconfigured pre-shared key between the SM and AP. • **Failed - SW Version Incompatibility:** The version of software resident on the AP is older than the software version on the SM. • **Failed - PTP Mode: ACL Policy**: The AP is configured with **PTP Access** set to **MAC Limited** and the SM's MAC address is not configured in the AP's **PTP MAC Address** field. • **Failed - Other**: The AP does not have the required available memory to allow network entry.
Session Time (hh:mm:ss) (SM Mode)	This timer indicates the time elapsed since the SM registered to the AP.
Wireless Security (SM mode)	This field indicates the security state of the AP to SM link.
Meets Reg Criteria (SM Mode)	**Yes**: The scanned AP meets the Network Entry criteria defined by the internal Network Algorithm. **No:** The scanned AP does not meet the Network Entry criteria defined by the internal Network Algorithm.

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 94 shows the Throughput Chart page.

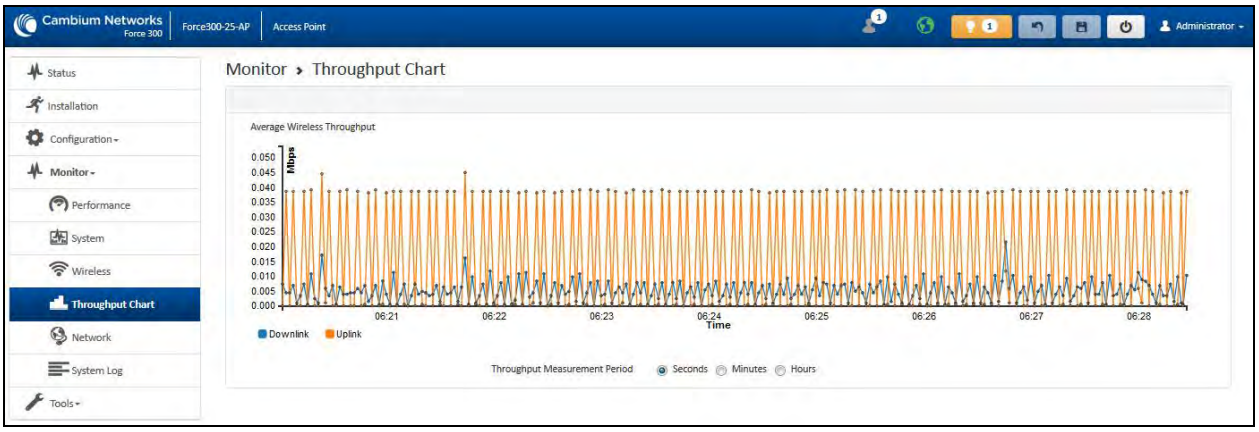


Figure 94: *Monitor > Throughput Chart page*

Table 142 Monitor > Throughput Chart page attributes

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

Monitor > GPS page (AP mode)

Use the GPS Status page to reference key information about the device's GPS readings, tracked satellites, and firmware version. Figure 95 shows the GPS page (AP mode).

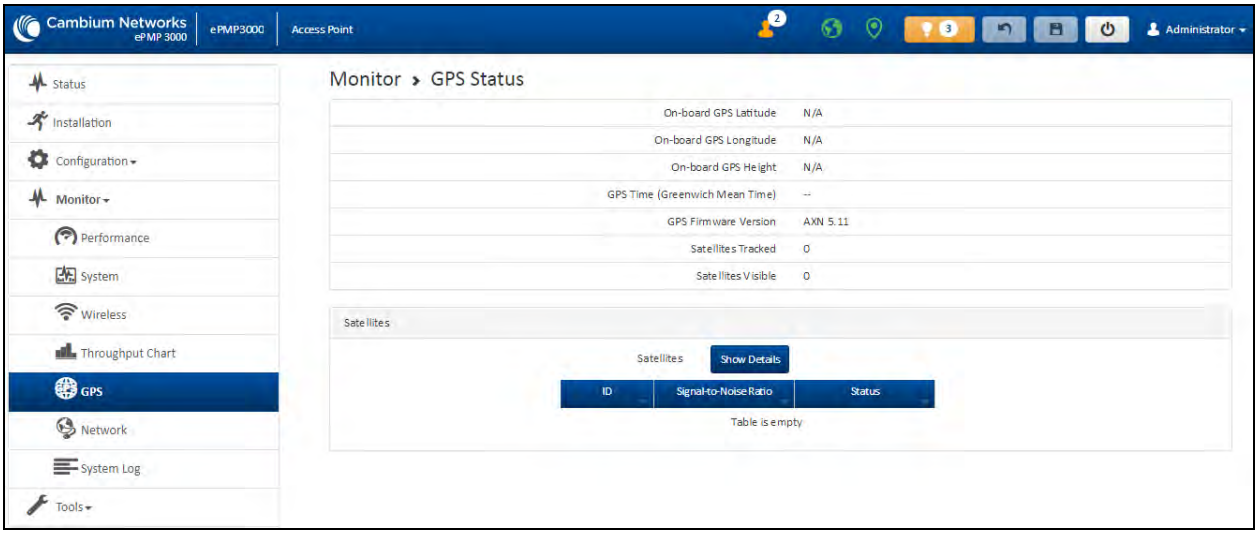


Figure 95: *Monitor > GPS page attributes (AP mode)*

Table 143 Monitor > GPS page attributes (AP mode)

Attribute	Description
On-board GPS Latitude (AP 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 (AP 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 (AP 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) (AP mode)	On a GPS Synchronized ePMP radio, the field is automatically populated with the time from the onboard GPS chip.
GPS Firmware version (AP mode)	On a GPS Synchronized ePMP radio, the field indicates the current firmware version of the onboard GPS chip.
Satellites Tracked (AP mode)	On a GPS Synchronized ePMP radio, the field indicates the number of satellites currently tracked by the onboard GPS chip.
Satellites Visible (AP mode)	On a GPS Synchronized ePMP radio, the field indicates the number of satellites visible to the onboard GPS chip.
Satellites (AP 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 (AP mode)	Represents the Satellite ID.
Signal-to-Noise Ratio (AP mode)	This is an expression of the carrier signal quality concerning signal noise.
Status (AP mode)	Status of each Satellite available.

Monitor > Network page

Use the Network Status page to reference key information about the device network status. Figure 96 shows the Network page.

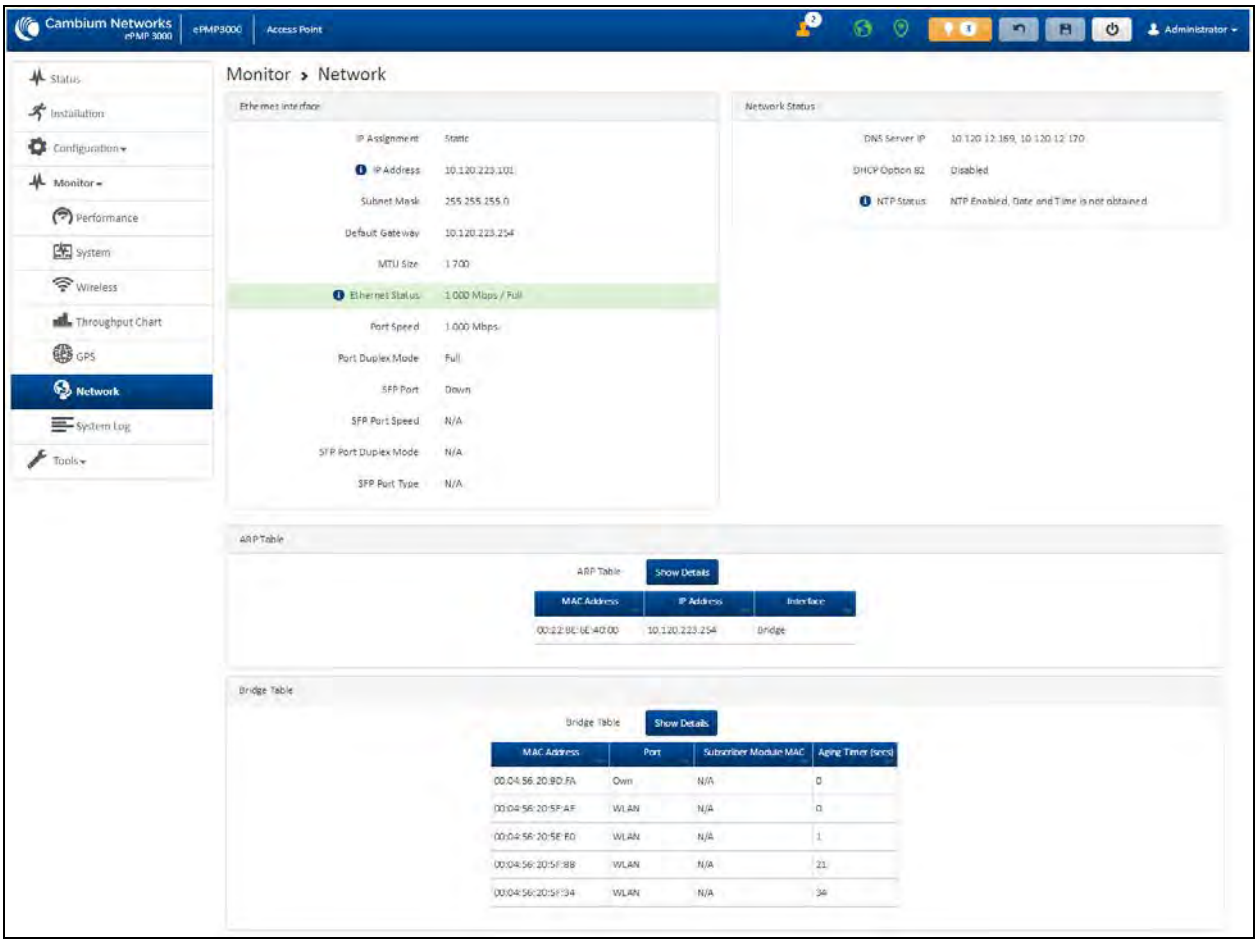


Figure 96: *Monitor > Network page*

Table 144 Monitor > Network page attributes

Attribute	Description
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 through 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).

Attribute	Description
Subnet Mask	Defines the address range of the connected IP network. For example, if Device IP Address (LAN) is configured to 192.168.2.1 and IP Subnet Mask (LAN) is configured to 255.255.255.0, the device will belong to subnet 192.168.2.X.
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.
SM MAC	MAC Address for the connected SM device.
Aging Timer (secs)	Time set for the MAC addresses in the Bridge table before renewal.

Monitor > System Log page

The **System Log** page is used to view the device system log and to download the log file to the accessing PC/device. Figure 97 shows the System Log page.

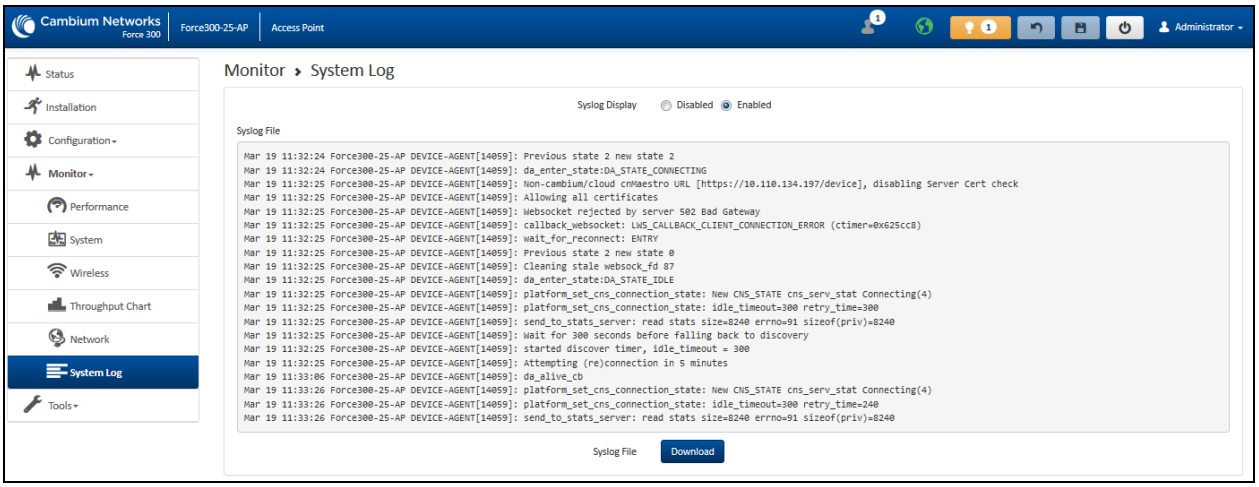


Figure 97: *Monitor > System Log page*

Table 145 Monitor > System Log page attributes

Attribute	Description
Syslog Display	**Enabled**: The system log file is displayed on the management UI. **Disabled**: The system log file is hidden on the management UI.
Download	Used 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

The **Software Upgrade** page is used to update the device radio software to take advantage of new software features and improvements. Figure 98 shows the Software Upgrade page.

Attention

Refer to **Release Notes** associated with each software release for special notices, feature updates, resolved software issues, and known software issues.

The Release Notes can be found at Cambium Networks Support Center.

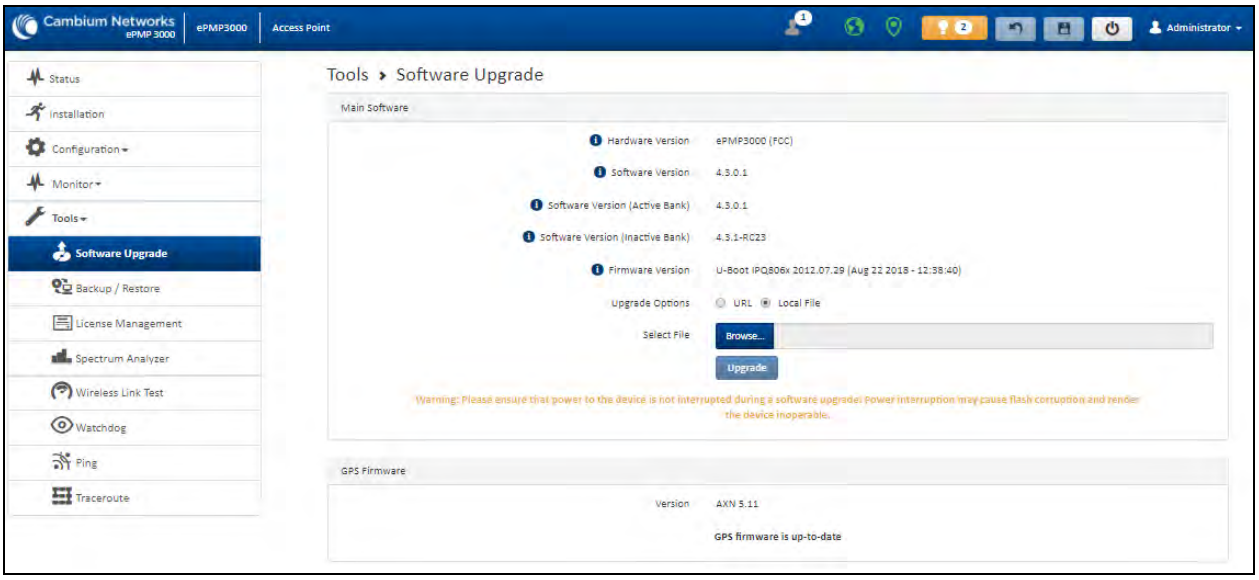


Figure 98: *Tools > Software Upgrade page*

Table 146 Tools > Software Upgrade page attributes

Attribute	Description
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 is 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 the software is 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 through 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.

Attribute	Description
Select File	Click **Browse** to select a local file (located on the device accessing the web management interface) for upgrading the device software.
Upgrade	Click the **Upgrade** button to begin the software upgrade process. Ensure that the 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 through 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** and select the local file containing the GPS firmware upgrade package.
Select File	Click **Browse** and 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

The **Backup/Restore** page is used to update the device radio software to take advantage of new software features and improvements. Figure 99 shows the Backup/Restore page.

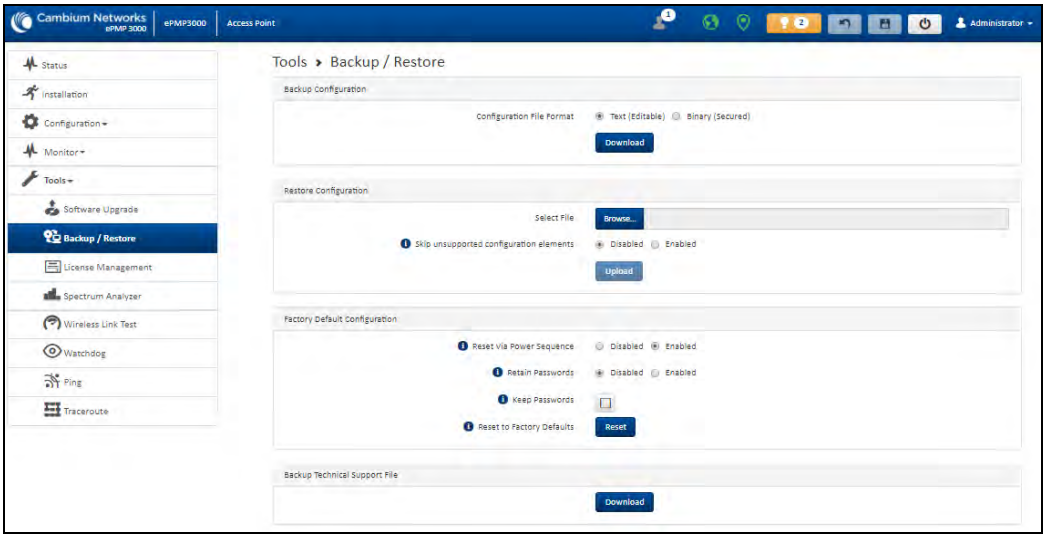


Figure 99: *Tools > Backup/Restore page*

Table 147 Tools > Backup/Restore page attributes

Attribute	Description
Backup Configuration	
Configuration File Format	**Text (Editable)**: This option downloads the configuration file in the **.json** format and can be viewed and/or edited using a standard text editor. **Binary (Secured)**: This option downloads 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** and 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. **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 UI and CLI access does not be defaulted and remains 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 the default and remains unchanged. This is a one-time option, and it does not apply to factory default procedures completed by power cycling (Reset through the 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 SM device in the default configuration, it may not be able to register to an AP 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 Networks 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:

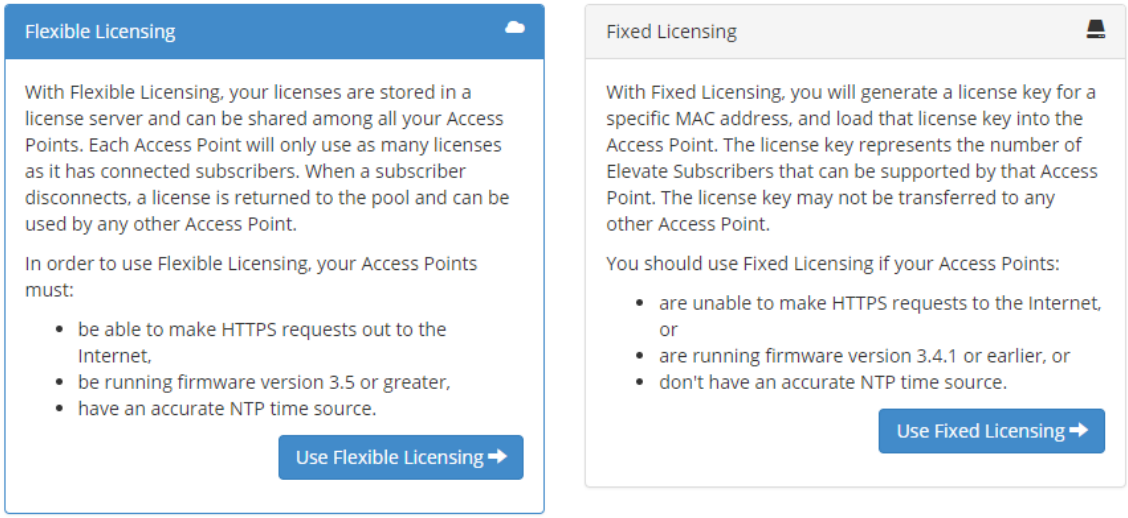


Figure 100: *AP ePMP Elevate license management options*

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. Figure 101 shows the License Management page.

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.

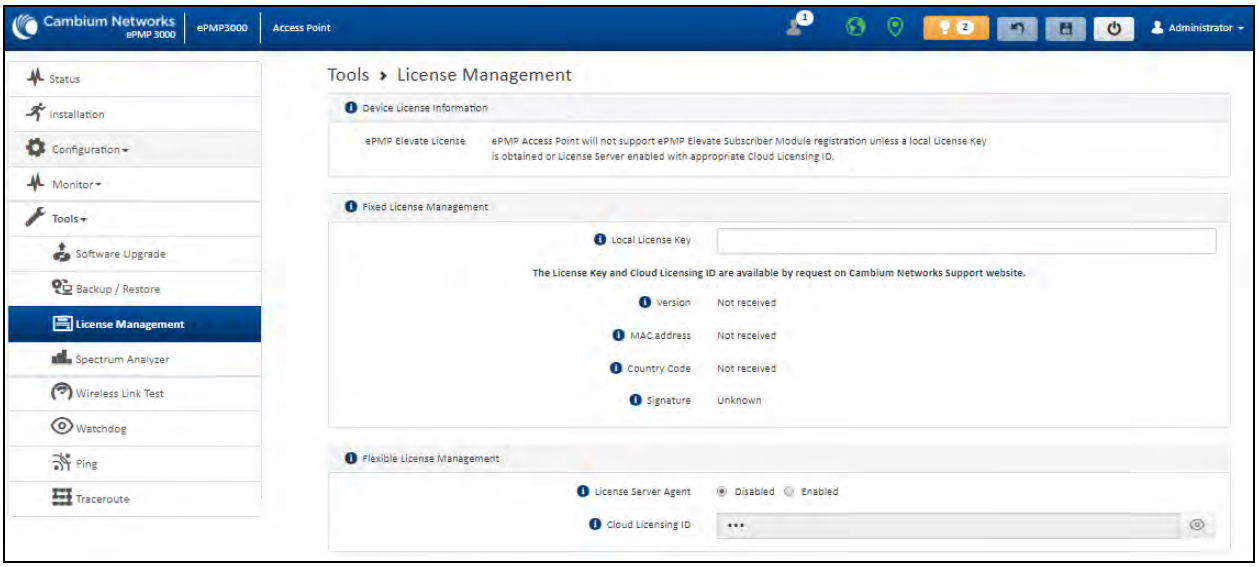


Figure 101: *Tools > License Management page*

Table 148 Tools > License Management attributes

Attribute	Description
Flexible License Management	
License Server Agent	**Disabled:** No communication with the License Server is established. **Enabled:** Enables the **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 the 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.

Attribute	Description
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.
NTP Status	Represents whether the current time and date are 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 Cambium Networks Support Site 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** displays **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

The Spectrum Analyzer feature is no longer available from the web User Interface. This tool is now available as a stand-alone application and available at: https://support.cambiumnetworks.com/files/epmp_tools_and_docs.

Tools > eAlign page

The eAlign page is used to aid with subscriber link alignment. Figure 102 shows the eAlign page.

Figure 102: *Tools > eAlign page*

Note

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

ePMP supports Automatic Transmit Power Control (ATPC) where the Subscriber Module devices are instructed by the Access Point to adjust their Tx power 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, perform the following steps:

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

Tools > Wireless Link Test page

The Wireless Link Test page is used 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 103 shows the Wireless Link Test page.

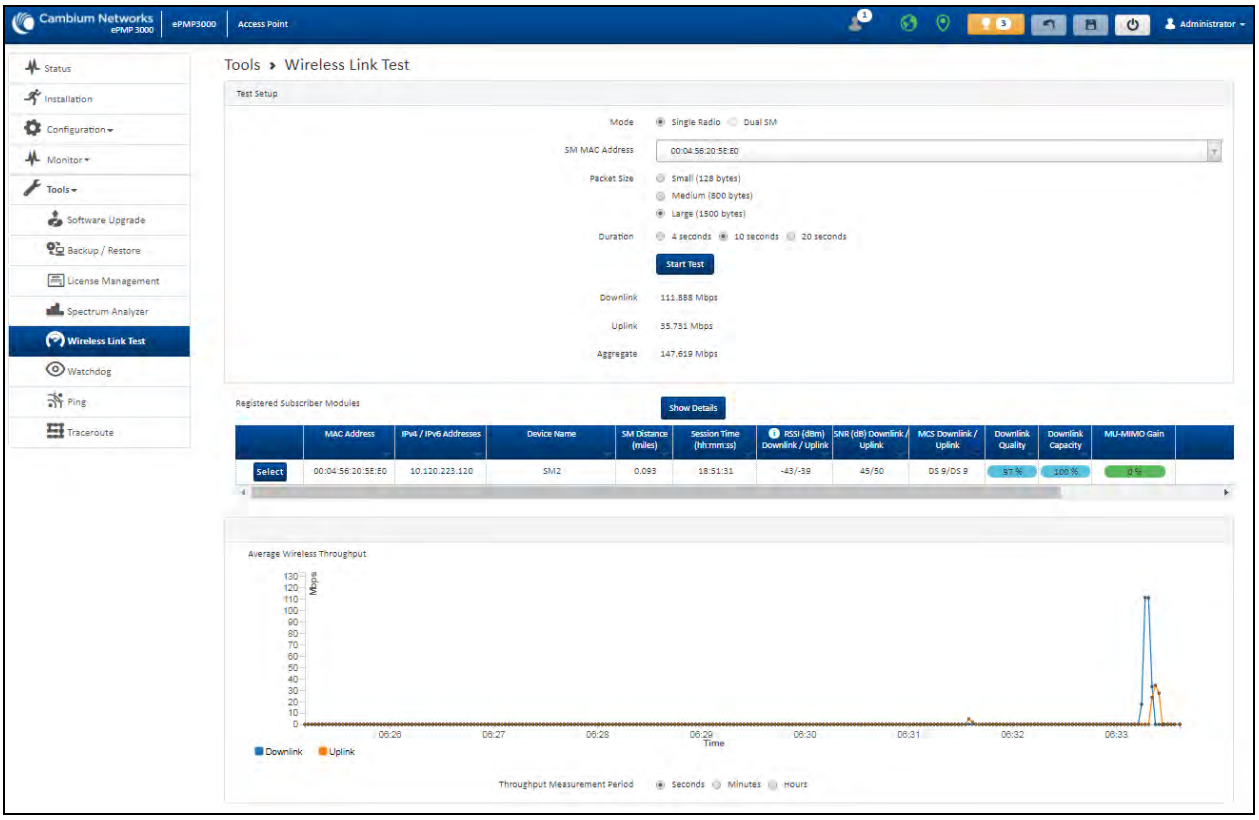


Figure 103: *Tools > Wireless Link Test page*

Table 149 Tools > Wireless Link Test page attributes

Attribute	Description
Test Setup	
Mode	**Single Radio:** The link test is conducted between the AP and one SM. **Dual SM:** The link test is conducted between the AP and two grouped SM (must be operating in MU-MIMO mode).
SM MAC Address	Choose the MAC Address of the SM with which the wireless link test is 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	Indicates the result of the throughput test on the downlink, in Mbps.
Uplink	Indicates the result of the throughput test on the uplink, in Mbps.

Attribute	Description
Average	An auto-adjusting chart displaying the average throughput of the link.
Registered SM	Provides information about the wireless link of each registered SM.

Tools > Watchdog page

The 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 104 shows the Watchdog page.

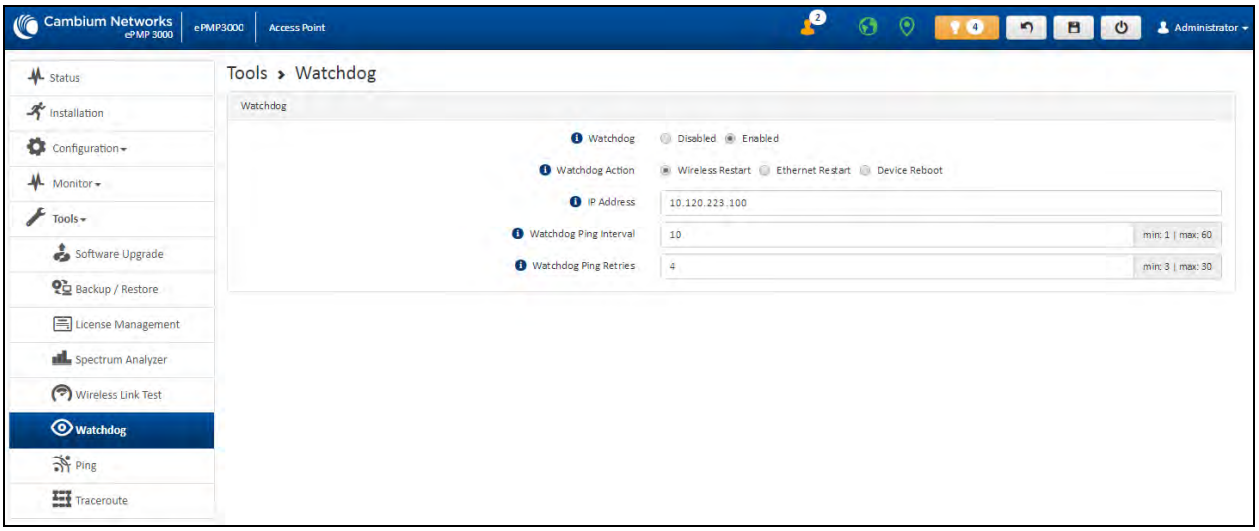


Figure 104: *Tools > Watchdog page*

Table 150 Tools > Watchdog page attributes

Attribute	Description
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.
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.

Attribute	Description
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 before considering the test failed (and conducting the action defined in **Watchdog Action**).

Tools > Ping page

The Ping page is used 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 (DNS server failure).

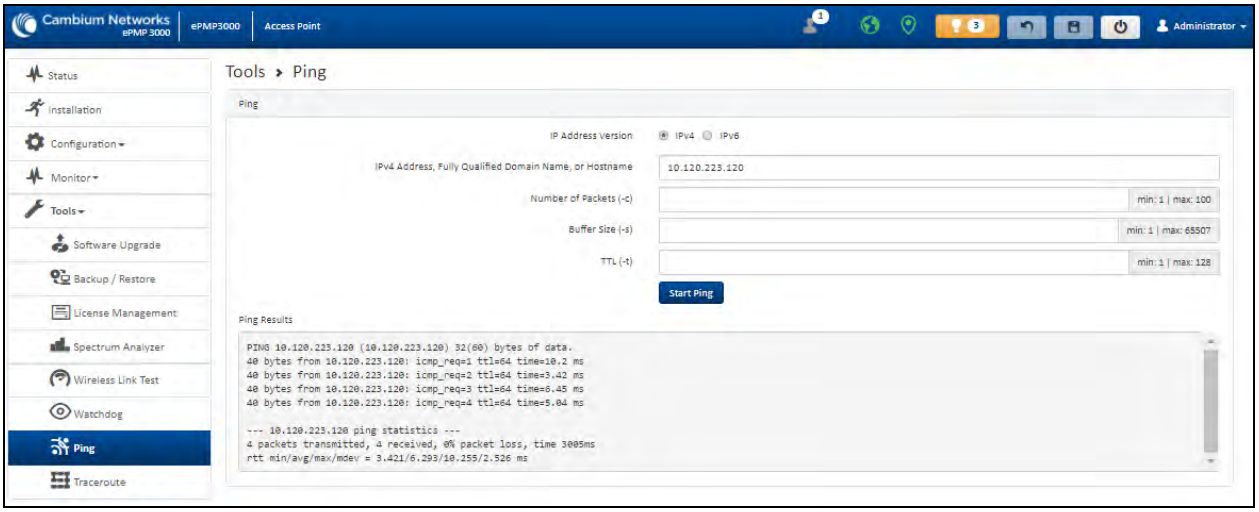


Figure 105: *Tools > Ping page*

Table 151 Tools > Ping page attributes

Attribute	Description
Ping	
IP Address Version	**IPv4:** The ping test is conducted via the IPv4 protocol. **IPv6**: The ping test is conducted via the IPv6 protocol.
IP Address	Enter the IP address of the ping target.
Number of packets (-c)	Enter the total number of ping requests to send to the target.
Buffer size (-s)	Enter the number of data bytes to be sent.
TTL (-t)	Set the IP Time-To-Live (TTL) for multicast packets. This flag applies if the ping target is a multicast address.
Ping results	The results of the ping test are displayed in the box.

Tools > Traceroute page

The Traceroute page is used to display the route (path) and associated diagnostics for IP connectivity between the device and the destination specified. Figure 106 shows the Traceroute page.

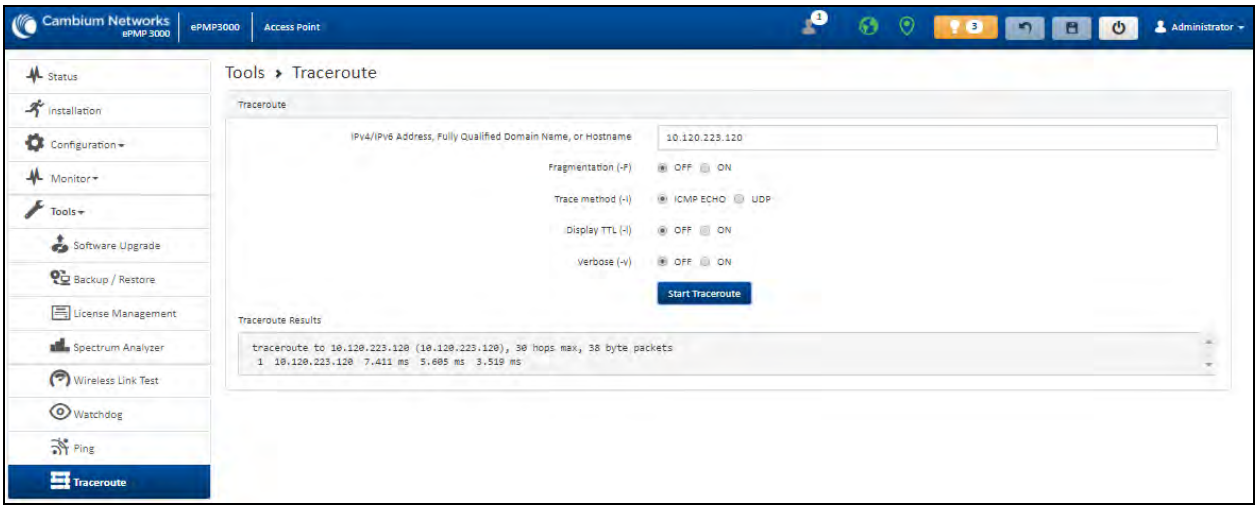


Figure 106: *Tools > Traceroute page*

Table 152 Tools > Traceroute page attributes

Attribute	Description
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 (-I)	**ON:** Display TTL values for each hop on the route. **OFF:** Suppress display of TTL values for each hop on the route.
Verbose (-v)	**ON:** ICMP packets other than TIME_EXCEEDED and UNREACHABLE are displayed in the output. **OFF**: Suppress display of extraneous ICMP messaging.
Traceroute Results	Traceroute test results are displayed in the box.

Operation and Troubleshooting

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

General Planning for troubleshooting

Effective troubleshooting depends in part on measures taken before experiencing the trouble in the network. Cambium Networks recommends the following measures for each site:

- Identify troubleshooting tools that are available at your site (such as a protocol analyzer).
- 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
- 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 an advantage of new features and software improvements for the ePMP system, visit Cambium Networks ePMP Software website: https://support.cambiumnetworks.com/files/epmp

To upgrade the device software, perform the following steps:

1. Login to the device UI through 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.

   Click **Upgrade**
5. 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 the hardware

This section describes the procedure to test the hardware when it fails while starting or during operation.

Before start testing the hardware, verify that all the outdoor cables which connects the device to equipment inside the building, are of the supported type, as defined in Ethernet cabling.

Checking the power supply LED

When the power supply is connected to the main power supply, the expected LED behavior is:

- The power LED illuminates continuously in Green color.

If the expected LED operation does not occur, or if a fault is suspected in the hardware, check the LED states and choose the correct test procedure.

- Power LED is OFF
- Ethernet LED is OFF

Power LED is OFF

Meaning: Either the power supply is not receiving power from the AC/DC outlet, or there is a wiring fault in the unit.

Action: Remove the device cable from the PSU and observe the effect on the power LED. If the power LED does not illuminate, confirm that the main 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 are correct and not crossed.

Test Ethernet packet errors reported by the device

Login 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 license this procedure and consider using the Test ping packet loss procedure.

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. Refer to *ePMP 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 ten in one 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.

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 takes 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 the number of 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 the process of testing 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, then perform the following steps:

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 AP, 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 AP and the SM **Preferred Access Points List**.
6. Check that the software at each end of the link is the same version.
7. Check that the desired AP SSID is configured in the SM **Preferred Access Points List**.
8. On the SM, check the **DL RSSI** and **DL CINR** values. Verify that for the SM installed distance, that the values are consistent with the values reported by the LINKPlanner tool.
9. Check Tx Power on the 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, ensure 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 the data rates required

If there is some activity, but the link is unreliable or does not achieve the data rates required, then perform the following steps:

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 the 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 .

1. Remove the Ethernet cable from the PoE jack of the power supply for at least 10 seconds.
2. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds**and disconnect the cable to power off the ePMP device for 3-5 seconds. (1st power cycle).
3. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds**and disconnect the cable to power off the ePMP device for 3-5 seconds. (2nd power cycle).
4. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds**and disconnect the cable to power off the ePMP device for 3-5 seconds. (3rd power cycle).
5. Reconnect the Ethernet cable to re-supply power to the ePMP device for **3-5 seconds**and disconnect the cable to power off the ePMP device for 3-5 seconds. (4th power cycle).
6. Reconnect the Ethernet cable to re-supply power to the ePMP device for at least **30 seconds** and allow it to go through the boot-up procedure

Note

Device goes through an additional reset automatically. This resets the current configuration files to factory default configuration (such as IP addresses, Device mode, and RF configuration). The device can be pinged from a PC to check if boot-up is complete (Successful ping replies indicate boot-up is complete).

7. Access the ePMP device using the default IP address of 192.168.0.1 (AP) or 192.168.0.2 (SM).

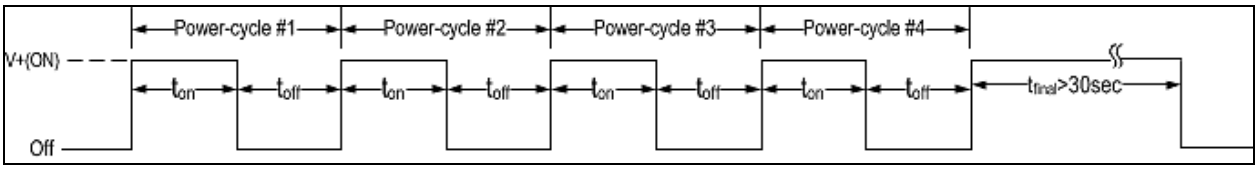


Figure 107: *Power cycle timings*

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 is powered on. This should be 3-5 seconds.
t_{off}	The time duration for which the device is powered off. This should be 3-5 seconds.

Glossary

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CINR	Carrier to Interference plus Noise Ratio
CMM	Cluster Management Module
DFS	Dynamic Frequency Selection
EIRP	Equivalent Isotropically Radiated Power
EMC	Electromagnetic Compatibility
EMD	Electromagnetic Discharge
ETH	Ethernet
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FEC	Forward Error Correction
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IC	Industry Canada
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LoS	Line of Sight
MIMO	Multiple In Multiple Out
MIR	Maximum Information Rate
MU-MIMO	Multi-User Multiple In Multiple Out
MTU	Maximum Transmission Unit
nLOS	Near Line of Sight
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PC	Personal Computer

Term	Definition
PMP	Point to Multipoint
PTP	Point to Point
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keyed
RF	Radio Frequency
RMA	Return Merchandise Authorization
RSSI	Received Signal Strength Indication
RTTT	Road Transport and Traffic Telematics
RX	Receive
SAR	Standard Absorption Rate
SNMP	Simple Network Management Protocol
SW	Software
TDD	Time Division Duplex
TDWR	Terminal Doppler Weather Radar
TX	Transmit
UNII	Unlicensed National Information Infrastructure
URL	Uniform Resource Locator

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified ConnectedPartners to deliver purpose-built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

User Guides	http://www.cambiumnetworks.com/guides
Technical training	https://learning.cambiumnetworks.com/learn
Support website (enquiries)	https://support.cambiumnetworks.com
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Cambium Networks™ www.cambiumnetworks.com