Radio page - PMP 450 AP 3.5 GHz

Figure 35: *PMP 450 AP Radio attributes - 3.5 GHz*

Device Type

Device Setting :	AP SM

Radio Configuration

Frequency Carrier :	None
Channel Bandwidth :	10 MHz
Frame Period :	5.0 ms 2.5 ms
Cyclic Prefix :	One Sixteenth
Color Code :	0 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	Enabled Disabled
Sector ID :	0

MAC Control Parameters

MIMO Rate Adapt Algorithm :	MIMO-A/B
Downlink Maximum Modulation Rate :	8x
Uplink Maximum Modulation Rate :	8x
Nomadic Mode :	Enabled Disabled

Frame Configuration

Max Range :	1 miles (Range: 1 — 40 miles / 64 km)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	4 (Range: 1 — 15)
Auto Contention :	Enabled Disabled
Broadcast Repeat Count :	2 (Range: 0 — 2)
Co-located Frame Configuration Option :	Disable

Power Control

Transmit Power :	16 dBm (Range: -30 — +25 dBm) (13 dBm B / 13 dBm A)
External Gain :	0 dBi (Range: 0 — +70 dBi)
SM Receive Target Level :	-52 dBm (Range: -77 — -37 dBm) combined power
Adjacent Channel Support :	Enabled Disabled

Multicast Data Control

Multicast Data Channel :	Disable
Multicast Repeat Count :	0 (Range: 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0 — 12187 kbps)

Advanced

SM Registration Limit :	238 (Range: 1 — 238)
Receive Quality Debug :	Enabled Disabled
Frame Alignment Legacy Mode :	OFF Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source.
SM Link Test Mode Restriction :	Enabled Disabled

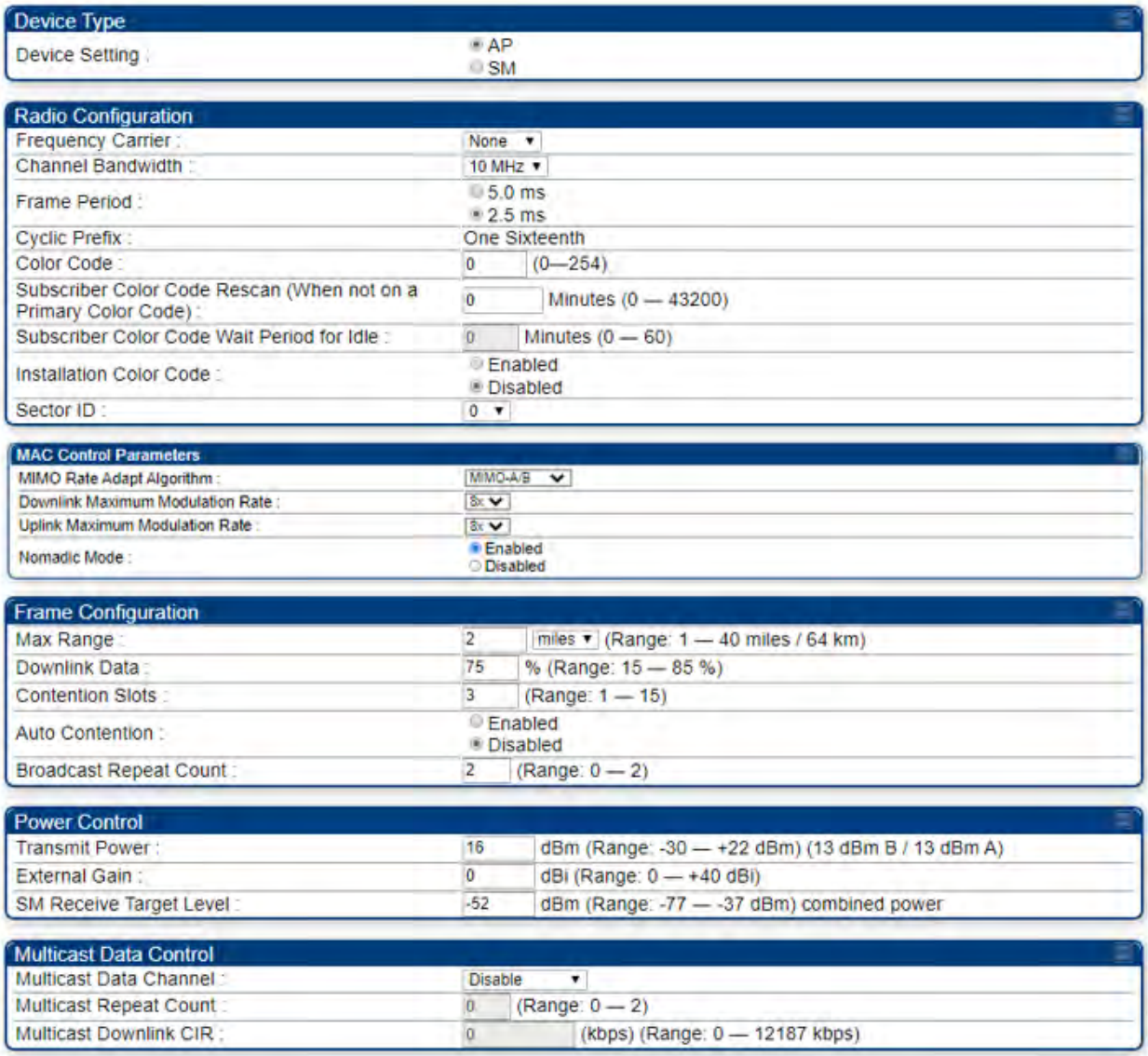
Sync Src.\ SW Rev	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0
Timing Port	OFF	OFF	OFF	OFF
Power Port	OFF	OFF	ON (Mode 1)	OFF

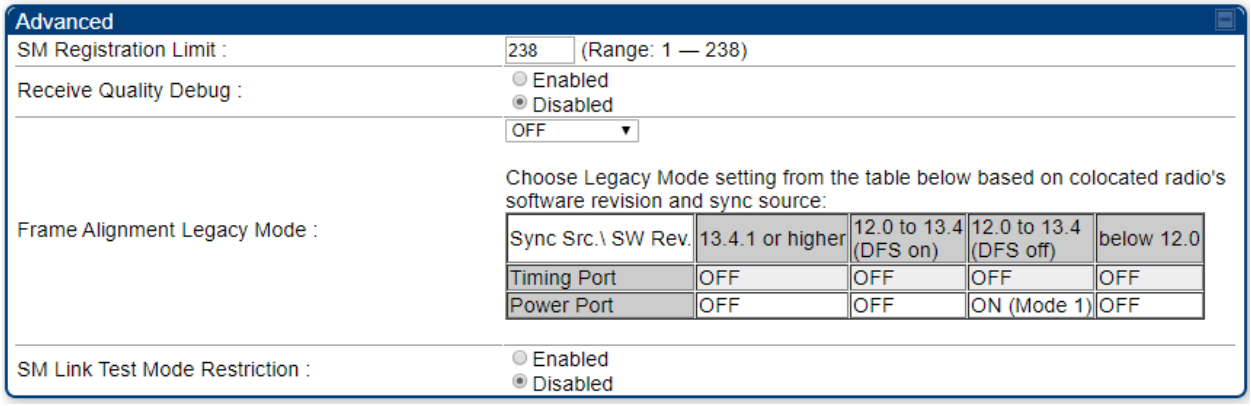
Attribute	Meaning
See PMP/PTP 450i Series – Configuring Radio for all parameters details.	

> **Note**
>
> The PMP 450 AP supports up to 119 Data Channels (instead of 238 Data Channels) when configured for 30 MHz channel bandwidth or 5 ms Frame Period. This limitation is not applicable for PMP 450i/450m Series.

Radio page - PMP 450 AP 2.4 GHz

Table 58: Table 64 PMP 450 AP Radio attributes - 2.4 GHz





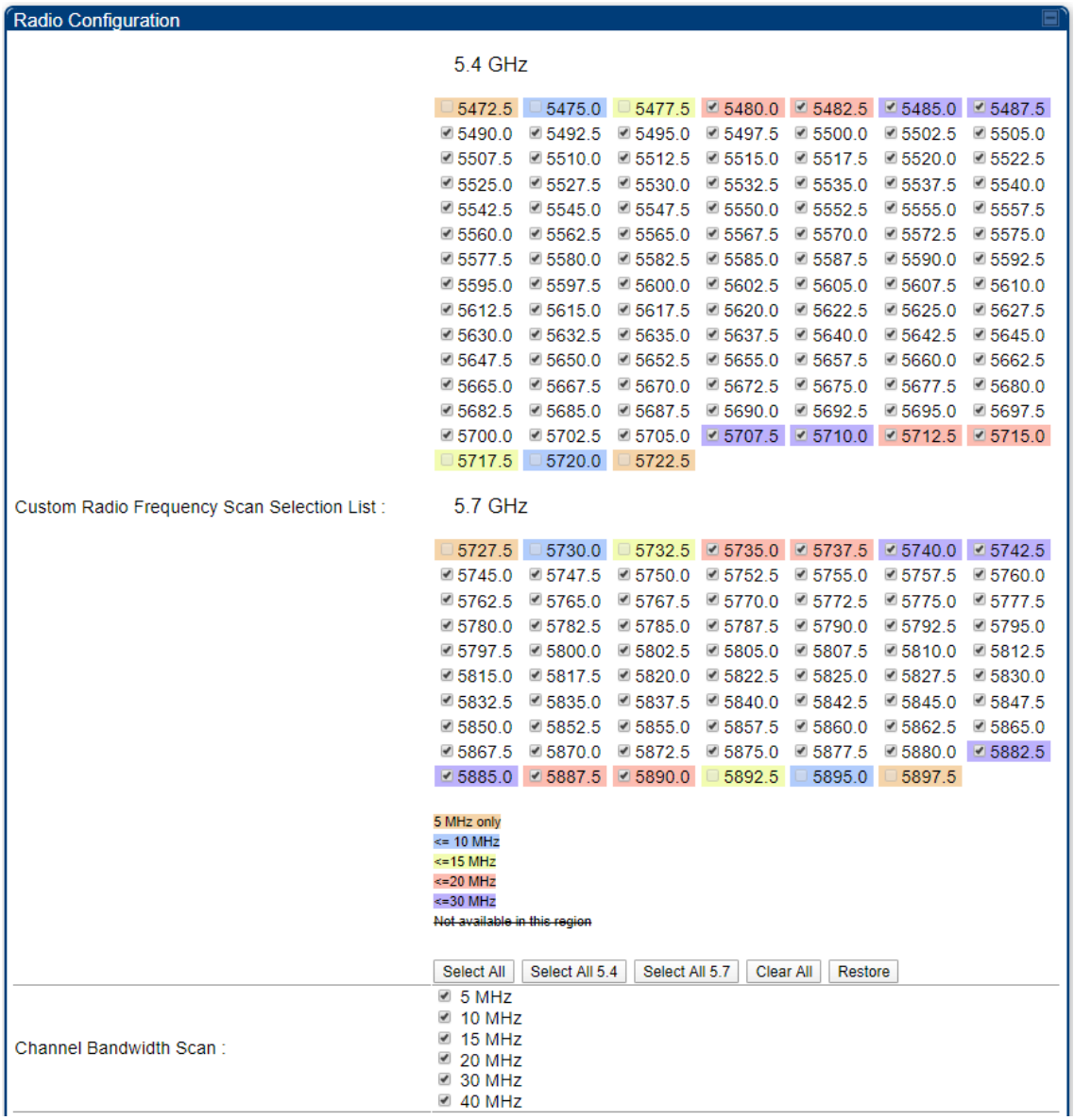
Attribute	Meaning
See PMP/PTP 450i Series – Configuring Radio for all parameters details.	

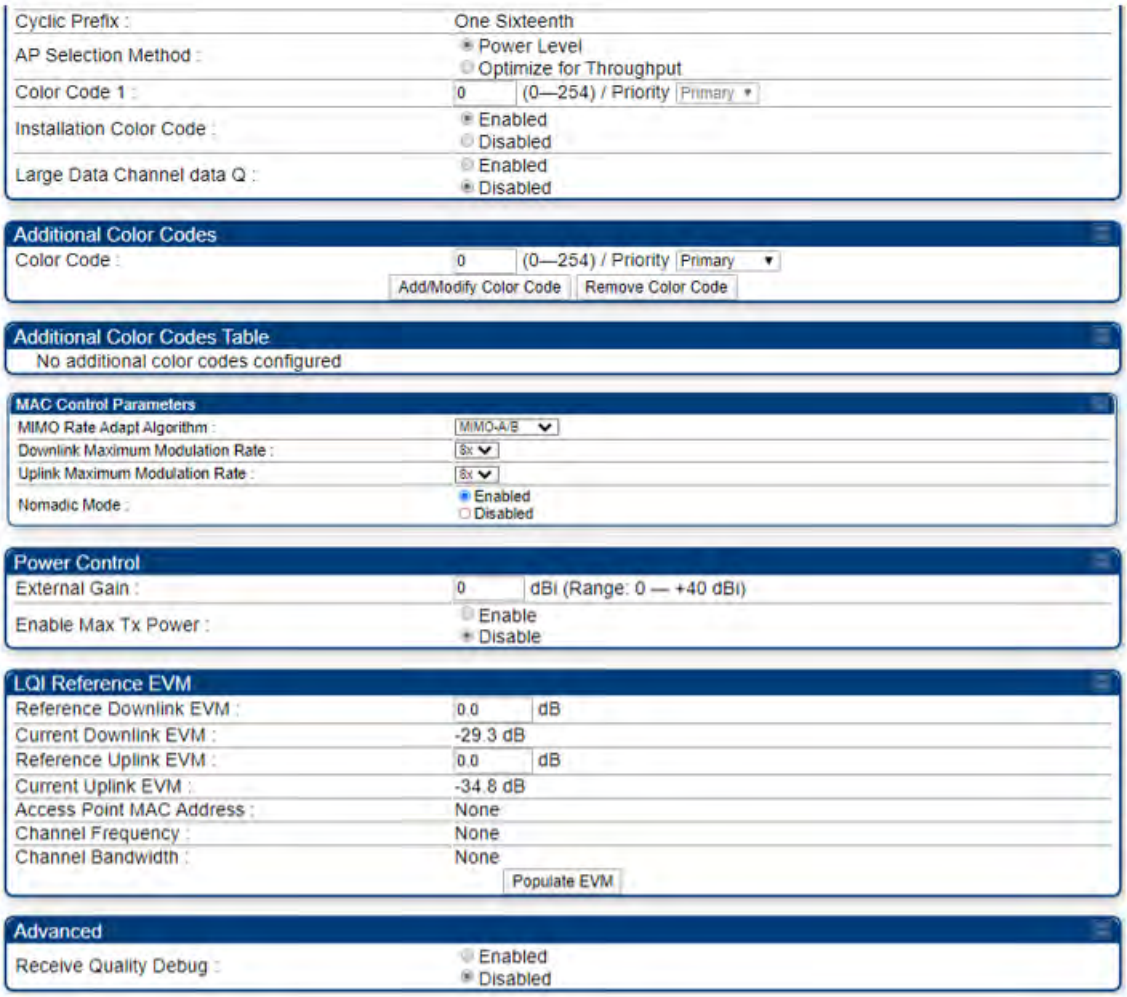
Note

The PMP 450 AP supports up to 119 Data Channels (instead of 238 Data Channels) when configured for 30 MHz channel bandwidth or 5 ms Frame Period. This limitation is not applicable for PMP 450i/450m Series.

Radio page - PMP 450 SM 5 GHz

Table 59: PMP 450 SM Radio attributes – 5 GHz





Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List
See PMP 450i SM Radio attributes – 5 GHz	

Note

The frequencies that a user can select are controlled by the country or a region and the Channel Bandwidth selected. There can be a case where a user adds a custom frequency (from the Custom Frequencies page) and cannot see it in the pull down menu.

Radio page - PMP 450 SM 3.65 GHz

Table 60: PMP 450 SM Radio attributes – 3.65 GHz

Radio Configuration

Custom Radio Frequency Scan Selection List :	2402.5 2405.0 2407.5 2410.0 2412.5 2415.0 2417.5 2420.0 2422.5 2425.0 2427.5 2430.0 2432.5 2435.0 2437.5 2440.0 2442.5 2445.0 2447.5 2450.0 2452.5 2455.0 2457.5 2460.0 2462.5 2465.0 2467.5 2470.0 2472.5 2475.0 2477.5 2480.0 5 MHz only <= 10 MHz <=15 MHz <=20 MHz ~~Not available in this region~~ Select All Clear All Restore
Channel Bandwidth Scan :	5 MHz 10 MHz 15 MHz 20 MHz 30 MHz
Cyclic Prefix :	One Sixteenth
AP Selection Method :	Power Level Optimize for Throughput
Color Code 1 :	0 (0—254) / Priority Primary
Installation Color Code :	Enabled Disabled
Large Data Channel data Q :	Enabled Disabled

Additional Color Codes

Color Code :	0 (0—254) / Priority Primary
	Add/Modify Color Code Remove Color Code

Additional Color Codes Table

No additional color codes configured

MAC Control Parameters

MIMO Rate Adapt Algorithm :	MIMO-A/B
Downlink Maximum Modulation Rate :	8x
Uplink Maximum Modulation Rate :	8x
Nomadic Mode :	Enabled Disabled

Power Control

External Gain :	0 dBi (Range: 0 — +40 dBi)
Enable Max Tx Power :	Enable Disable

LQI Reference EVM

Reference Downlink EVM :	0.0 dB
Current Downlink EVM :	-32.8 dB
Reference Uplink EVM :	0.0 dB
Current Uplink EVM :	-29.1 dB
Access Point MAC Address :	None
Channel Frequency :	None
Channel Bandwidth :	None
	Populate EVM

Advanced

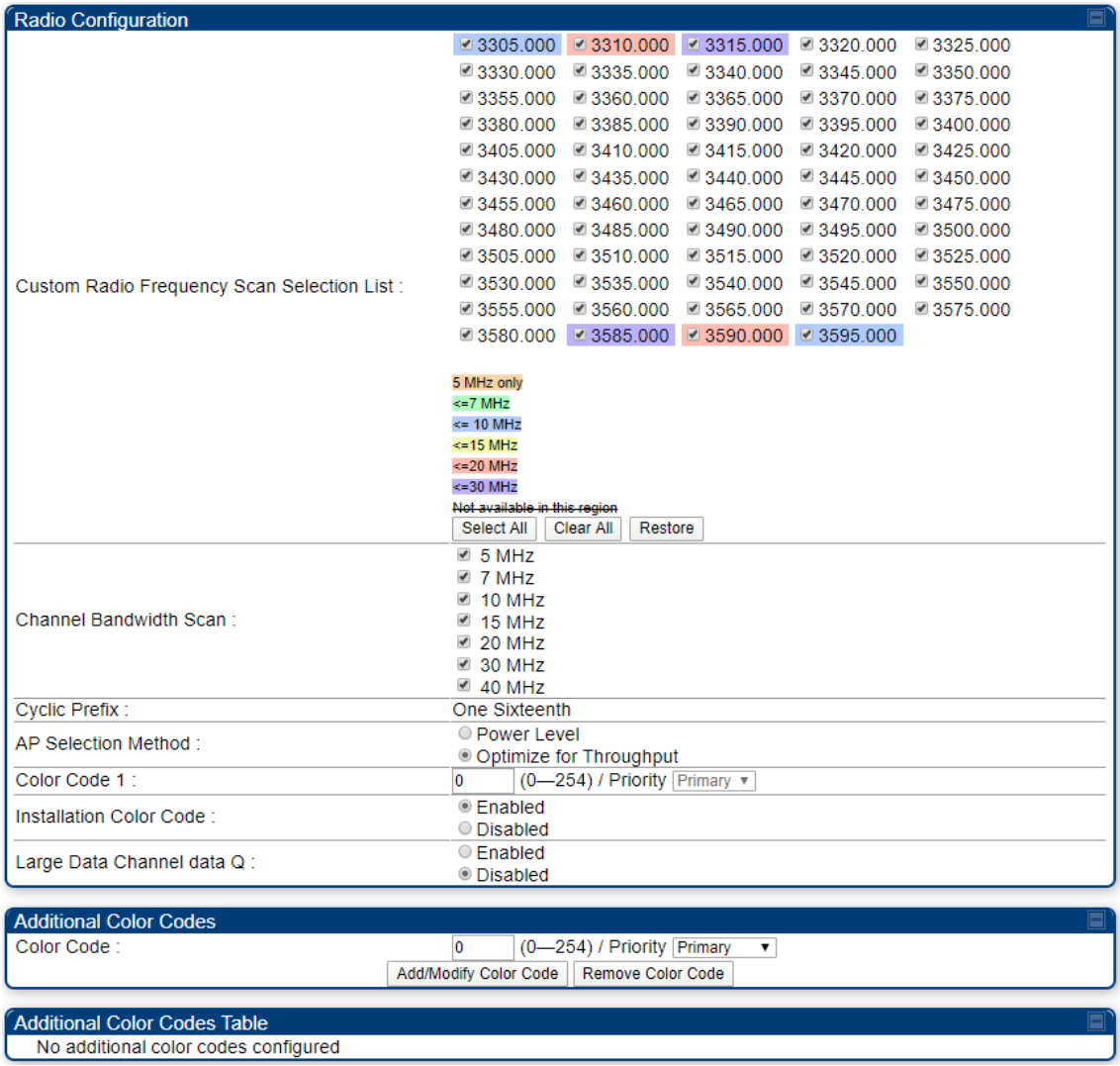
Receive Quality Debug :	Enabled Disabled

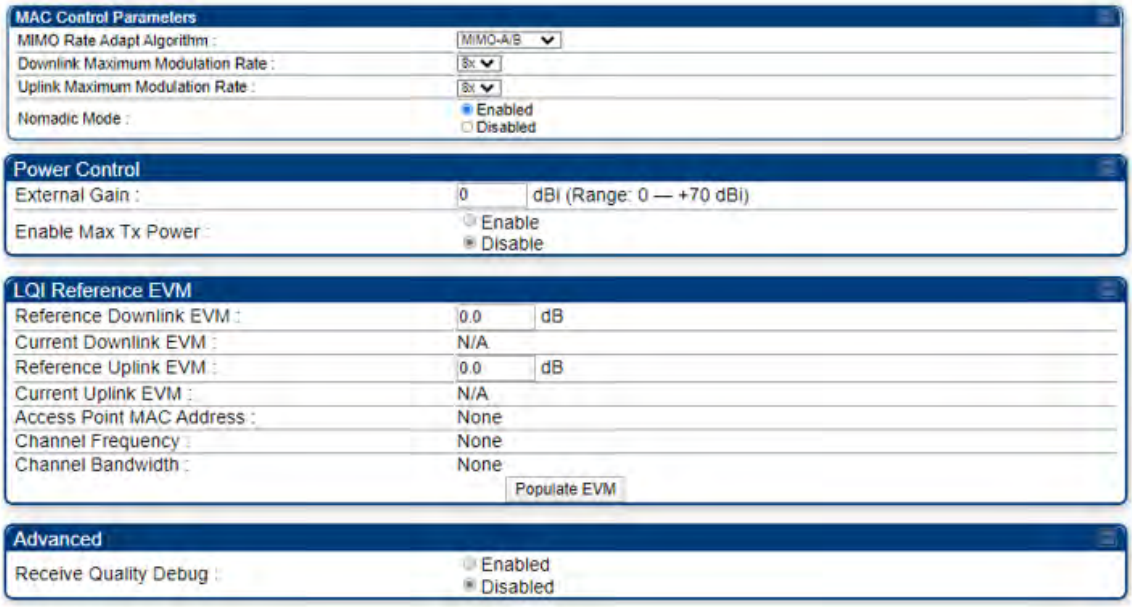
Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List
See PMP 450i SM Radio attributes – 5 GHz	

> **Note**
>
> The frequencies that a user can select are controlled by the country or a region and the Channel Bandwidth selected. There can be a case where a user adds a custom frequency (from the Custom Frequencies page) and cannot see it in the pull down menu.

Radio page - PMP 450 SM 3.5 GHz

Table 61: PMP 450 SM Radio attributes – 3.5 GHz





Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List
See PMP 450i SM Radio attributes – 5 GHz	

Note

The frequencies that a user can select are controlled by the country or a region and the Channel Bandwidth selected. There can be a case where a user adds a custom frequency (from the Custom Frequencies page) and cannot see it in the pull down menu.

Radio page - PMP 450 SM 2.4 GHz

Table 62: PMP 450 SM Radio attributes – 2.4 GHz

Radio Configuration

Custom Radio Frequency Scan Selection List :	2402.5 2405.0 2407.5 2410.0 2412.5 2415.0 2417.5 2420.0 2422.5 2425.0 2427.5 2430.0 2432.5 2435.0 2437.5 2440.0 2442.5 2445.0 2447.5 2450.0 2452.5 2455.0 2457.5 2460.0 2462.5 2465.0 2467.5 2470.0 2472.5 2475.0 2477.5 2480.0 5 MHz only <= 10 MHz <=15 MHz <=20 MHz ~~Not available in this region~~ Select All Clear All Restore
Channel Bandwidth Scan :	5 MHz 10 MHz 15 MHz 20 MHz 30 MHz
Cyclic Prefix :	One Sixteenth
AP Selection Method :	Power Level Optimize for Throughput
Color Code 1 :	0 (0—254) / Priority Primary
Installation Color Code :	Enabled Disabled
Large Data Channel data Q :	Enabled Disabled

Additional Color Codes

Color Code :	0 (0—254) / Priority Primary Add/Modify Color Code Remove Color Code

Additional Color Codes Table

No additional color codes configured

MAC Control Parameters

MIMO Rate Adapt Algorithm :	MIMO-A/B
Downlink Maximum Modulation Rate :	8x
Uplink Maximum Modulation Rate :	8x
Nomadic Mode :	Enabled Disabled

Power Control

External Gain :	0 dBi (Range: 0 — +40 dBi)
Enable Max Tx Power :	Enable Disable

LQI Reference EVM

Reference Downlink EVM :	0.0 dB
Current Downlink EVM :	N/A
Reference Uplink EVM :	0.0 dB
Current Uplink EVM :	N/A
Access Point MAC Address :	None
Channel Frequency :	None
Channel Bandwidth :	None Populate EVM

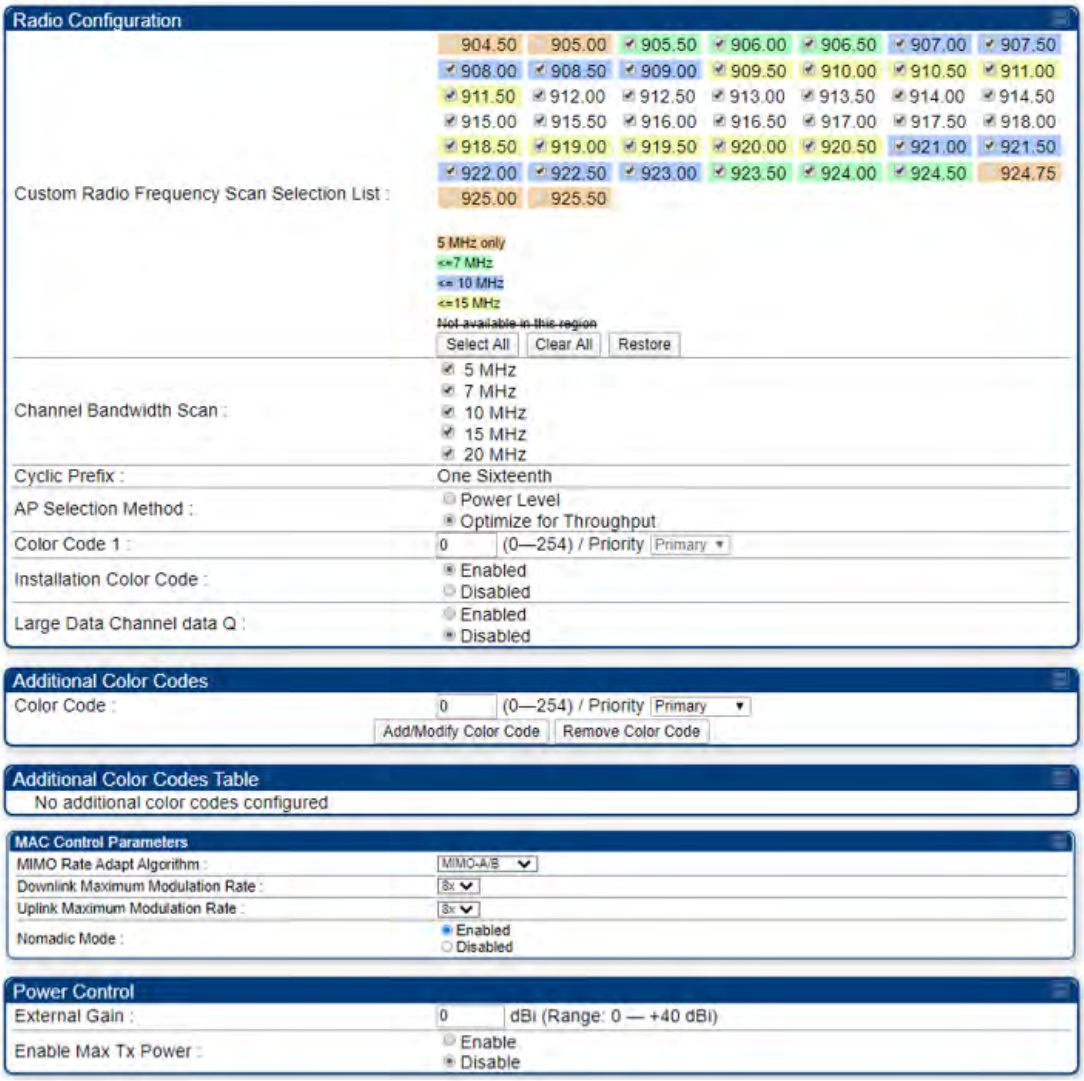
Advanced

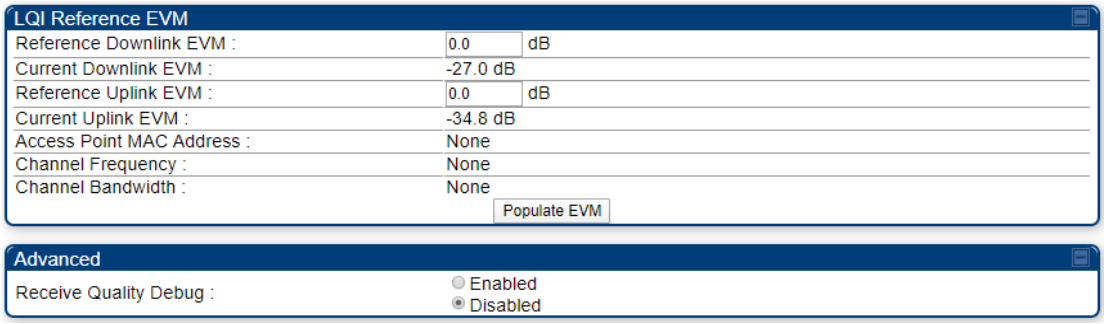
Receive Quality Debug :	Enabled Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List
See PMP 450i SM Radio attributes – 5 GHz	

Radio page - PMP 450 SM 900 MHz

Table 63: PMP 450 SM Radio attributes –900 MHz





Attribute	Meaning
Custom Radio Frequency Scan Selection List	See PMP 450i SM Radio attributes – 5 GHz.
Channel Bandwidth Scan	
Cyclic Prefix	
AP Selection Method	
Color Code 1	
Installation Color Code	
Large Data Channel data Q	
Color Code	
MIMO Rate Adapt Algorithm	
Downlink Maximum Modulation Rate	
Uplink Maximum Modulation Rate	
Nomadic Mode	
External Gain	
Enable Max Tx Power	
Reference Downlink EVM	
Current Downlink EVM	
Reference Uplink EVM	
Current Uplink EVM	
Access Point MAC Address	
Channel Frequency	
Channel Bandwidth	
Receive Quality Debug	

Radio page - PTP 450 BHM 5 GHz

Table 64: PTP 450 BHM Radio attributes –5 GHz

Device Type

Timing Mode :	◉ Timing Master ○ Timing Slave

Radio Configuration

Frequency Band :	5.7 GHz ▾
Frequency Carrier :	None ▾
Channel Bandwidth :	10 MHz ▾
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Cyclic Prefix :	One Sixteenth
Color Code :	0 (0—254)
Sector ID :	0 ▾
Large Data Channel data Q :	○ Enabled ◉ Disabled

MAC Control Parameters

MIMO Rate Adapt Algorithm :	MIMO-A/B ▾
Downlink Maximum Modulation Rate :	8x ▾
Uplink Maximum Modulation Rate :	8x ▾
Minimum Modulation Rate :	1x ▾ Bridging will be disabled if the transmit modulation rate is below this setting

Frame Configuration

Downlink Data :	75 % (Range: 15 — 85 %)

Power Control

Transmit Power :	16 dBm (Range: -30 — +22 dBm) (13 dBm V / 13 dBm H)
External Gain :	0 dBi (Range: 0 — +40 dBi)

Advanced

Receive Quality Debug :	○ Enabled ◉ Disabled
Frame Alignment Legacy Mode :	OFF ▾ Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4 (DFS on)	12.0 to 13.4 (DFS off)	below 12.0
Timing Port	OFF	OFF	OFF	OFF
Power Port	OFF	OFF	ON (Mode 1)	OFF

Attribute	Meaning
Refer PTP 450i BHM Radio page attributes – 5 GHz for all parameters details.	

Radio page - PTP 450 BHS 5 GHz

Table 65: PTP 450 BHS Radio attributes –5 GHz

Device Type

Timing Mode : ○ Timing Master ◉ Timing Slave

Radio Configuration

Custom Radio Frequency Scan Selection List :

5.4 GHz

5472.5	5475.0	5477.5	5480.0	5482.5	5485.0	5487.5
5490.0	5492.5	5495.0	5497.5	5500.0	5502.5	5505.0
5507.5	5510.0	5512.5	5515.0	5517.5	5520.0	5522.5
5525.0	5527.5	5530.0	5532.5	5535.0	5537.5	5540.0
5542.5	5545.0	5547.5	5550.0	5552.5	5555.0	5557.5
5560.0	5562.5	5565.0	5567.5	5570.0	5572.5	5575.0
5577.5	5580.0	5582.5	5585.0	5587.5	5590.0	5592.5
5595.0	5597.5	5600.0	5602.5	5605.0	5607.5	5610.0
5612.5	5615.0	5617.5	5620.0	5622.5	5625.0	5627.5
5630.0	5632.5	5635.0	5637.5	5640.0	5642.5	5645.0
5647.5	5650.0	5652.5	5655.0	5657.5	5660.0	5662.5
5665.0	5667.5	5670.0	5672.5	5675.0	5677.5	5680.0
5682.5	5685.0	5687.5	5690.0	5692.5	5695.0	5697.5
5700.0	5702.5	5705.0	5707.5	5710.0	5712.5	5715.0
5717.5	5720.0	5722.5				

5.7 GHz

5727.5	5730.0	5732.5	5735.0	5737.5	5740.0	5742.5
5745.0	5747.5	5750.0	5752.5	5755.0	5757.5	5760.0
5762.5	5765.0	5767.5	5770.0	5772.5	5775.0	5777.5
5780.0	5782.5	5785.0	5787.5	5790.0	5792.5	5795.0
5797.5	5800.0	5802.5	5805.0	5807.5	5810.0	5812.5
5815.0	5817.5	5820.0	5822.5	5825.0	5827.5	5830.0
5832.5	5835.0	5837.5	5840.0	5842.5	5845.0	5847.5
5850.0	5852.5	5855.0	5857.5	5860.0	5862.5	5865.0
5867.5	5870.0	5872.5	5875.0	5877.5	5880.0	5882.5
5885.0	5887.5	5890.0	5892.5	5895.0	5897.5	

5 MHz only
<= 10 MHz
<=15 MHz
<=20 MHz
<=30 MHz
~~Not available in this region~~

Select All | Select All 5.4 | Select All 5.7 | Clear All | Restore

Channel Bandwidth Scan :	☑ 5 MHz ☑ 10 MHz ☑ 15 MHz ☑ 20 MHz ☑ 30 MHz ☑ 40 MHz
Cyclic Prefix :	One Sixteenth
Color Code :	0 (0—254)
Large Data Channel data Q :	○ Enabled ◉ Disabled

MAC Control Parameters

MIMO Rate Adapt Algorithm :	MIMO-A/B ▾
Downlink Maximum Modulation Rate :	8x ▾
Uplink Maximum Modulation Rate :	8x ▾
Minimum Modulation Rate :	1x ▾ Bridging will be disabled if the transmit modulation rate is below this setting

Power Control

Transmit Power :	16 dBm (Range: -30 — +22 dBm) (13 dBm V / 13 dBm H)
External Gain :	0 dBi (Range: 0 — +40 dBi)

LQI Reference EVM

Reference Downlink EVM :	0.0 dB
Current Downlink EVM :	-31.4 dB
Reference Uplink EVM :	0.0 dB
Current Uplink EVM :	-30.2 dB
Access Point MAC Address :	None
Channel Frequency :	None
Channel Bandwidth :	None
	Populate EVM

Advanced

Receive Quality Debug :	○ Enabled ◉ Disabled

Attribute	Meaning
Refer PTP 450i BHS Radio attributes – 5 GHz for all parameters details.	

Note

The PMP 450 AP supports up to 119 Data Channels (instead of 238 Data Channels) when configured for 30 MHz channel bandwidth or 5 ms Frame Period. This limitation is not applicable for PMP 450i/450m Series.

Radio Frequency Scan Selection List

The SM or BHS scans complete spectrum as per Full Spectrum Band Scan feature. SMs or BHS first boot into the smallest selected channel bandwidth (10 MHz, if selected) and scan all selected frequencies across both the 5.4 GHz and 5.7 GHz frequency bands.

After this scan, if a wider channel bandwidth is selected (20 MHz), the SM/BHS automatically changes to 20 MHz channel bandwidth and then scans for APs/BHSs. After the SM/BHS finishes this final scan it will evaluate the best AP/BHM with which to register. If required for registration, the SM/BHS changes its channel bandwidth back to 10 MHz to match the best AP/BHM.

The SM/BHS will attempt to connect to an AP/BHM based on power level (which affects the modulation state), channel bandwidth (which affects throughput) and number of SM/BHS registrations to the AP/BHM (which affects system contention performance).

If it is desired to prioritize a certain AP/BHM over other available APs/BHMs, operators may use the Color Code Priority feature on the SM/BHS. Utilization of the Color Code feature on the AP/BHM is recommended to further constrain the AP selection.

If the SM does not find any suitable APs/BHMs for registration after scanning all channel bandwidths, the SM restarts the scanning process beginning with the smallest configured channel bandwidth.

Selecting multiple frequencies and multiple channel bandwidths impacts the SM/BHS scanning time. The biggest consumption of time is in the changing of the SM/BHS channel bandwidth setting.

The worst case scanning time is approximately two minutes after boot up (SM/BHS with all frequencies and channel bandwidths selected and registering to an AP/BHM at 10 MHz). If only one channel bandwidth is selected the time to scan all the available frequencies and register to an AP/BHM is approximately one minute after boot up.

Other scanning features such as Color Code, Installation Color Code, and RADIUS authentication are unaffected by the Full Band Scan feature.

Dedicated Multicast Data Channel

A Multicast Data Channel allows to configure multicast packets to be transmitted over a dedicated channel at a configurable rate of 2X, 3X, 4X, 5X or 6X. This feature is available only for the PMP 450 and PMP 450i and is not backward compatible with PMP 430 series of radios.

To configure Multicast Data Channel, the AP must have this enabled. This can be enabled in the “Multicast Data Control” section (under **Configuration -> Radio page**). The default value is “Disable”. If set to the default value, all multicast packets are transmitted over the Broadcast Data Channel data path. To enable, select the data rate that is desired for the Multicast Data Channel Data Rate parameter and click Save Changes button. The radio requires no reboot after any changes to this parameter.

The Multicast Data Channel allows three different parameters to be configured on the AP. These can be changed on the fly and are saved on the flash memory.

Note

If the Multicast Data Channel Data Rate is set to a modulation that the radio is not currently capable of or operates in non-permitted channel conditions, multicast data is sent but not received.

Ex: If Multicast Data Channel Data Rate is set to 6x and the channel conditions only permit 4x mode of operation, then multicast data is sent at 6x modulation but the SM will not receive the data.

Note

- Actual Multicast CIR honored by the AP = Configured Multicast CIR/ (Multicast Repeat Count + 1).
- Increasing the Multicast data rate has no impact on the Unicast data rate.
- For multicast and unicast traffic mix scenario examples, see .

Table 66: Example for mix of multicast and unicast traffic scenarios

Repeat Count	Multicast Data Rate (Mbps)	Unicast Data Rate (Mbps)	Aggregate DL Data Rate (Mbps)
0	10	40	50
1	5	40	45
2	3.33	40	43.33

The statistics have been added to the Data Channel page (under **Statistics > Data Channel**). The table displays the multicast row on the PMP 450 Platform Family AP. The SM displays the multicast row if it is a PMP 450 Platform Family.

Figure 36: *Data Channel statistics*

Data Channel Statistics

Subscriber	LUID	Channel Priority	Inbound Statistics					Outbound Statistics					Queue Overflow	High Priority Queue
			octets	ucast pkts	nucast pkts	discards	errors	octets	ucast pkts	nucast pkts	discards	errors		
SM1-10.110.233.10	002	Low	2331271	12968	44	0	0	9528653	13684	0	0	0	0	3530
SM2-10.110.233.11	003	Low	673675	3957	83	0	0	274635	2150	0	0	0	0	953
SM3-10.110.233.12	004	Low	487028	3638	81	0	0	233167	1922	0	0	0	0	791
Retro-10.110.233.13	005	Low	2530	4	1	0	0	171136	1328	0	0	0	0	172
Retro-10.110.233.13	005	Medium	0	0	0	0	0	0	0	0	0	0	0	0
Retro-10.110.233.13	005	High	0	0	0	0	0	0	0	0	0	0	0	0
Retro-10.110.233.13	005	Ultra High	321880	2876	81	0	0	66133	629	0	0	0	0	629
Multicast	252	NA	NA	NA	NA	NA	NA	0	0	0	0	0	NA	NA
Broadcast	255	NA	NA	NA	NA	NA	NA	1729190	0	11383	0	0	NA	NA

The AP and SM display Transmit and Receive Multicast Data Count (under the Statistics > Scheduler page), as shown in below figure.

Figure 37: *Multicast scheduler statistics*

Radio Statistics

Transmit Unicast Data Count :	20778
Transmit Broadcast Data Count :	13
Transmit Multicast Data Count :	0
Receive Unicast Data Count :	20828
Receive Broadcast Data Count :	206042
Receive Multicast Data Count :	0
Transmit Control Count :	160
Receive Control Count :	39
In Sync Count :	62
Out of Sync Count :	0
Overrun Count :	0
Underrun Count :	0
Receive Corrupt Data Count :	0
Receive Corrupt Control Data Count :	0
Receive Bad Broadcast Control Count :	0
Unsupported Feature Beacon Received :	0
Unknown Feature Beacon Received :	0
Old Version Beacon Received :	0
Wrong Frequency Beacon Received :	0
Non Lite Beacon Received :	0
Bad In Sync ID Received :	0
Rcv LT Start :	0
Rcv LT Start HS :	0
Rcv LT Result :	0
Xmt LT Result :	0
Frame Too Big :	0
Bad Acknowledgment :	0

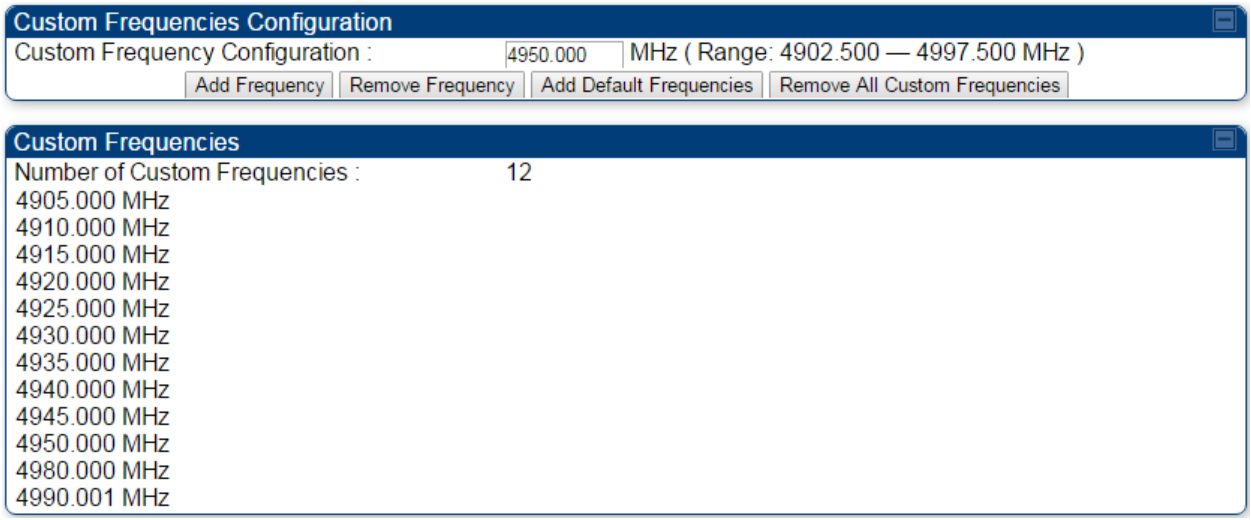
Custom Frequencies page

In addition to the Radio tab, AP/SM/BH has another tab called Custom Frequencies as shown in 450 Platform Family AP/SM/BH Custom Frequencies page – 5 GHz.

The custom frequency tab allows to configure custom frequency at 1 kHz raster. It means that the custom frequencies can be at granularity of 1 kHz e.g. 4910.123 MHz, 4922.333 MHz, 4933.421 MHz etc.

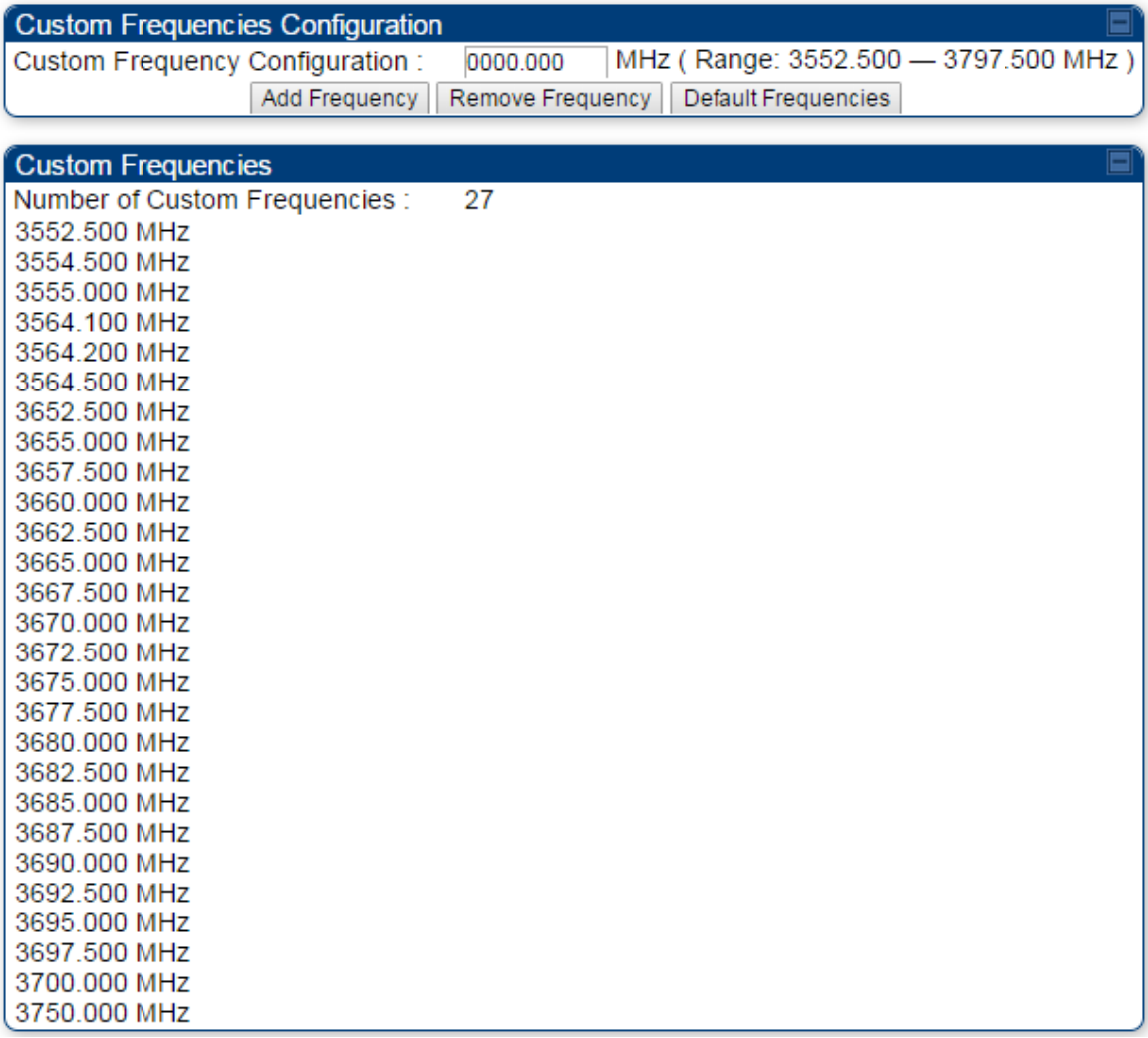
> Note
>
> Ensure that a customer frequency exists before using SNMP to set the radio to a Custom Frequency.

Table 67: 450 Platform Family AP/SM/BH Custom Frequencies page – 5 GHz



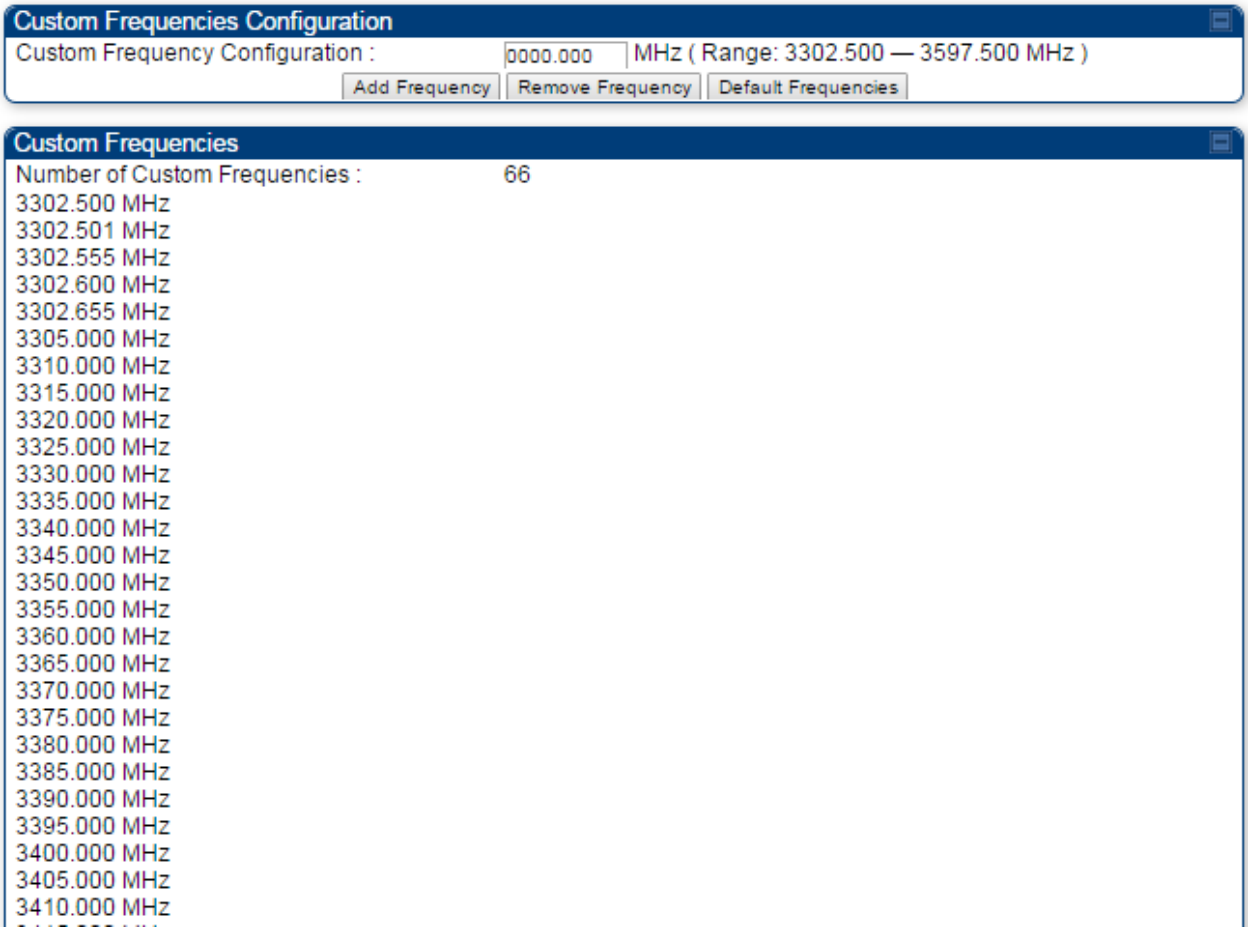
Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 kHz can be added from the available range by keying in the frequency and then clicking the Add Frequency button. Click Remove Frequency button to delete a specific frequency keyed in the text box. Click Default Frequencies button to add a pre-defined list of frequencies that can be used in this band. This list can be reduced or increased by manually removing or adding other custom frequencies.
Custom Frequencies	Displays the complete list of user configured custom frequencies.

Table 68: PMP/PTP 450 SM/BH Custom Frequencies page – 3.65 GHz



Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 kHz can be added from the available range by keying in the frequency and then clicking the Add Frequency button. Click Remove Frequency button to delete a specific frequency keyed in the text box. Click Default Frequencies button to add a pre-defined list of frequencies that can be used in this band. This list can be reduced or increased by manually removing or adding other custom frequencies.
Custom Frequencies	Displays the complete list of user configured custom frequencies.

Table 69: PMP/PTP 450 SM/BH Custom Frequencies page – 3.5 GHz



Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 kHz can be added from the available range by keying in the frequency and then clicking the Add Frequency button. Click Remove Frequency button to delete a specific frequency keyed in the text box. Click Default Frequencies button to add a pre-defined list of frequencies that can be used in this band. This list can be reduced or increased by manually removing or adding other custom frequencies.

DFS for 5 GHz Radios

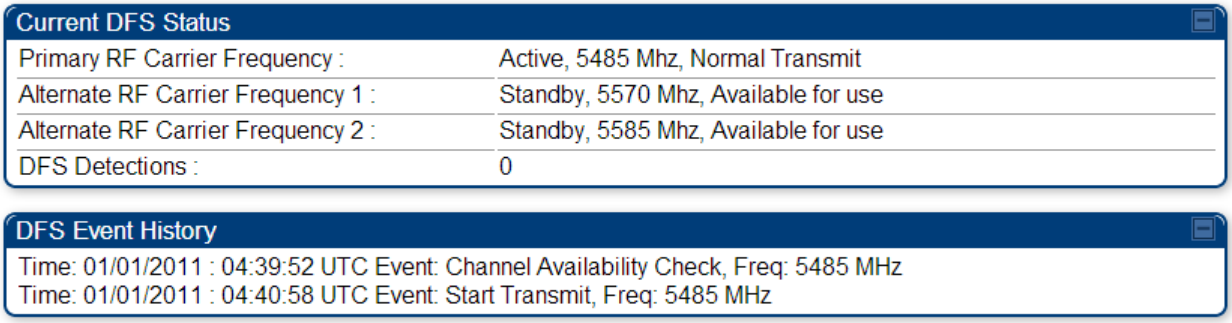
Dynamic Frequency Selection (DFS) is a requirement in several countries and regions for 5 GHz unlicensed systems to detect radar systems and avoid co-channel operation. DFS and other regulatory requirements drive the settings for the following parameters, as discussed in this section:

- Country Code
- Primary Frequency

- Alternate 1 and Alternate 2 Frequencies
- External Antenna Gain

On the AP, the Home > DFS Status page shows current DFS status of all three frequencies and a DFS log of past DFS events.

Figure 38: *AP DFS Status*



Current DFS Status	
Primary RF Carrier Frequency :	Active, 5485 Mhz, Normal Transmit
Alternate RF Carrier Frequency 1 :	Standby, 5570 Mhz, Available for use
Alternate RF Carrier Frequency 2 :	Standby, 5585 Mhz, Available for use
DFS Detections :	0

DFS Event History

Time: 01/01/2011 : 04:39:52 UTC Event: Channel Availability Check, Freq: 5485 MHz
Time: 01/01/2011 : 04:40:58 UTC Event: Start Transmit, Freq: 5485 MHz

DFS operation

The ODUs use region-specific DFS based on the Country Code selected on the module's Configuration, General page. By directing installers and technicians to set the Country Code correctly, the operator gains confidence the module is operating according to national or regional regulations without having to deal with the details for each region.

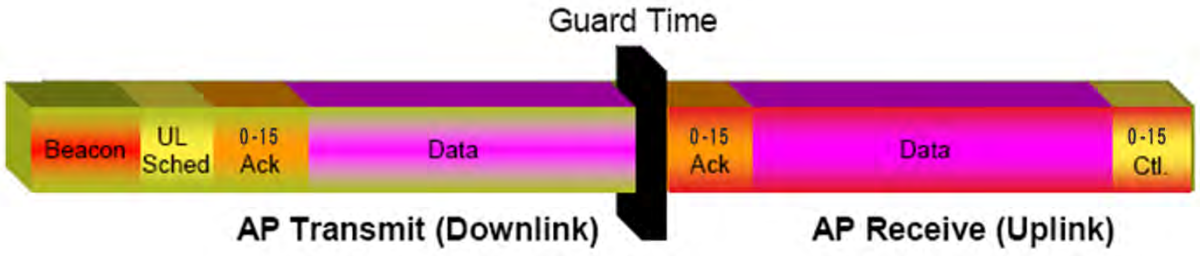
The details of DFS operation for each Country Code, including whether DFS is active on the AP, SM, and which DFS regulations apply is shown in Country & Bands DFS setting.

Contention slots

Contention slots are symbols at the end of the uplink subframe that are reserved for random access (network entry and bandwidth requests) and cannot be used for data transmission. These symbols form the contention space.

The frame is 2.5 ms or 5 ms long, and it is divided into a downlink subframe (data transmitted from the AP to the SM) and an uplink subframe (data transmitted from the SM to the AP).

Figure 39: *Frame structure*



The symbols in the uplink subframe can be scheduled or unscheduled. All scheduled symbols come before all unscheduled symbols. The number of scheduled and unscheduled symbols changes frame by frame depending on the amount of uplink requests received by the AP.

The contention slots number is selected by the operator and indicates the number of symbols that are reserved in the unscheduled portion of the uplink. The total number of unscheduled symbols in each frame is the sum of the contention slots and any additional symbol that was not used in uplink data transmission. This means that the unscheduled portion of the uplink can be as small as the number of contention slots, or as big as the whole uplink. This allows SMs in sectors with a small number of contention slots configured to still successfully transmit bandwidth requests using unused data slots.

Random access

When an SM needs to send an unscheduled message (for network entry or a bandwidth request), it randomly selects one symbol out of the unscheduled portion of the uplink subframe and uses that symbol for transmission. The higher the number of unscheduled symbols, the lower the probability two or more SMs will select the same symbol for transmission and their messages will collide. When two messages collide at the AP receiver, most likely neither will be decoded correctly, and both SMs need to start the random-access process one more time. If this happens frequently, the latency of the system increases.

A higher number of contention slots give higher probability that an SM's bandwidth request will be correctly received when the system is heavily loaded, but with the tradeoff that sector capacity is reduced, so there will be less capacity to handle the request. The sector capacity reduction is about 200 kbps for each contention slot configured in a 20 MHz channel at QPSK modulation, for 2.5 ms frame sizes. The reduction in sector capacity is proportionally higher at MIMO modulations, as shown in the following table.

Table 70: Throughput penalty per modulation

Modulation mode	Throughput penalty for each additional contention slot	
	2.5 ms frame	5 ms frame
QPSK (1X)	204 kbps	102 kbps
QPSK MIMO (2X)	409 kbps	204 kbps
16-QAM MIMO (4X)	819 kbps	409 kbps
64-QAM MIMO (6X)	1.22 Mbps	614 kbps
256-QAM MIMO (8X)	1.63 Mbps	819 kbps

Throughput penalty per modulation shows that the throughput penalty for each additional contention slot increases with modulation mode. The reason is that at higher modulation modes more fragments can be transmitted in a symbol. If additional symbols are reserved for random access, the number of fragments that cannot be sent in these symbols is higher at higher modulations, and therefore the throughput penalty is higher. However, the penalty expressed as a percentage of the throughput is the same for each modulation mode. For example, if a frame has 80 total symbols, each additional symbol reserved for random access reduces the sector throughput by 1.25%, regardless of the modulation mode.

Selection of contention slots parameter

The number of contention slots has to be selected according to the specific deployment parameters in each sector. If the number of contention slots is too small, then latency increases in high traffic periods. If the number of contention slots is too high, then the maximum capacity is unnecessarily reduced.

The two main contributing factors to the selection of the number of contention slots are the number of SMs in a sector, and the type of traffic in the sector.

The System Release 16.1 introduces Auto Contention Slots that usually eliminates the need to configure optimal number of contention slots. When this feature is enabled, AP dynamically adjusts the number of contention slots resulting in improved uplink performance.

However, if using Nomadic Mode, in some cases it might be desirable to disable the Auto contention feature to increase the number of contention slots in use. The Nomadic Mode feature is introduced with System Release 21.0 and is supported for all AP/BHM types except 450m.

Note

Auto Contention Slots feature is not currently supported on PMP 450m AP.

Note

Contention Slots configuration parameter is used to determine the number of Downlink/Uplink+Contention slots in a Frame. Therefore, there is no need to change Contention Slots parameter, unless AP's Tx/Rx configuration is changed which should be consistent for the entire site for co-location.

Number of SMs in a sector

If the number of SMs in a sector is large, it is recommended to increase the number of contention slots, in order to reduce the probability of two or more requests colliding. The suggested contention slot settings as a function of the number of active data channels in the sector, and the frame size, are shown below:

Table 71: Contention slot settings

Number of SMs	Controls Slots recommendation 2.5 ms	Control Slots Recommendation 5.0 ms
1 to 10	3	3
11 to 50	4	8
51 to 150	6	12
151 and above	8	15

Note

The above table has been updated with the System Release 22.0 documentation release to suggest the higher number of contention slots for 5.0 ms frame configurations. This documentation revision is not because of any software changes, but due to a more careful analysis of recent field and test data.

Type of traffic in a sector

Besides the number of SMs, the other main factor in contention slots selection is the type of traffic. If the sector experiences a lot of uplink traffic composed of small packets, for example in a sector that serves several VoIP streams, the average number of bandwidth requests transmitted by each SM is high. Another scenario with constant uplink traffic is video surveillance, which also generate a large number of uplink bandwidth requests.

In these cases, the probability of two or more SMs transmitting a request in the same symbol is high. When this happens, the latency of the system increases, and it is recommended to increase the number of contention slots from the number in Contention slot settings. If an AP is experiencing latency or SM-

servicing issues, increasing the number of contention slots may increase system performance, depending on traffic mix over time.

Recommendation on Contention Slots number selection

1. Calculate the number of active SMs in the sector.
2. Evaluate the traffic mix that is expected in the sector, more specifically the expected percentage of real-time traffic (ex. VoIP, gaming, video conferencing, and video surveillance).
3. If the expected amount of real-time traffic is small, select the number of contention slots according to Contention slot settings.
4. If the expected amount of real-time traffic is large, select a number of contention slots larger than the number in Contention slot settings.
5. Monitor latency in your system. If the percentage of real-time traffic increases and the sector experiences increasing latency and SM-servicing issues, increase the number of contention slots from the current setting.
   This is the reason why the maximum number of contention slots is 15, even if Table 2 shows 8 contention slots for more than 150 data channels. If the number of data channels is more than 150 and a significant portion of the traffic is real-time, the frequency with which bandwidth request messages are transmitted requires a higher number of contention slots, potentially as high as 15. A sector with a high number of video surveillance cameras would also require a larger number of contention slots to reduce the probability of collision between requests.
6. Monitor the percentage of BW requests successfully received and the UL frame utilization: if the frame utilization is high (close to 100%), then it is not recommended to change the number of contention slots, even if the percentage success rate of BW requests is low. However, if the percentage success rate of BW requests is low and the frame utilization is also low, then increasing the number of contention slots is recommended.

Cluster of APs

It is recommended to use care when changing the contention slots configuration of only some APs in a cluster, because changes affect the effective downlink/uplink ratio and can cause co-location issues.
In a typical cluster, each AP should be configured with the same number of contention slots to assure proper timing in the send and receive cycles. The number of contention slots is used by the frame calculator to define the downlink and uplink times, which should not overlap from one AP to another. However, if the traffic experienced by two APs in the same cluster is different (for example, one supports significantly more VoIP traffic), the number of contention slots selected for each AP may not be the same. For APs in a cluster of mismatched contention slots setting, it is recommended to use the frame calculator to verify that send and receive times do not overlap (see the Frame calculator for co-location).

> Note
>
> Change contention slot configuration in an operating, stable system cautiously and with a back-out plan. After changing a contention slot configuration, monitor the system closely for problems as well as improvements in system performance.

Frame calculator for co-location

The frame calculator is a tool available for the PMP 450 series systems, that calculates the length of the transmit and receive times, together with the number of downlink and uplink symbols, for a given set of

configuration parameters. The frame calculator can be used to verify that co-location of APs using different contention slots settings does not create overlapping transmit and receive times.

Basic rules

For co-location of AP1 and AP2, we want to ensure that AP1 stops transmitting before AP2 starts receiving, and that AP2 stops transmitting before AP1 starts receiving.

These are the rules that have to be satisfied for a correct co-location of the two APs:

- AP1 Receive Start > AP2 Transmit End
- AP2 Receive Start > AP1 Transmit End

Steps for co-location

Let us assume that in a cluster of multiple APs with all the same settings, one AP's settings are modified with a different number of contention slots.

1. Obtain all configuration settings for the APs that do not change parameters (duty cycle, contention slots, max distance)
2. Input these configuration parameters into the OFDM Frame Calculator tool found under "Tools".
3. Click "Calculate"
4. Note the following values from the results:
    - AP Antenna Receive Start: _____
    - AP Antenna Transmit End: _____
5. Access the AP that needs to have a different contention slots setting and use the frame calculator tool found under "Tools"
6. Input the configuration parameters for this AP (same duty cycle and max distance as the other APs, different contention slots)
7. Click "Calculate"
8. Note the following values from the results:
    - AP Antenna Receive Start: _____
    - AP Antenna Transmit End: _____
9. Check that the two following equations are both true:
    - AP2 Receive Start > AP1 Transmit End
    - AP1 Receive Start > AP2 Transmit End
10. If one or both equations are not true, adjust the duty cycle until they become true (or the max distance if possible).

Example

Let us assume that all APs in a cluster have the same Max range settings, a 2.5 ms frame length and a 20 MHz channel BW, but the operator has fine-tuned the DL duty % per AP as follows:

AP1:

Max range: 2 miles

Contention slots: 3

DL duty cycle = 75%

AP2:

Max range: 2 miles

Contention slots: 3

DL duty cycle = 80%

Running the frame calculator as explained in the Steps for co-location, the AP1 Antenna Transmit End and Antenna Receive start times are:

- AP1 Antenna Transmit End = 1.6440 ms
- AP1 Antenna Receive Start = 1.7972 ms

AP2's Antenna Transmit End and Antenna Receive start times are:

- AP2 Antenna Transmit End = 1.7411 ms
- AP2 Antenna Receive Start = 1.8943 ms

The settings in AP1 in the cluster are now modified by changing the number of contention slots from 3 to 7, for example because this sector is constantly experiencing a higher volume of VoIP traffic.

Running the frame calculator again, the new AP1 Antenna Transmit End and Antenna Receive start times are:

- AP1 Antenna Transmit End = 1.5711 ms
- AP1 Antenna Receive Start = 1.7243 ms

The two equations above have to be checked for correct co-location:

- AP1 Antenna Receive Start > AP2 Antenna Transmit End à 1.7243 ms >1.7411 ms NOT OK
- AP2 Antenna Receive Start > AP1 Antenna Transmit End à 1.8943 ms >1.5711ms OK

The first of the two equations are not true. AP2 is still transmitting when AP1 has already started receiving. This creates interference at the AP1 receiver.

To avoid this interference scenario, the duty cycle of AP2 can be further adjusted slightly. For example, changing the duty cycle of AP2 from 80% to 79% changes the AP2 Antenna Transmit End and Antenna Receive start times as follows:

- AP2 Antenna Transmit End = 1.7168 ms
- AP2 Antenna Receive Start = 1.8700 ms

The two equations have to be checked again for co-location:

- AP1 Antenna Receive Start > AP2 Transmit End à 1.7243 ms >1.7168 ms OK
- AP2 Receive Start > AP1 Transmit End à 1.8700 ms >1.5711 ms OK

Now both equations are true and the APs can be co-located.

Cambium co-location tool

As an alternative to using the frame calculator on the AP GUI, cambium provides a co-location tool for these calculations. This tool is a free download available on the Cambium website:

https://support.cambiumnetworks.com/files/colocationtool/#r2

PMP/PTP 450/450i/450m CO-LOCATION TOOL AND THROUGHPUT CALCULATOR

Release 15.1.1

Device 1 Configuration	
Mode	PMP
Channel Bandwidth (MHz)	20
Max Range (mi)	2
Dowlink Data	75%
Contention slots	3
Frame Period (ms)	2.5

Device 1 Timing (ms)	
DL end	1.644
UL start	1.797
DL/UL symbols	61/20
DL/UL/Total Throughput (Mbps)	98.3/31.1/129.4

Device 2 Configuration	
Mode	PMP
Channel Bandwidth (MHz)	20
Max Range (mi)	2
Downlink Data	80%
Contention Slots	3
Frame Period (ms)	2.5

Device 2 Timing (ms)	
DL end	1.741
UL start	1.894
DL/UL symbols	65/16
DL/UL/Total Throughput (Mbps)	104.9/24.6/129.5

CHECKS					
Device 1 DL end	1.644	<	Device 2 UL start	1.894	OK
Device 2 DL end	1.741	<	Device 1 UL start	1.797	OK

MIMO-A mode of operation

450 Platform Family supports MIMO-B mode using the following modulation levels: QPSK, 8-QAM, 16-QAM, 32-QAM, 64-QAM, 128-QAM and 256-QAM. System Release 13.2 introduces MIMO-A mode of operation using the same modulation levels as the MIMO-B mode. With MIMO-B, the radio sends different streams of data over the two antennas whereas with MIMO-A, the radio uses a scheme that tries to optimize coverage by transmitting the same data over both antennas. This redundancy improves the signal to noise ratio at the receiver making it more robust, at the cost of throughput.

In addition to introducing MIMO-A modes, improvements have been made to the existing rate adapt algorithm to switch between MIMO-A and MIMO-B seamlessly without any intervention or added configuration by the operator. The various modulation levels used by the 450 Platform Family are shown in below table.

Table 72: 450 Platform Family Modulation levels

Rate	MIMO-B	MIMO-A
QPSK	2X MIMO-B	1X MIMO-A
8-QAM	3X MIMO-B	
16-QAM	4X MIMO-B	2X MIMO-A
32-QAM	5XMIMO-B	

Rate	MIMO-B	MIMO-A
64-QAM	6X MIMO-B	3X MIMO-A
128-QAM	7X MIMO-B	
256-QAM	8X MIMO-B	4X MIMO-A

System Performance

For System Performance details of all the 450 Platform Family ODUs, refer to the tools listed below:

Link Capacity Planner for PMP/PTP 450 and 450i:

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

LINKPlanner for PMP/PTP 450/450i and PMP 450m:

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

Table 73: Co-channel Interference per (CCI) modulation level

Modulation of Victim	Modulation of Interferer	Channel BW (MHz)	CCI
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	7 dB
2X (16-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	14 dB
3X (64-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	22 dB
4X (256-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	30 dB
2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	10 dB
3X (8-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	13 dB
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	17 dB
5X (32-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	21 dB
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	25 dB
7X (128-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	29 dB
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	33 dB

Table 74: Adjacent Channel Interference (ACI) per modulation level

Modulation of Victim	Modulation of Interferer	Channel BW (MHz)	ACI	Guard Band
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
3X (8-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
5X (32-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None

Modulation of Victim	Modulation of Interferer	Channel BW (MHz)	ACI	Guard Band
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
7X (128-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-13 dB	None
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-10 dB	None

Guard Band

When synchronized, no Guard Bands are needed for the 450, 450i, and 450m Series.

- For PMP 450 AP (3.6 GHz) and 450 series APs with 450b SM (5 GHz) connected, **Configuration-> Radio -> Power Control -> Adjacent Channel Support** must be enabled.

Improved PPS performance of 450 Platform Family

The 450m, 450i, and 450b Series provides improved packets per second (PPS) performance compared to 450 Series.

Through hardware and software enhancements, the PPS performance of the PMP 450i Series AP and PMP 450b SM has been improved to more than 100,000 packets/second, measured through a standard RFC2544 test using 64 bytes packets. With this enhancement, operators are able to provide higher bandwidth including better VoIP and video services to end customers using existing SM deployments.

PMP 450m is capable of supporting more than 100k PPS (packets per second).

Setting up SNMP agent

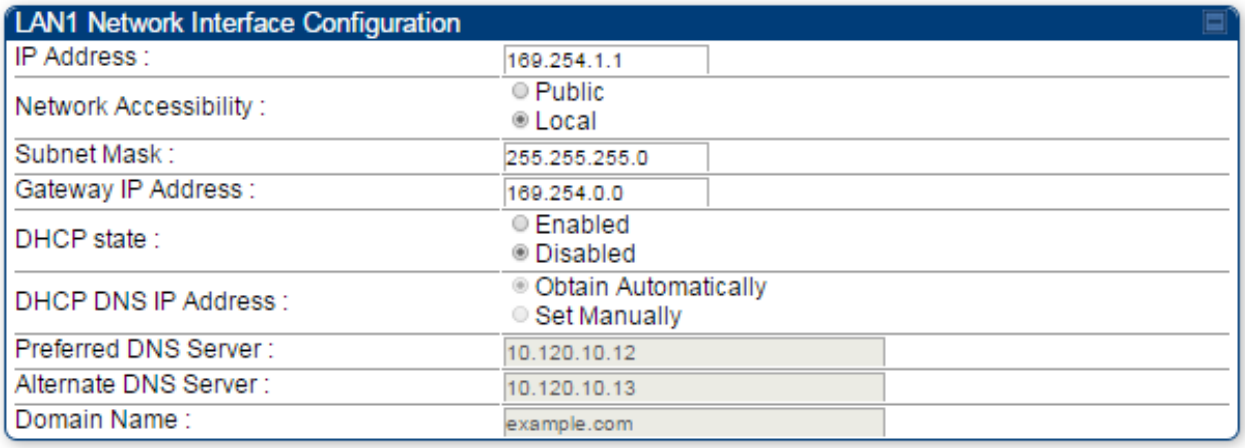
Operators may use SNMP commands to set configuration parameters and retrieve data from the AP and SM modules. Also, if enabled, when an event occurs, the SNMP agent on the 450 Platform Family sends a trap to whatever SNMP trap receivers configured in the management network.

- SNMPv2c
- SNMPv3

Configuring SM/BHS's IP over-the-air access

To access the SM/BHS management interface from a device situated above the AP, the SM/BHS's Network Accessibility parameter (under the web GUI at Configuration > IP) may be set to Public.

Table 75: LAN1 Network Interface Configuration tab of IP page attributes



Attribute	Meaning
IP Address	Internet Protocol (IP) address. This address is used by family of Internet protocols to uniquely identify this unit on a network.
Network Accessibility	Specify whether the IP address of the SM/BHS must be visible to only a device connected to the SM/BHS by Ethernet (Local) or be visible to the AP/BHM as well (Public).
Subnet Mask	If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the subnet mask of the SM/BHS for RF management traffic.
Gateway IP Address	If Static IP is set as the Connection Type of the WAN interface, then this parameter configures the gateway IP address for the SM/BHS for RF management traffic.
DHCP state	If Enabled is selected, the DHCP server automatically assigns the IP configuration (IP address, subnet mask, and gateway IP address) and the values of those individual parameters (above) are not used. The setting of this DHCP state parameter is also viewable (read only), in the Network Interface tab of the Home page.
DNS IP Address	Canopy devices allow for configuration of a preferred and alternate DNS server IP address either automatically or manually. Devices must set DNS server IP address manually when DHCP is disabled for the management interface of the device. The default DNS IP addresses are 0.0.0.0 when configured manually.
Preferred DNS Server	The first address used for DNS resolution.
Alternate DNS Server	If the Preferred DNS server cannot be reached, the Alternate DNS Server is used.
Domain Name	The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.

Configuring SNMP

The SNMP page configuration is explained below.

> **Note**
>
> The SNMP page for AP, SM, BHM and BHS has the same parameter attributes.

SNMP page – AP/SM/BHM/BHS

The SNMP page is explained in below table.

Table 76: SNMP page attributes

SNMPv2c Settings	
SNMP Community String 1 :	Canopy
SNMP Community String 1 Permissions :	(●) Read Only ( ) Read / Write
SNMP Community String 2 (Read Only) :	Canopyro

SNMPv3 Settings	
Engine ID :	800000a1030a003e4586f0 Use Default Engine ID
SNMPv3 Security Level :	auth,priv
SNMPv3 Authentication Protocol :	md5
SNMPv3 Privacy Protocol :	cbc-des
SNMPv3 Read-Only User :	Username Canopyro Authorization Key •••••••••••• Privacy Key ••••••••••••••••
SNMPv3 Read/Write User :	(●) Enable R/W User ( ) Disable R/W User Username Canopy Authorization Key ••••••••••• Privacy Key ••••••••••••••
Additional SNMPv3 User1 :	Username ( ) Enable User (●) Disable User Authorization Key Privacy Key ( ) ReadWrite User (●) ReadOnly User
Additional SNMPv3 User2 :	Username ( ) Enable User (●) Disable User Authorization Key Privacy Key ( ) ReadWrite User (●) ReadOnly User
Additional SNMPv3 User3 :	Username ( ) Enable User (●) Disable User Authorization Key Privacy Key ( ) ReadWrite User (●) ReadOnly User
SNMPv3 Trap Configuration :	Disabled

SNMP Accessing Addresses

Accessing IP / Subnet Mask 1 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 2 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 3 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 4 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 5 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 6 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 7 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 8 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 9 :	0.0.0.0	/ 0
Accessing IP / Subnet Mask 10 :	0.0.0.0	/ 0

Trap Addresses

SNMP Trap Server DNS Usage :	Append DNS Domain Name Disable DNS Domain Name
Trap Address 1 :	0.0.0.0
Trap Address 2 :	0.0.0.0
Trap Address 3 :	0.0.0.0
Trap Address 4 :	0.0.0.0
Trap Address 5 :	0.0.0.0
Trap Address 6 :	0.0.0.0
Trap Address 7 :	0.0.0.0
Trap Address 8 :	0.0.0.0
Trap Address 9 :	0.0.0.0
Trap Address 10 :	0.0.0.0

Trap Enable

Sync Status :	Enabled Disabled
Session Status :	Enabled Disabled

LQI Traps

LQI Traps :	Enabled Disabled
LQI threshold to raise trap (delta from reference LQI value) :	30
LQI threshold to clear trap (delta from reference LQI value) :	25
Minimum observation period :	1 Minutes (Range : 1 — 15 Minutes)

Site Information

Site Information Viewable to Guest Users :	Enabled Disabled
Site Name :	sucessful
Site Contact :	No Site Contact
Site Location :	No Site Location

Attribute	Meaning
SNMP Community String 1	Specify a control string that can allow a Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is Canopy.
SNMP Community String 1 Permissions	You can designate the SNMP Community String 1 to be the password for WM, for example, to have Read / Write access to the module via SNMP or for all SNMP access to the module to be Read Only.
SNMP Community String 2 (Read Only)	Specify an additional control string that can allow a Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is Canopyro. This password will never authenticate a user or an NMS to read/write access. The Community String value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the Accessing Subnet, Trap Address, and Permission parameters.
Engine ID	The Engine ID may be between 5 and 32 hex characters. The hex character input is driven by RFC 3411 recommendations on the Engine ID. The default Engine ID is the MAC address of the device
SNMPv3 Security Level	Specify security model where users are defined and authenticated before granting access to any SNMP service. Each device can configure the security level of SNMPv3 to No authentication/No privacy, Authentication/No privacy, or Authentication/Privacy.
SNMPv3 Authentication Protocol	The SNMPv3 authentication protocol is supported with: • MD5 • SHA-1 • SHA-256
SNMPv3 Privacy Protocol	The SNMPv3 privacy protocol is supported with: • CBC-DES • CFB-AES
SNMPv3 Read-Only User	This field allows for a read-only user per devices. The default values for the Read-Only users is: • Username = Canopyro • Authentication Password = authCanopyro • Privacy Password = privacyCanopyro
SNMPv3 Read/Write User	Read-write user by default is disabled. The default values for the Read/Write users is: • Username = Canopy • Authentication Password = authCanopy • Privacy Password = privacyCanopy

Attribute	Meaning
Additional SNMP v3 User 1	This field allows to configure the Additional SNMP v3 User 1. The configurations include: • Enable/Disable User: These fields allow to enable or disable the user using the Enable User or Disable User radio buttons. • Authorizaton Key: This field allows to configure an authorization key for the user. • Privacy Key: This field allows to configure a privacy key for the user. **Note** Set SNMP v3 Security Level field to: auth, priv to enable the Authorization Key and Privacy Key fields. Enabled User can be set with following privacy settings: • ReadWrite User • ReadOnly User
Additional SNMP v3 User 2	This field allows to configure the Additional SNMP v3 User 2. The configurations include: • Enable/Disable User: These fields allow to enable or disable the user using the Enable User or Disable User radio buttons. • Authorizaton Key: This field allows to configure an authorization key for the user. • Privacy Key: This field allows to configure a privacy key for the user. **Note** Set SNMP v3 Security Level field to: auth, priv to enable the Authorization Key and Privacy Key fields. Enabled User can be set with following Privacy settings: • ReadWrite User • ReadOnly User
Additional SNMP v3 User 3	This field allows to configure the Additional SNMP v3 User 3. The configurations include: • Enable/Disable User: These fields allow to enable or disable the user using the Enable User or Disable User radio buttons. • Authorizaton Key: This field allows to configure an authorization key for the user. • Privacy Key: This field allows to configure a privacy key for the user. Note Set SNMP v3 Security Level field to: auth, priv to enable the Authorization Key and Privacy Key fields.

Attribute	Meaning
	Enabled User can be set with following Privacy settings: • ReadWrite User • ReadOnly User
SNMPv3 Trap Configuration	When enabling transmission of SNMPv3 traps the read-only or read-write user credentials must be used and selected properly in order for the SNMP manager to correctly interpret the traps. By default transmission of SNMPv3 traps is disabled and all traps sent from the radios are in SNMPv2c format.
Accessing IP / Subnet Mask 1 to 10	Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both • The network IP address in the form xxx.xxx.xxx.xxx • The CIDR (Classless Interdomain Routing) prefix length in the form /xx For example: • the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet). • 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct Community String value. The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.” You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations. RECOMMENDATION: The subscriber can access the SM/BHS by changing the subscriber device to the accessing subnet. This hazard exists because the Community String and Accessing Subnet are both visible parameters. To avoid this hazard, configure the SM/BHS to filter (block) SNMP requests.
SNMP Trap Server DNS Usage	The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.
Trap Address 1 to 10	Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) or DNS names to which SNMP traps must be sent. Traps inform Wireless Manager or an NMS that something has occurred. For example, trap information is sent • after a reboot of the module. • when an NMS attempts to access agent information but either • supplied an inappropriate community string or SNMP version number. • is associated with a subnet to which access is disallowed.
Trap Enable, Sync Status	If the sync status traps (sync lost and sync regained) have to be sent to Wireless Manager or an NMS, select Enabled. If these traps have to be suppressed, select Disabled.

Attribute	Meaning
Trap Enable, Session Status	If you want session status traps sent to Wireless Manager or an NMS, select Enabled.
LQI Traps	This field enables and disables traps for LQI.
LQI threshold to raise trap (delta from reference LQI value)	It is configured in percentage. The LQI trap is raised if the LQI values goes below the configured threshold to raise trap from reference LQI. For example, if the LQI threshold to raise trap is set as 30, the LQI trap will be raised once the LQI goes below 70% (100-30).
LQI threshold to clear trap (delta from reference LQI value)	It is configured in percentage. The LQI trap is cleared if the LQI values goes above the configured threshold to clear trap from reference LQI. For example, if the LQI threshold to clear trap is set as 25, the LQI trap will be clear once the LQI goes above 75% (100-25).
Minimum observation period	It is minimum observation period to raise and clear the traps after LQI threshold. It can be configured between 1 to 15 minutes.
Site Information Viewable to Guest Users	Operators can enable or disable site information from appearing when a user is in GUEST account mode.
Site Name	Specify a string to associate with the physical module. This parameter is written into the sysName SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Contact	Enter contact information for the module administrator. This parameter is written into the sysContact SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Location	Enter information about the physical location of the module. This parameter is written into the sysLocation SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.

Configuring syslog

450 Platform Family includes:

- Syslog event logging
- Configuring system logging

Syslog event logging

Following events are logged in syslog as explained in below table.

Table 77: Syslog parameters

Attribute	Meaning
Timestamp	All syslog messages captured from the radio have a timestamp.

Attribute	Meaning
Configuration Changes	This includes any device setting that has changed and includes the old or new parameter value, including the device reboots.
User Login and Logout	Syslog records each user login and logout, with username.
Add or Delete of user accounts through GUI and SNMP	Syslog captures any user accounts that are added or deleted.
Spectrum Analysis	Syslog records a message every time Spectrum Analysis runs. Note Since the AP/BHM must be set to a SM/BHS for Spectrum Analysis, syslog messages are not reported from the radio until the scan is done and the radio mode is switched back to AP/BHM.
Link Test	Syslog records a message every time a Link Test is run.
Clear Statistics	Syslog sends a message when Statistics are cleared. This is done individually for each statistics page that is cleared.
SM Register or De-register	Syslog records a message when a SM registers or deregisters.
BHS Connect or Disconnect	Syslog records a message when a BHS connects or disconnects.

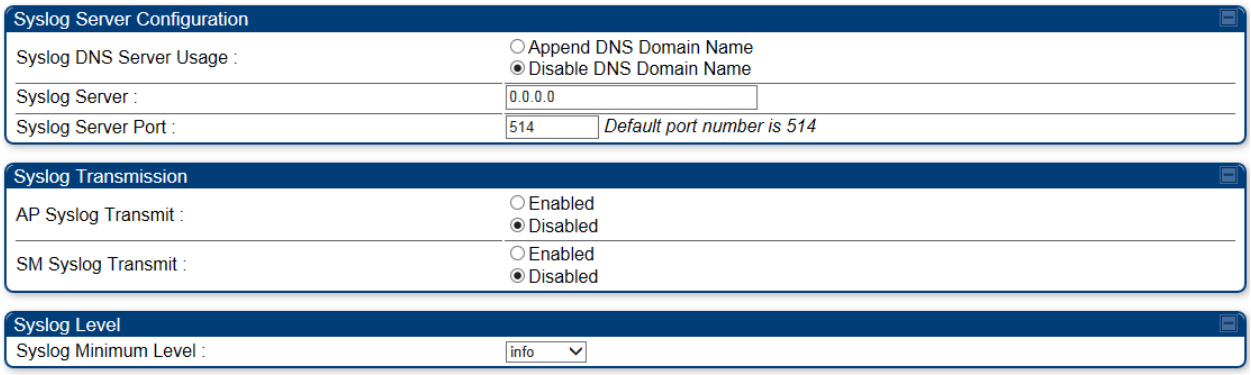
Configuring system logging

To configure system logging, select the menu option Configuration > Syslog.

Syslog page of AP/BHM

The Syslog Configuration page for AP/BHM is shown in below table.

Table 78: Syslog Configuration attributes - AP



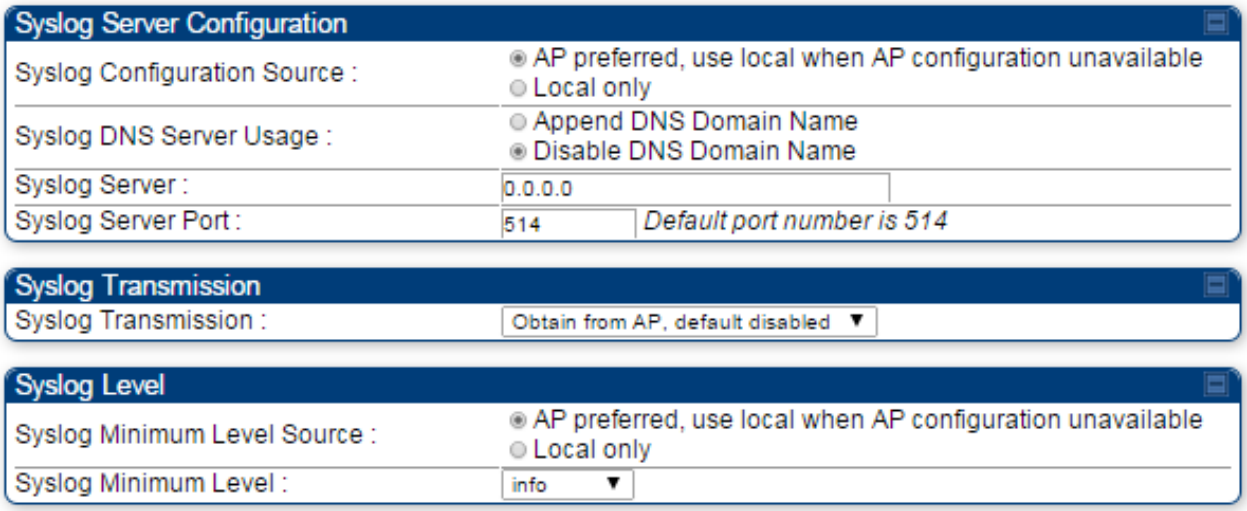
Attribute	Meaning
Syslog DNS Server Usage	To configure the AP/BHM to append or not append the DNS server name to the syslog server name.

Attribute	Meaning
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
AP Syslog Transmit Or BHM Syslog Transmit	When enabled, syslog messages are sent from the AP/BHM.
SM Syslog Transmit Or BHS Syslog Transmit	When enabled, syslog messages are sent from all the registered SMs/BHS, unless they are individually set to override this.
Syslog Minimum Level	This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity). For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

Syslog page of SM

To configure system logging, select the menu option Configuration > Syslog. The Syslog Configuration page is shown in below table.

Figure 40: *Syslog Configuration attributes - SM*



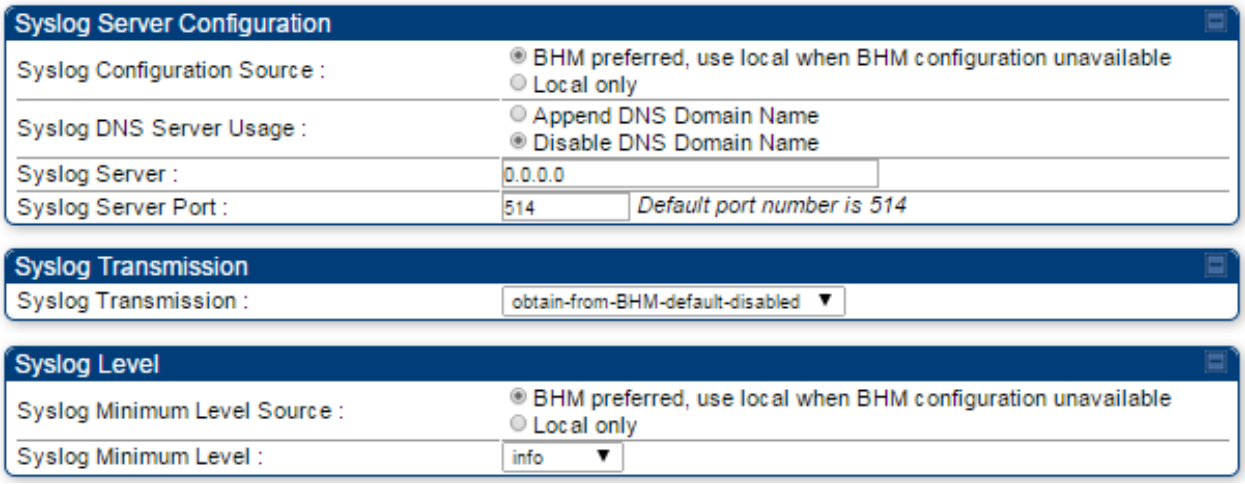
Attribute	Meaning
Syslog Configuration Source	This control determines whether the SM will attempt to use the syslog server definition from the AP, or whether it will use a local server definition.

Attribute	Meaning
	When set to AP preferred, use local when AP configuration unavailable, and if the SM can register with an AP, then it uses the syslog server defined on that AP. If the SM cannot register then it will syslog to its locally defined syslog server through its wired connection, if any. When set to Local only the SM ignores the AP's definition of the syslog server and allows the syslog server to be configured individually for each SM.
Syslog DNS Server Usage	To configure the SM to append or not the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
Syslog Transmission	Controls the SMs ability to transmit syslog messages. When set to "Learn from AP" the AP will control whether this SM transmits syslog messages. When set to "enable" or "disable" the SM will control whether it sends syslog messages. This allows an operator to override the AP settings for individual SMs in a sector.
Syslog Minimum Level Source	This control determines whether the SM attempts to use the minimum syslog level defined by the AP, or whether it uses a local defined value using the "Syslog Minimum Level" parameter. When set to "AP preferred, use local when AP configuration unavailable", and if the SM can register with an AP, then it uses the Syslog Minimum Level defined on that AP. If the SM cannot register then it uses its own Syslog Minimum Level setting. When set to "Local only" the SM will always use its own Syslog Minimum Level setting and ignores the AP's setting.
Syslog Minimum Level	This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity). For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

Syslog page of BHS

The Syslog Configuration page is shown in below table.

Table 79: Syslog Configuration attributes - BHS



Attribute	Meaning
Syslog Configuration Source	This control determines whether the BHS will attempt to use the syslog server definition from the BHM, or whether it will use a local server definition. • When set to BHM preferred, use local when BHM configuration unavailable, and if the BHS can register with a BHM, then it uses the syslog server defined on that BHM. If the BHS cannot register then it will syslog to its locally defined syslog server through its wired connection, if any. • When set to Local only the BHS ignores the BHM's definition of the syslog server and allows the syslog server to be configured individually for each BHS.
Syslog DNS Server Usage	To configure the BHS to append or not to append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
Syslog Transmission	Controls the BHSs ability to transmit syslog messages. When set to Learn from BHM the BHM will control whether this BHS transmits syslog messages. When set to enable or disable the BHS will control whether it sends syslog messages. This allows an operator to override the BHM settings for individual BHSs in a sector.
Syslog Minimum Level Source	This control determines whether the BHS attempts to use the minimum syslog level defined by the BHM, or whether it uses a local defined value using the Syslog Minimum Level parameter. • When set to BHM preferred, use local when BHM configuration unavailable, and if the BHS can register with a BHM, then it uses the Syslog Minimum Level defined on that BHM. If the BHS cannot register then it uses its own Syslog Minimum Level setting. When set to Local only the BHS will always use its own Syslog Minimum Level setting and ignores the BHM's setting.

Attribute	Meaning
Syslog Minimum Level	This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity). For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

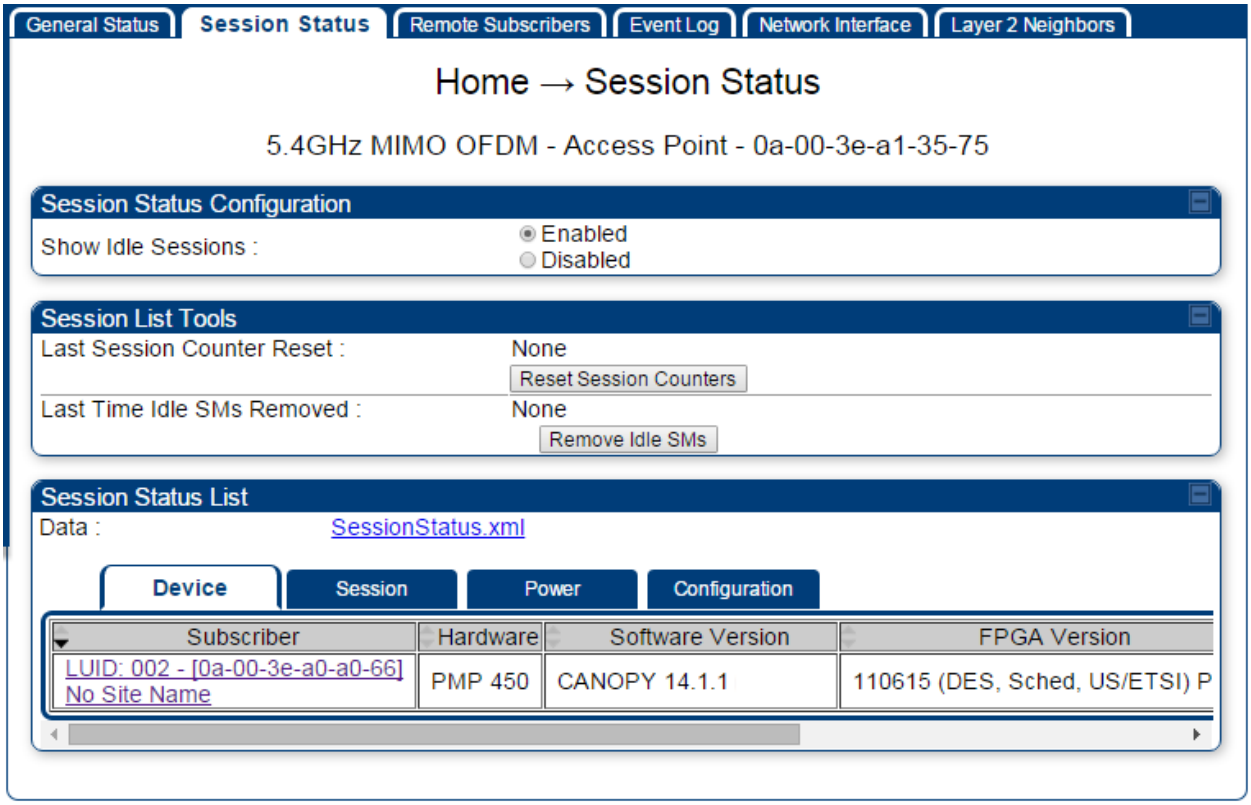
Configuring remote access

Accessing SM/BHS over-the-air by Web Proxy

The SM/BHS may be accessed via the AP/BHM management GUI by navigating to Home > Session Status (or Home > Remote Subscribers for AP only) and clicking on the SM's hyperlink.

For example, to access one of the SMs, click LUID: 002 – [0a-00-3e-37-b9-fd], as shown in below table.

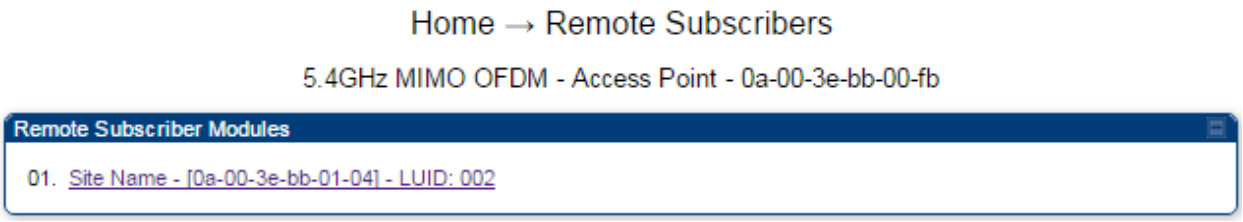
Figure 41: *AP Session Status page*



The SessionStatus.xml hyper link allows user to export all displayed SM data in Session Status table into an xml file.

To access any one of the SMs, click 450 Platform Family - SM hyperlink, as shown in below figure.

Figure 42: *AP Remote Subscribers page*



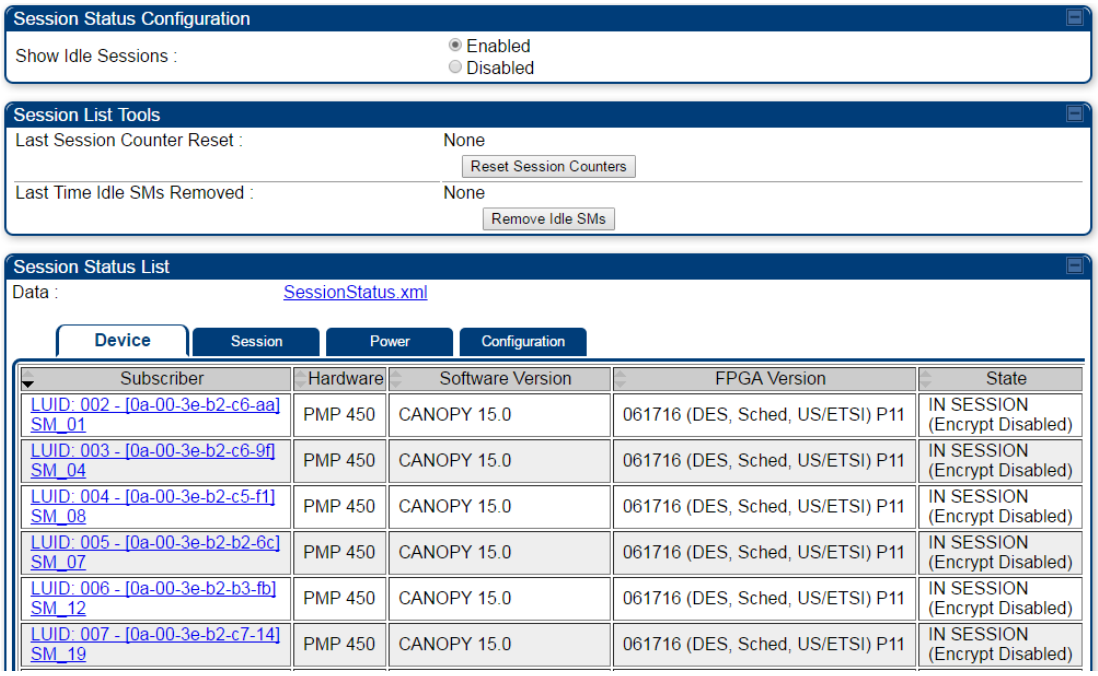
Monitoring the Link

Link monitoring procedure

After configuring the link, either an operator in the network office or the SM/BHS INSTALLER user in the field (if read access to the AP/BHM is available to the INSTALLER) must perform the following procedure. Who is authorized and able to do this depends on local operator password policy, management VLAN setup and operational practices.

To monitor the link for performance, follow these instructions:

Procedure 14 Monitoring the AP-SM link

1	Access the web interface of the AP/BHM
2	In the left-side menu of the AP/BHM interface, select Home.
3	Click the Session Status tab. Figure 43: *Session Status page* 

Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-b2-c6-aa] SM_01	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 003 - [0a-00-3e-b2-c6-9f] SM_04	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 004 - [0a-00-3e-b2-c5-f1] SM_08	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 005 - [0a-00-3e-b2-b2-6c] SM_07	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 006 - [0a-00-3e-b2-b3-fb] SM_12	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)
LUID: 007 - [0a-00-3e-b2-c7-14] SM_19	PMP 450	CANOPY 15.0	061716 (DES, Sched, US/ETSI) P11	IN SESSION (Encrypt Disabled)

4	The Device tab of Session Status List display all displayed SMs – MAC address, PMP/PTP Hardware, Software Version, FPGA Version and State
5	Click Session Count tab of Session Status List to display values for Session Count, Reg Count, and Re-Reg Count.

	• Session Count: This field displays how many sessions the SM/BHS has had with the AP/BHM. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.
	• Reg Count: When a SM/BHS makes a Registration Request, the AP/BHM checks its local session database to see whether it was registered earlier. If the AP/BHM concludes that the SM/BHS is not currently in session database and it is valid Registration Request, then the request increments the value of this field.
	• Re-Reg Count: When a SM/BHS makes a Registration Request, the AP/BHM checks its local session database to see whether it was registered earlier. If the AP/BHM concludes that the SM/BHS is currently in session database, then the request increments the value of this field.
	• Typically, a Re-Reg is the case where both
	  • SM/BHS attempts to reregister for having lost communication with the AP/BHM.
	  • AP/BHM has not yet observed the link to the SM/BHS as being down.
	See Session tab.

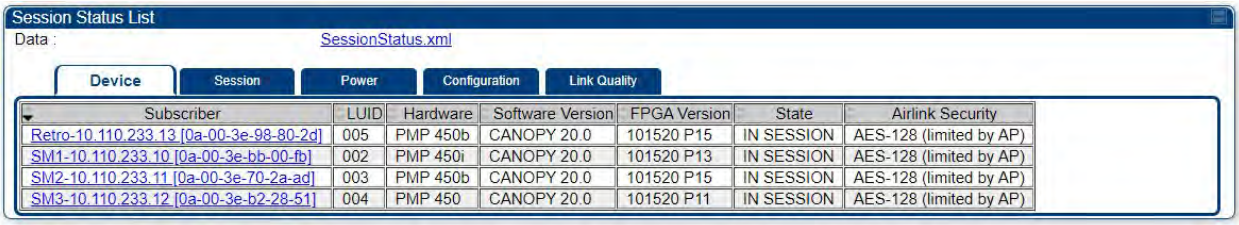
6	Click Power tab of Session Status list to display Downlink Rate, AP Rx Power (dBm), Signal Strength Radio (dB) for Uplink and Signal to Noise Radio (dB) for Uplink. See Power tab.
7	Click Configuration tab of Session Status list to get QoS configuration details: • Sustained Data Rate (kbps) • Burst Allocation (kbit) • Max Burst Rate (kbit) • Low Priority CIR (kbps)
8	Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.
9	If these values are low (for example, 1, 1, and 0, respectively, meaning that the SM/BHS registered and started a stable session once) and are not changing: • Consider the installation successful. • Monitor these values from the network office over the next several hours and days. If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, Use Receive Power Level for aiming and then use Link Tests to confirm alignment).

Refer Viewing Session Status on page 1 for more details.

Exporting Session Status page of AP/BHM

The SessionStatus.xml hyper link allows user to export all displayed SMs or BHS data in Session Status table into an xml file.

Figure 44: *Exporting Session Status page of PMP 450m AP*



Subscriber	LUID	Hardware	Software Version	FPGA Version	State	Airlink Security
Retro-10.110.233.13 [0a-00-3e-98-80-2d]	005	PMP 450b	CANOPY 20.0	101520 P15	IN SESSION	AES-128 (limited by AP)
SM1-10.110.233.10 [0a-00-3e-bb-00-fb]	002	PMP 450i	CANOPY 20.0	101520 P13	IN SESSION	AES-128 (limited by AP)
SM2-10.110.233.11 [0a-00-3e-70-2a-ad]	003	PMP 450b	CANOPY 20.0	101520 P15	IN SESSION	AES-128 (limited by AP)
SM3-10.110.233.12 [0a-00-3e-b2-28-51]	004	PMP 450	CANOPY 20.0	101520 P11	IN SESSION	AES-128 (limited by AP)

In case of PMP, if the session status page does not list any SM, the SessionStatus.xml will still be visible but the file would be empty. The file will contain data from all of the 5 different tables.

Export from command line

The scripts users can also get this file from command line, you have to authenticate successfully in order to download the file.

http://169.254.1.1/SessionStatus.xml?CanopyUsername=test&CanopyPassword=test

Configuring quality of service

Maximum Information Rate (MIR) Parameters

Point-to-multipoint links use the following MIR parameters for bandwidth management:

- Sustained Uplink Data Rate (kbps)
- Uplink Burst Allocation (kb)
- Sustained Downlink Data Rate (kbps)
- Downlink Burst Allocation (kb)
- Max Burst Downlink Data Rate (kbps)
- Max Burst Uplink Data Rate (kbps)

Set each of these parameters per AP or per SM independently.

Note

You can refer below whitepaper for 450 Platform Family Max Burst MIR:

http://www.cambiumnetworks.com/resources/pmp-450-maxburst/

Token Bucket Algorithm

The software uses a token bucket algorithm that has the following features:

- Stores credits (tokens) for the SM to spend on bandwidth for reception or transmission.
- Drains tokens during reception or transmission.
- Refills with tokens at the sustained rate set by the network operator.

For each token, the SM can send toward the network in the uplink (or the AP can send toward the SM in the downlink) an equivalent number of kilobits. Two buckets determine the permitted throughput: one in the SM for uplink and one in the AP for downlink.

The applicable set of Uplink Burst Allocation and Downlink Burst Allocation parameters determine the number of tokens that can fill each bucket. When the SM transmits (or the AP transmits) a packet, the equivalent number of tokens is removed from the uplink (or downlink) bucket.

Except when full, the bucket is continuously being refilled with tokens at rates that the applicable set of Sustained Uplink Data Rate and Sustained Downlink Data Rate parameters specify. The bucket often drains at a rate that is much faster than the sustained data rate but can refill at only the sustained data rate. Thus, the effects of the allocation and rate parameters on packet delay are as follows:

- The burst allocation affects how many kilobits are processed before packet delay is imposed.
- The sustained data rate affects the packet delay that is imposed.

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in below figure.

> **Note**
>
> In these figures, entry refers to the setting in the data rate parameter, not the burst allocation parameter.

Figure 45: *Uplink and downlink rate caps adjusted to apply aggregate cap*

$$\text{uplink cap enforced} = \frac{\text{uplink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

$$\text{downlink cap enforced} = \frac{\text{downlink entry} \times \text{aggregate cap for the SM}}{\text{uplink entry} + \text{downlink entry}}$$

For example, in the SM, if you set the Sustained Uplink Data Rate parameter to 2,000 kbps and the Sustained Downlink Data Rate parameter to 10,000 kbps, then the uplink and downlink MIR that is enforced for the SM can be calculated as shown in below figure.

Figure 46: *Uplink and downlink rate cap adjustment example*

$$\text{uplink cap enforced} = \frac{2{,}000\ \text{kbps} \times 7{,}000\ \text{kbps}}{2{,}000\ \text{kbps} + 10{,}000\ \text{kbps}} = 1{,}167\ \text{kbps}$$

$$\text{downlink cap enforced} = \frac{10{,}000\ \text{kbps} \times 7{,}000\ \text{kbps}}{2{,}000\ \text{kbps} + 10{,}000\ \text{kbps}} = 5{,}833\ \text{kbps}$$

In this example case, the derived 1,167-kbps uplink and 5,833-kbps downlink MIR sum to the fixed 7,000-kbps aggregate cap of the SM.

Committed Information Rate (CIR)

The Committed Information Rate (CIR) capability feature enables the service provider to guarantee to any subscriber that bandwidth will never decrease to below a specified minimum unless CIR is oversubscribed or RF conditions are degraded. CIR is oversubscribed when there is not enough available bandwidth to support CIR configuration for all subscribers. In this condition, SMs which are configured with a nonzero CIR will all operate at the maximum data rate supported by the link (subject to Maximum Information Rate and Burst Rate/Allocations). SMs which are configured with a CIR of 0 kbps will not transmit until CIR-configured SMs have completed transmission. CIR may be configured independently for low priority traffic, medium priority traffic, high priority traffic, and ultra high priority traffic.

> Note
>
> CIR settings only apply to the Legacy scheduler. Starting in release 16.1 a new Proportional scheduler can optionally be enabled via Configuration -> Quality of Service -> Scheduler setting. If Proportional Scheduler is set, CIR's are not used.

CIR parameters may be configured in the following ways:

- Web-based management GUI
- SNMP
- Authentication Server (RADIUS) - when an SM successfully registers and authenticates, CIR information is retrieved from the RADIUS server.

Active CIR configuration can be verified via the AP's Home > Session Status page.

Bandwidth from the SM Perspective

In the SM, normal web browsing, e-mail, small file transfers and short streaming video are rarely rate limited with practical bandwidth management (QoS) settings. When the SM processes large downloads such as software upgrades and long streaming video or a series of medium-size downloads, the bucket rapidly drains, the burst limit is reached, and some packets are delayed. The subscriber experience is more affected in cases where the traffic is more latency sensitive.

Interaction of Burst Allocation and Sustained Data Rate Settings

If the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps, a data burst of 1000 kb is transmitted at full speed because the Burst Allocation is set high enough. After the burst, the

bucket experiences a significant refill at the Sustained Data Rate. This configuration uses the advantage of the settable Burst Allocation.

If both the Burst Allocation and the Sustained Data Rate are set to 128 kb, a burst is limited to the Burst Allocation value. This configuration does not take advantage of the settable Burst Allocation.

If the Burst Allocation is set to 128 kb and the Sustained Data Rate is set to 256 kbps, the actual rate is the burst allocation (but in kbps). As above, this configuration does not take advantage of the settable Burst Allocation.

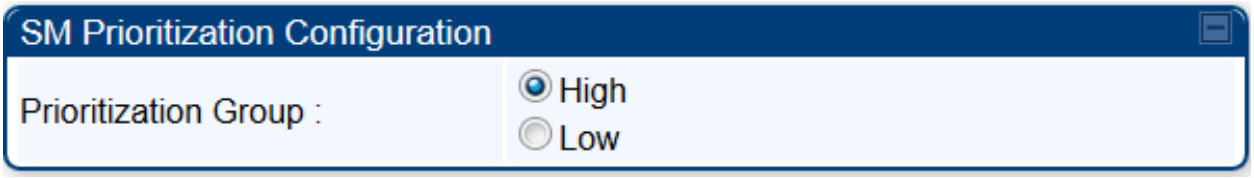
SM Prioritization

> Note
>
> This feature is not supported on PMP 450m.

SM Prioritization provides a way to designate a subset of a PMP sector's SMs with a guaranteed portion of air interface resources - slots, which are handled first during scheduling. SMs by default are configured in the SM Prioritization Low Group, and can be configured for the SM Prioritization High Group if desired.

The selection of which prioritization group each SM is configured in Configuration > Quality of Service tab > SM Prioritization Configuration on the SM GUI, as shown in below figure.

Figure 47: *SM Prioritization on SM*



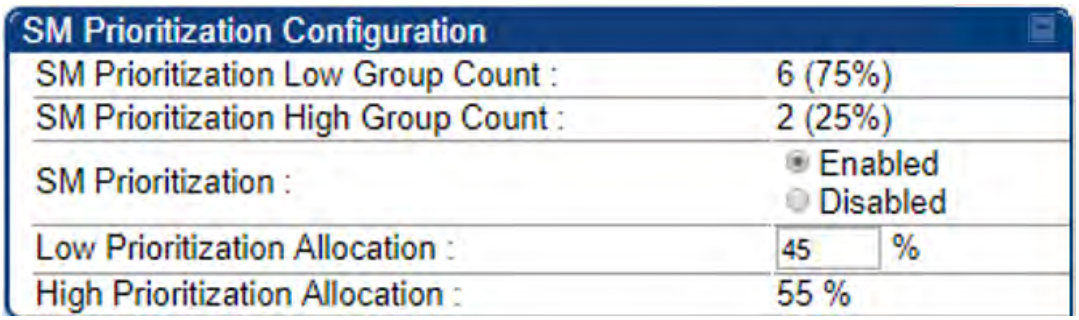
The feature does not take effect, however, until SM Prioritization is enabled on the AP, because the scheduler runs on the AP. Prioritization Allocation percentages per group are configured on the AP to determine how many timeslot resources are dedicated to each priority group.

Enabling of the feature and allocation percentages per group are configured in **Configuration -> Quality of Service tab -> SM Prioritization** Configuration on the AP GUI as shown in SM Prioritization on AP.

With Cambium's SM prioritization feature, we guarantee a percentage of slot resources to each prioritization group. If the resource allocation demands of the SMs in the High Priority allocation group are met without allocating all of that group's allocation percentage, the remaining resources can be used for any unmet demands for SMs in the Low Group. Similarly, if the resource allocation demands of the SMs in the Low Priority allocation group are met without allocating all of that group's allocation percentage, the remaining resources can be used for any unmet demands for SMs in the High Group. If the sector has 100% utilization, the resource allocation per group will equal the percentages configured on the AP. This feature can be used to provide guaranteed frame allocation to high priority clients, such as business customers. Although SM Prioritization Group 1 is called the "High Priority" group, and SM Prioritization Group 2 is called the "Low Priority" group, this does not mean that 1 group is scheduled resources before the other group. The intention is, by adjusting the number of SMs in the High Priority group and the allocation percentages per group, the SMs in the High Priority group will have a higher "slots/SMs" ratio.

The following figure shows the SM Prioritization configuration at the AP with this feature enabled.

Figure 48: *SM Prioritization on AP*



In the example shown in SM Prioritization on AP, 2 of the 8 SMs have been configured for the High Priority Group. The other 6 are in the Low Priority group. 45% of the air interface timeslot resources have been allocated to the Low Priority group. If, for example, all SMs are fully active and all resources in this sector are fully utilized, then 55% of the air interface slot resources will be shared between the 2 High Priority SMs, per direction, and the remaining 45% of the resources will be shared between the other 6 SMs.

If, on the other hand, only 40% of the resources are needed to meet the scheduling demands of the 2 High Priority SMs, the additional 15% that was pre-allocated to the High Priority group can then be used for the Low Priority group, maintaining 100% slot utilization in the sector.

SM Prioritization with CIR

When the SM Prioritization feature is used with CIR, Cambium's scheduler will first prioritize scheduling of data channels configured with a CIR, but only within the limits of that SMs Prioritization Group allocation. In the example configuration shown in SM Prioritization on AP, there are 6 SMs in the Low Prioritization group. If 3 of those 6 SMs each have a 1Mbps CIR configured, the Cambium scheduler will attempt to meet this 1Mbps CIR per SM before scheduling the other 3 SMs. But if both prioritization groups are overloaded, this 3Mbps committed load on these 3 SMs will only be achieved if it can be done with 55% of the resources or less – per direction.

Weighted Fair Queuing (WFQ)

Note

This feature is not supported on PMP 450m.

This feature lets the user assign a percentage of air interface resources to each of the Data Channel levels. The WFQ apply both to the DL and the UL. Note that there is no BC/MC traffic in the UL direction.

One of the benefits of WFQ is that the configuration can be accomplished at the AP rather than at each individual SMs. This feature can be used with or in place of existing CIR settings. Unlike CIR, which is set in kbps independent of the modulation rate, the WFQ feature operates on a percentage of air interface resources, or timeslots.

Weighted Fair Queuing Configuration is an example of a WFQ configuration on the AP. This can be found in Configuration > Quality of Service tab > Weighted Fair Queuing Configuration on the AP GUI.

In this particular sector, we have 30 Data channels spread across 8 registered SM's. 4 levels of QoS have been configured on 7 of the SM's, 2 levels of QoS have been configured on 1 of the SM's.

Figure 49: *Weighted Fair Queuing Configuration*

Weighted Fair Queuing Configuration	
Data Channel Count - Low Priority :	1 (25%)
Data Channel Count - Medium Priority :	1 (25%)
Data Channel Count - High Priority :	1 (25%)
Data Channel Count - Ultra High Priority :	1 (25%)
Weighted Fair Queuing :	◉ Enabled ○ Disabled
WFQ Configuration :	**Valid**
Data Channel Allocation - Broadcast/Multicast :	4 %
Data Channel Allocation - Low Priority :	22 %
Data Channel Allocation - Medium Priority :	22 %
Data Channel Allocation - High Priority :	26 %
Data Channel Allocation - Ultra High Priority :	26 %

The above figure shows that 4% of the air interface resources have been reserved for Broadcast/Multicast traffic, 22% of the available air interface timeslot have been reserved for the lowest priority traffic, 22% for medium priority traffic, 26% for high priority traffic, and 26% for the highest priority traffic (Ultra High Priority).

If, at any point in the time, the aggregate traffic load across all SMs on 1 QoS level is less than that level's Weighted Fair Queue allocation, then those unused slots will be allocated for traffic in other QoS levels, based on strict priority.

For example, if, during peak traffic hours, the Ultra High, High, and Low priority Data channels were experiencing heavy traffic loads, but the medium priority aggregate traffic load was light and only used 10% of the scheduling slots in a particular direction, the remaining unused 12% of the slots would be allocated first to the Ultra High priority traffic in queue. When all the Ultra High priority traffic has been scheduled, then any remaining unused slots would be used for High Priority traffic. Finally, after High Priority traffic has been serviced, any remaining slots would be used for Low Priority traffic. The "Low Priority" in the sub-heading "Low Priority SM's WFQ Configuration" shown above simply indicates that the SM Prioritization feature is turned off in this example above. The "Valid" indication in this screenshot is a simple software check to make sure that the configured percentages add up to 100%.

WFQ with CIR

> Note
>
> This feature is not supported on PMP 450m.

The WFQ feature can be used with, or as a replacement for, configuring Committed Information Rates (CIR) per data channel. When the WFQ feature is used with CIR's, Cambium's scheduler will first prioritize scheduling of the Data channels configured with a CIR, but only within the limits of that QoS level's WFQ allocation.

Using the example configuration show in Weighted Fair Queuing Configuration, there are 8 high priority Data channels. If 5 of those 8 Data channels have a CIR configured, then the Cambium scheduler will prioritize traffic on those 5 Data channels up to their CIR limits, for those 26% of the timeslots allocated to that QoS level. Operators should try to avoid oversubscription of CIR's. But if CIR's have been oversubscribed at any 1 QoS level such that the desired CIR rates cannot be met within the limits of that

level's WFQ allocation, the scheduler will use unallocated slots from another QoS level in strict priority order.

From the prior example, if there is less than 22% of timeslots worth of traffic on the medium priority Data channels, those unused slots would be allocated to Ultra High Priority traffic on Data channels that had not met their CIR commitment within the WFQ allocation, then on High Priority Data channels that had not met their CIR commitment within WFQ allocation, then on Low Priority Data channels that had not met their CIR commitment with WFQ allocation, then on Ultra High Priority traffic above and beyond any CIR configurations, and so on.

WFQ with SM Prioritization

> **Note**
>
> This feature is not supported on PMP 450m.

WFQ with SM Prioritization shows a WFQ configuration with the SM Prioritization feature also enabled.

Figure 50: *WFQ with SM Prioritization*

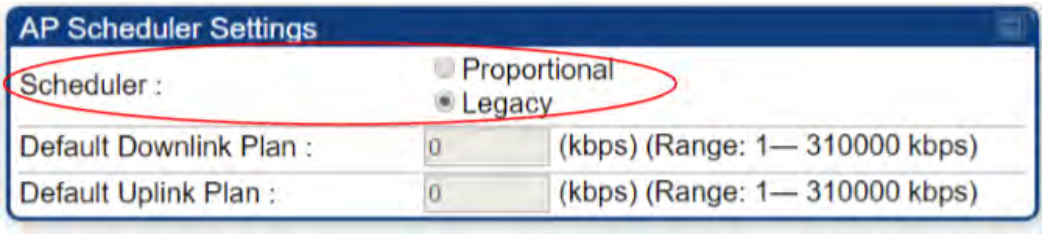
Weighted Fair Queuing Configuration	
Data Channel Count - Low Priority :	1 (25%)
Data Channel Count - Medium Priority :	1 (25%)
Data Channel Count - High Priority :	1 (25%)
Data Channel Count - Ultra High Priority :	1 (25%)
Weighted Fair Queuing :	◉ Enabled ○ Disabled
WFQ Configuration (SM Prioritization Low Group) :	**Valid**
Data Channel Allocation - Broadcast/Multicast :	4 %
Data Channel Allocation - Low Priority :	22 %
Data Channel Allocation - Medium Priority :	22 %
Data Channel Allocation - High Priority :	26 %
Data Channel Allocation - Ultra High Priority :	26 %
WFQ Configuration (SM Prioritization High Group) :	**Valid**
Data Channel Allocation - Low Priority :	25 %
Data Channel Allocation - Medium Priority :	25 %
Data Channel Allocation - High Priority :	25 %
Data Channel Allocation - Ultra High Priority :	25 %

In the example shown in WFQ with SM Prioritization, 2 of the 8 SMs have been configured for the High Priority Group. The other 6 are in the Low Priority group. 45% of air interface timeslot resources have been allocated to the Low priority group. The same allocation rules described above still apply to the WFQ allocation, but now these allocations are done within the confines of each Prioritization group. So, in this configuration shown in WFQ with SM Prioritization, the 2 Medium Priority QoS level Data channels in the High Priority SM Prioritization Group together share 12% of the committed air interface resources per direction. (.55 x .22 = .12) The same CIR allocation rules apply. The Cambium scheduler will attempt to meet those CIR allocations within the confines of that 12% allocation. If the traffic load on those 2 data channels is light, for example using only 5% of the available slots, then the remaining 7% of resources can be used for other traffic in a strict priority manner. (i.e. attempt to honor CIR's first, then Ultra High Priority traffic, then High Priority traffic, and so on, as described previously).

Proportional Scheduler

This feature, also known as the Rate Plan feature, allows a user to set Plans per SM in units of Kbps. The proportional scheduler maintains the proportions of the SMs' plans when the sector is congested. A default plan setting per direction also exists on the AP and is used in case an SM is not configured with a Plan (for example, the SM is not upgraded to system release 16.1 yet).

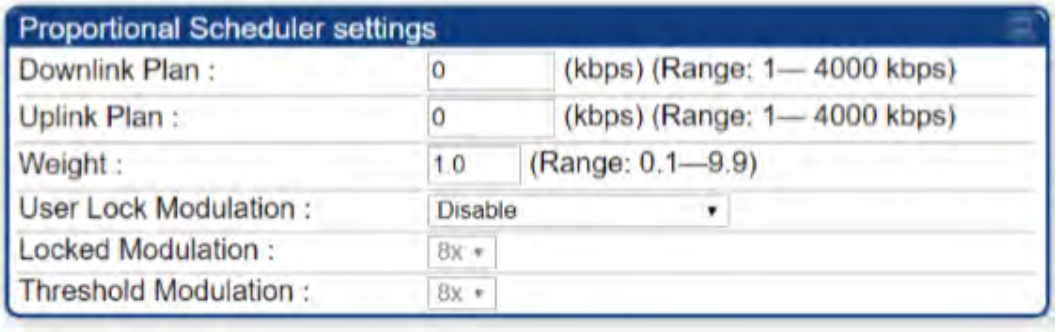
Figure 51: *Scheduler Settings on AP*



When selecting the Proportional scheduler, CIR is no longer applicable.

In system release 16.1, the SM supports a Proportional Scheduler setting section in the Configuration-> Quality of Service (QoS) page. These settings are applicable only if the AP is configured to use the Proportional scheduler.

Figure 52: *Proportional Scheduler Settings on SM*



The above 6 settings parameters are described in detail in the Quality of Service (QoS) page of SM later in this document.

The proportional scheduler works in conjunction with the Weighted Fair Queuing feature (in the products that support it), but preserving the plans ratios takes precedence in the scheduler decisions over honoring the WFQ percentages

High Priority Bandwidth Traffic

To support low-latency traffic such as VoIP (Voice over IP) or video, or critical traffic such as control packets, the system implements priority data channels. Prior to PMP 450 Release 15.2, the system allowed for a single High Priority Channel to be configured per SM and per direction, in addition to the default low priority channel. This channel did not affect the inherent latencies in the system but allowed high-priority traffic to be immediately served. The high-priority pipe separates low-latency traffic from traffic that is latency tolerant, such as standard web traffic and file downloads.

From system release 15.2, the system supports up to 4 QoS levels, or data channels, per SM. These are called Low, Medium, High, and Ultra High data channels.

The number of data channels available on the AP is still limited to 238 in release 15.2 This could be 238 SM's each configured with a single Low Priority channel, or, for example, 59 SMs with 4 data channels configured and 1 SM with 2 data channels configured.

A module prioritizes traffic by:

- reading the 802.1p field of the 802.1Q header in a received packet, where VLAN is enabled on the module.
- comparing the 6-bit Differentiated Services Code Point (DSCP) field in the ToS byte of a received packet to a corresponding value in the Diffserv tab of the Configuration page of the module.

Modules monitor ToS bytes with DSCP fields, but with the following differences:

- The 6-bit length of the field allows it to specify one of 64 service differentiations.
- These correlate to 64 individual (CodePoint) parameters in the Diffserv tab of the Configuration page.
- The 8 Class Selector code points are fixed in code and not user settable.
- For any or all of the remaining 56 CodePoint parameters, you can specify a value of
- 0, 1 for low-priority handling.
- 2, 3 for medium-priority handling.
- 4,5 for high-priority handling.
- 6, 7 for ultra-high-priority handling.

The above mapping applies if 4 QoS levels are configured. If fewer than that are configured, see the mapping table in the IPv4 and IPv6 Prioritization of this document.

Note

Ensure that your Differentiated Services domain boundary nodes mark any entering packet, as needed, so that it specifies the appropriate Code Point for that traffic and domain. This prevents theft of service level.

An example of the Diffserv page in the Configuration menu and parameter descriptions are provided under IPv4 and IPv6 Prioritization on page IPv4 and IPv6 Prioritization. This tab and its rules are identical from module type to module type. However, any of the 61 configurable Code Points can be set to a different value from module to module, thus defining unique per-hop behavior for some traffic.

This tab in the AP sets the priorities for the various packets in the downstream (sent from the public network). This tab in the SM sets the priorities for the various packets in the upstream (sent to the public network).

Typically, some SMs attach to older devices that use the ToS byte as originally formatted, and others to newer devices that use the DSCP field. The default values in the Diffserv page allow your modules to prioritize traffic from the older devices roughly the same as they traditionally have. However, these default values may result in more high-priority traffic as DSCP fields from the newer devices are read and handled. So, after making changes in the Diffserv page, carefully monitor the high-priority channel for high packet rates

- In SMs that you have identified as those to initially set and watch.
- Across your network when you have broadly implemented Code Point values, such as via SNMP.

Traffic Scheduling

The characteristics of traffic scheduling in a sector are summarized in below table.

Table 80: Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	132 Mbps for 20 MHz Higher for 30 MHz or 40 MHz and lower for smaller bandwidths.
Latency	Number of frames required for the scheduling process	1
	Round-trip latency	6 ms
	AP broadcast the download schedule	No
Priority Data Channels	Allocation for uplink high-priority data channel traffic on amount of traffic at these higher QoS levels.	Dynamic, based on amount of high-priority traffic
	Allocation for downlink high-priority data channel traffic on amount of traffic at these higher QoS levels	Dynamic, based on amount of high-priority traffic
	Order of transmission	1- Ultra High Priority data channels below CIR limit 2- High Priority data channel's below CIR limit 3- Medium Priority data channels below CIR limit 4- Low Priority data channels below CIR limit 5- Ultra High Priority data channels above CIR limit 6- High Priority data channels above CIR limit 7- Medium Priority data channels above CIR limit 8- Low Priority data channels above CIR limit

> **Note**
>
> This strict priority transmission order is only true in all cases if the SM Prioritization and Weighted Fair Queue features are disabled. If either feature is enabled, see the description of those features in this document for how they impact and interact with this transmission order.

Setting the Configuration Source

The AP includes a Configuration Source parameter, which sets where SMs that register to the AP are controlled for MIR, CIR, VLAN, and the high-priority channel as follows. The Configuration Source parameter affects the source of:

- all MIR settings:
    - Sustained Uplink Data Rate
    - Uplink Burst Allocation
    - Max Burst Uplink Data Rate
    - Sustained Downlink Data Rate
    - Downlink Burst Allocation
    - Max Burst Downlink Data Rate
- all CIR settings:
    - Low Priority Uplink CIR
    - Low Priority Downlink CIR
    - Medium Priority Uplink CIR
    - Medium Priority Downlink CIR
    - High Priority Uplink CIR
    - High Priority Downlink CIR
    - Ultra High Priority Uplink CIR
    - Ultra High Priority Downlink CIR
- all SM VLAN settings
    - Dynamic Learning
    - Allow Only Tagged Frames
    - VLAN Aging Timeout
    - Untagged Ingress VID

    - Management VID
    - VLAN Membership
- the High Priority Channel setting

Table 81: Recommended combined settings for typical operations

Most operators who use...	must set this parameter...	in this web page/tab...	in the AP to...
no authentication server	Authentication Mode	Configuration/ Security	Disabled
	Configuration Source	Configuration/ General	SM
Wireless Manager (Authentication Server)	Authentication Mode	Configuration/ Security	Authentication Server
	Configuration Source	Configuration/ General	Authentication Server
RADIUS AAA server	Authentication Mode	Configuration/ Security	RADIUS AAA
	Configuration Source	Configuration/ General	Authentication Server

Table 82: Where feature values are obtained for an SM registered under an AP with Authentication Mode set to something other than "DISABLED"

Configuration Source Setting in the AP	Values are obtained from		
	MIR Values	VLAN Values	Data Channel Count per SM
Authentication Server	Authentication Server	Authentication Server	Authentication Server
SM	SM	SM	SM
Authentication Server+SM	Authentication Server	Authentication Server, then SM	Authentication Server, then SM

Note

Where Authentication Server, then SM is the indication, parameters for which Authentication Server does not send values are obtained from the SM. This is the case where the Authentication Server is operating on an Authentication Server release that did not support the feature. This is also the case where the feature enable/disable flag in Authentication Server is set to disabled. The values are those previously set or, if none ever were, then the default values.

Where Authentication Server is the indication, values in the SM are disregarded.

Where SM is the indication, values that Authentication Server sends for the SM are disregarded.

For any SM registered under an AP with Authentication Mode set to something other than **DISABLED**, the listed settings are derived as shown in below table.

Table 83: MIR, VLAN, HPC, and CIR Configuration Sources, Authentication Disabled

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	VLAN Values	Data Channel Count per SM	CIR Values
Authentication Server	AP	AP		
SM	SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM	SM

Note

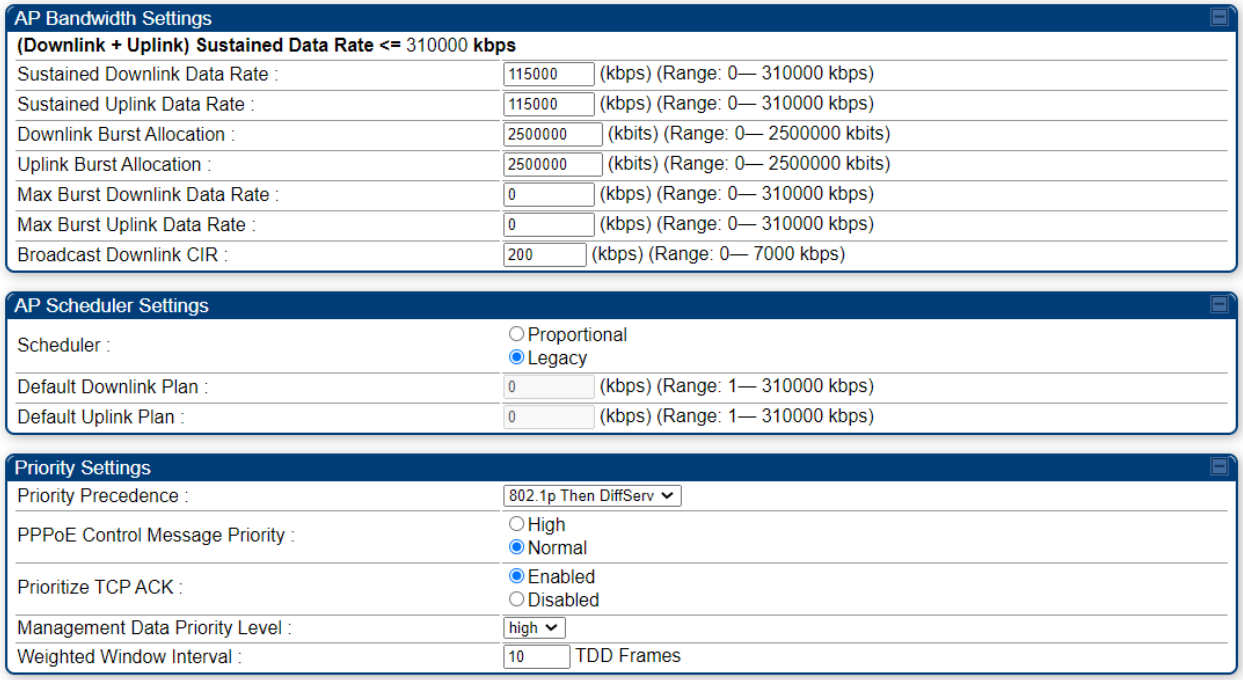
For the case where configuration source is set to Authentication Server, the Data Channel Count per SM, and the CIR values for those data channels, is defaulted to Low Priority data Channel only with no CIR's configured.

Configuring Quality of Service (QoS)

Quality of Service (QoS) page of AP

The QoS page of AP is explained in below table.

Table 84: QoS page attributes - AP



SM Prioritization Configuration	
SM Prioritization Low Group Count :	0 (0%)
SM Prioritization High Group Count :	0 (0%)
SM Prioritization :	◉ Enabled ○ Disabled
Low Prioritization Allocation :	50 %
High Prioritization Allocation :	50 %
Note: SM Prioritization is not applicable for proportional scheduler	

Weighted Fair Queuing Configuration	
Data Channel Count - Low Priority :	0 (0%)
Data Channel Count - Medium Priority :	0 (0%)
Data Channel Count - High Priority :	0 (0%)
Data Channel Count - Ultra High Priority :	0 (0%)
Weighted Fair Queuing :	◉ Enabled ○ Disabled
WFQ Configuration (SM Prioritization Low Group) :	**Valid**
Data Channel Allocation - Broadcast/Multicast :	4 %
Data Channel Allocation - Low Priority :	24 %
Data Channel Allocation - Medium Priority :	24 %
Data Channel Allocation - High Priority :	24 %
Data Channel Allocation - Ultra High Priority :	24 %
WFQ Configuration (SM Prioritization High Group) :	**Valid**
Data Channel Allocation - Low Priority :	25 %
Data Channel Allocation - Medium Priority :	25 %
Data Channel Allocation - High Priority :	25 %
Data Channel Allocation - Ultra High Priority :	25 %

Speed Test Prioritization	
Speed Test Server IP :	0.0.0.0 *Set 0.0.0.0 to disable*

Attribute	Meaning
Sustained Downlink Data Rate	Specify the rate at which the AP is replenished with credits (tokens) for transmission to each of the SMs in its sector. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings. • Configuration Source
Sustained Uplink Data Rate	Specify the rate that each SM registered to this AP is replenished with credits for transmission. This default imposes no restriction on the uplink. See • Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings • Configuration Source
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the Sustained Downlink Data Rate. See • Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings

Attribute	Meaning
	• Configuration Source
Uplink Burst Allocation	Specify the maximum amount of data to allow each SM to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. See Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings • Configuration Source
Max Burst Downlink Data Rate	These parameters allow operators to specify the data rate at which an SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Downlink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which an SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Uplink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Broadcast Downlink CIR	Broadcast Downlink CIR (Committed Information Rate, a minimum) supports system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default. Broadcast Downlink CIR is closely related to the Broadcast Repeat Count parameter, which is settable in the Radio tab of the Configuration page in the AP: when the Broadcast Repeat Count is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the Broadcast Repeat Count parameter.
Scheduler	This parameter allows the operator to either select the Proportional scheduler or the Legacy scheduler.
Default Downlink Plan	This parameter allows the operator to configure the default downlink plan. The value range for this parameter is 1 – 310000 kbps. Note: Configure this parameter when an SM is not configured with a plan or an SM is still running software older than system release 16.1.
Default Uplink Plan	This parameter allows the operator to configure the default uplink plan. The value range for this parameter is 1 – 310000 kbps. Note: Configure this parameter when an SM is not configured with a plan or an SM is still running software older than system release 16.1.
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the SM to utilize the high priority channel for PPPoE control messages. Configuring the SM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the SM.

Attribute	Meaning
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements.
Management Data Priority Level	This parameter allows to set the priority level of the VC used by Management data. Low: Management data uses low priority VC. High: Management data uses highest priority VC
SM Prioritization Low Group Count	This parameter displays the number and percentage of SMs allocated with low prioritization.
SM Prioritization High Group Count	This parameter displays the number and percentage of SMs allocated with high prioritization.
SM Prioritization	To associate a group of SMs at the same prioritization level with a guaranteed percentage of time for data to/from SMs in the group, enable this parameter. Low Prioritization Allocation and High Prioritization Allocation parameters are visible when SM Prioritization is enabled. Note: SM Prioritization is not applicable for proportional scheduler.
Low Prioritization Allocation	This parameter configures the percentage of timeslots dedicated to low prioritization group of SMs
High Prioritization Allocation	Once the Low Prioritization Allocation parameter is configured, this parameter automatically allocates the percentage of slots dedicated to high prioritization group of SMs such that the sum of parameters Low Prioritization Allocation and High Prioritization Allocation is 100%.
Data Channel Count - Low Priority	This parameter displays the percentage of time committed to transfer data to/from VCs at Low Priority QoS level.
Data Channel Count - Medium Priority	This parameter displays the percentage of time committed to transfer data to/from VCs at Medium Priority QoS level.
Data Channel Count - High Priority	This parameter displays the percentage of time committed to transfer data to/from VCs at High Priority QoS level.
Data Channel Count - Ultra High Priority	This parameter displays the percentage of time committed to transfer data to/from VCs at Ultra High Priority QoS level.
Weighted Fair Queuing	To provide a committed frame space for all QoS levels, enable this parameter.
WFQ Configuration (SM Prioritization Low Group): If the percentage of Low Priority SMs is configured as 100%, or SM Prioritization is disabled, or the WFQ feature is disabled, then the GUI displays the following set of five WFQ configuration parameters	

Attribute	Meaning
Data Channel Allocation - Broadcast/Multicast	This parameter allows to configure the percentage of frame space allocated for broadcast/multicast.
Data Channel Allocation - Low Priority	This parameter allows to configure the percentage of frame space allocated for low priority QoS level.
Data Channel Allocation - Medium Priority	This parameter allows to configure the percentage of frame space allocated for medium priority QoS level.
Data Channel Allocation - High Priority	This parameter allows to configure the percentage of frame space allocated for high priority QoS level.
Data Channel Allocation - Ultra High Priority	This parameter allows to configure the percentage of frame space allocated for ultra high priority QoS level.
WFQ Configuration (SM Prioritization High Group): If SM Prioritization is enabled and the percentage of Low Priority SMs is configured as anything less than 100%, which means that the percentage of High Priority SMs is not 0, and the WFQ feature is enabled, then the GUI displays the WFQ Configuration (SM Prioritization Low Group) and the following set of five WFQ configuration parameters for High group.	
Data Channel Allocation - Low Priority	This parameter allows to configure the percentage of frame space allocated for low priority QoS level.
Data Channel Allocation - Medium Priority	This parameter allows to configure the percentage of frame space allocated for medium priority QoS level.
Data Channel Allocation - High Priority	This parameter allows to configure the percentage of frame space allocated for high priority QoS level.
Data Channel Allocation - Ultra High Priority	This parameter allows to configure the percentage of frame space allocated for ultra high priority QoS level.
Speed Test Server IP	This feature allows AP to prioritize traffic to/from a unique IP address . AP prioritizes any packets to/from a unique IP address in the downlink direction.

Quality of Service (QoS) page of SM

The QoS page of SM is explained in below table.

Figure 53: *QoS page attributes - SM*

MIR Bandwidth Settings

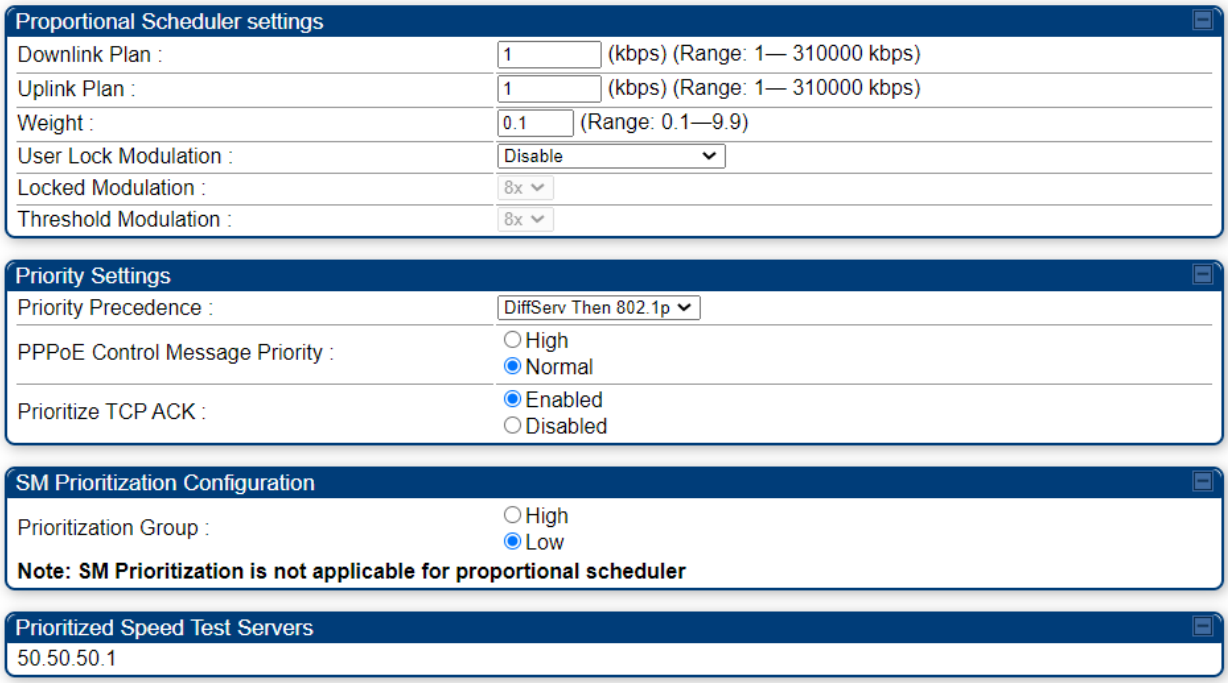
(Downlink + Uplink) Sustained Data Rate <= 310000 **kbps**

Sustained Downlink Data Rate :	155000 (kbps) (Range: 0— 310000 kbps)
Sustained Uplink Data Rate :	155000 (kbps) (Range: 0— 310000 kbps)
Downlink Burst Allocation :	2500000 (kbits) (Range: 0 — 2500000 kbits)
Uplink Burst Allocation :	2500000 (kbits) (Range: 0 — 2500000 kbits)
Max Burst Downlink Data Rate :	0 (kbps) (Range: 0— 310000 kbps)
Max Burst Uplink Data Rate :	0 (kbps) (Range: 0— 310000 kbps)
Enable Broadcast/Multicast Data Rate :	○ Enabled ◉ Disabled
Broadcast/Multicast Uplink Data Rate :	Kbps 310000 (Range: 1— 310000 kbps/65535 pps)

Data Channel Priority Settings

Number of Data Channels :	4 - Low, Medium, High, Ultra High
Low Priority Channel Configuration :	
Low Priority Channel :	Enabled
Low Priority Downlink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Low Priority Uplink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Medium Priority Channel Configuration :	
Medium Priority Channel :	Enabled
Medium Priority Downlink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Medium Priority Uplink CIR :	0 (kbps) (Range: 0— 65534 kbps)
High Priority Channel Configuration :	
High Priority Channel :	Enabled
High Priority Downlink CIR :	0 (kbps) (Range: 0— 65534 kbps)
High Priority Uplink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Ultra High Priority Channel Configuration :	
Ultra High Priority Channel :	Enabled
Ultra High Priority Downlink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Ultra High Priority Uplink CIR :	0 (kbps) (Range: 0— 65534 kbps)

Note: CIR values are not applicable for proportional scheduler



Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings • Configuration Source
Sustained Downlink Data Rate	Specify the rate at which the AP is replenished with credits (tokens) for transmission to this SM. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings • Configuration Source
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the Sustained Downlink Data Rate with transmission credits. See Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings • Configuration Source
Uplink Burst Allocation	Specify the maximum amount of data to allow this SM to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. See Maximum Information Rate (MIR) Parameters • Interaction of Burst Allocation and Sustained Data Rate Settings • Configuration Source

Attribute	Meaning
Max Burst Downlink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Downlink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the Sustained Uplink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.
Enable Broadcast / Multicast Data Rate	This parameter allows the operator to specify if Broadcast and Multicast data is rate-limited. This data rate can be entered in Kbps or PPS (Packets Per Second).
Broadcast / Multicast Data Rate	This parameter allows the operator to specify a data rate at which Broadcast and Multicast traffic is sent via the radio link.
Number of Data Channels	This parameter allows the operator to specify the number of priority channels to be used for data transmission which is configurable from 1 to 4. • 1: Select 1 to enable Low Priority channel. • 2: Select 2 to enable Low and High Priority channels. • 3: Select 3 to enable Low, Medium, and High Priority channels. • 4: Select 4 to enable all channels. For each enabled channel, configure the respective Downlink CIR and Uplink CIR.
Low Priority Channel	This parameter shows whether low priority data channel is enabled or not. Its value is derived based on the number of data channels selected. This parameter is enabled by default.
Low Priority Downlink CIR	This field indicates the minimum rate at which low priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) Note: CIR values are not applicable for proportional scheduler.
Low Priority Uplink CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) Note: CIR values are not applicable for proportional scheduler.
Medium Priority Channel	This parameter shows whether medium priority data channel is enabled or not. Its value is derived based on the number of data channels selected.

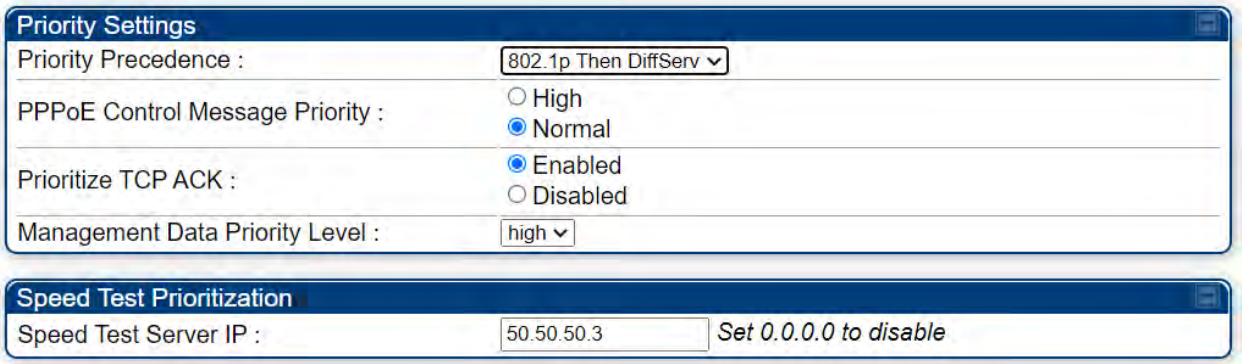
Attribute	Meaning
Medium Priority Downlink CIR	This field indicates the minimum rate at which medium priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note:** CIR values are not applicable for proportional scheduler.
Medium Priority Uplink CIR	This field indicates the minimum rate at which medium priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note:** CIR values are not applicable for proportional scheduler.
High Priority Channel	This parameter shows whether high priority data channel is enabled or not. Its value is derived based on the number of data channels selected.
High Priority Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note**: CIR values are not applicable for proportional scheduler.
High Priority Uplink CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) Note: CIR values are not applicable for proportional scheduler.
Ultra High Priority Channel	This parameter allows the operator to enable or disable one of the data channels with the highest priority bandwidth.
Downlink Plan	This parameter allows the operator to configure the default downlink plan. The value range for this parameter is 1 – 310000 kbps.
Uplink Plan	This parameter allows the operator to configure the default uplink plan. The value range for this parameter is 1 – 310000 kbps.
Weight	This parameter ranges from 0.1 to 9.9 to prioritize SM services. This is a scaling factor to be applied to the Downlink and Uplink plan. Note: There is only one weight used for a plan in both directions. The default value for this parameter is 1.0.
User Lock Modulation	This parameter contains the following three modes. Disable: When disabled, the Proportional scheduler allocates resources to meet the configured plan. When there is congestion, the Proportional scheduler allocates a reduced value proportional to the other plans regardless of the modulation. If the modulation of one SM degrades, the resources allocated to meet this SM's plan increases, affecting the overall sector capacity. The reduced capacity is divided among all SMs proportional to their plans affecting all SMs.

Attribute	Meaning
	Enable: When enabled, the Locked Modulation drop-down list is enabled supporting values from 1x to 8x. Enable Below Threshold: When enabled, the Threshold Modulation drop-down list is enabled supporting values from 2x to 8x. In this mode, the proportional scheduler behaves as per the Disabled mode until SM's modulation is above the configured Threshold Modulation. If the modulation goes below the Threshold Modulation, then proportional scheduler behaves as per the Enabled mode using the Threshold Modulation as Locked Modulation.
Locked Modulation	Using Locked Modulation, the proportional scheduler guarantees an amount of resources required to transfer data corresponding to the configured plan. If the SM's modulation decreases, the resource allocation is not changed but the SM's throughput is reduced which is no longer proportional to the configured plan. Therefore, the SM's plan is scaled down proportional to the reduced modulation resulting in not affecting other SMs' throughput based on one SM's modulation degrading.
Threshold Modulation	Using Threshold Modulation, if one SM's modulation degrades, then all other SMs' throughputs are affected as long as the degraded modulation is above the threshold. Once the modulation goes below the threshold, the reaources are no longer increased for that SM, effectively capping the effect to other SMs.
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the SM to utilize the high priority channel for PPPoE control messages. Configuring the SM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the SM.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to Disabled.
Prioritization Group	This parameter allows to configure the SM with high or low prioritization.
Prioritized Speed Test Servers	This feature allows SM to prioritize traffic to a unique IP address. SM prioritizes any packets to a unique IP address in the uplink direction. SMs learn the Speed Test server's IP address from the AP.

Quality of Service (QoS) page of BHM

The QoS page of BHM is explained in below table.

Table 85: QoS page attributes - BHM

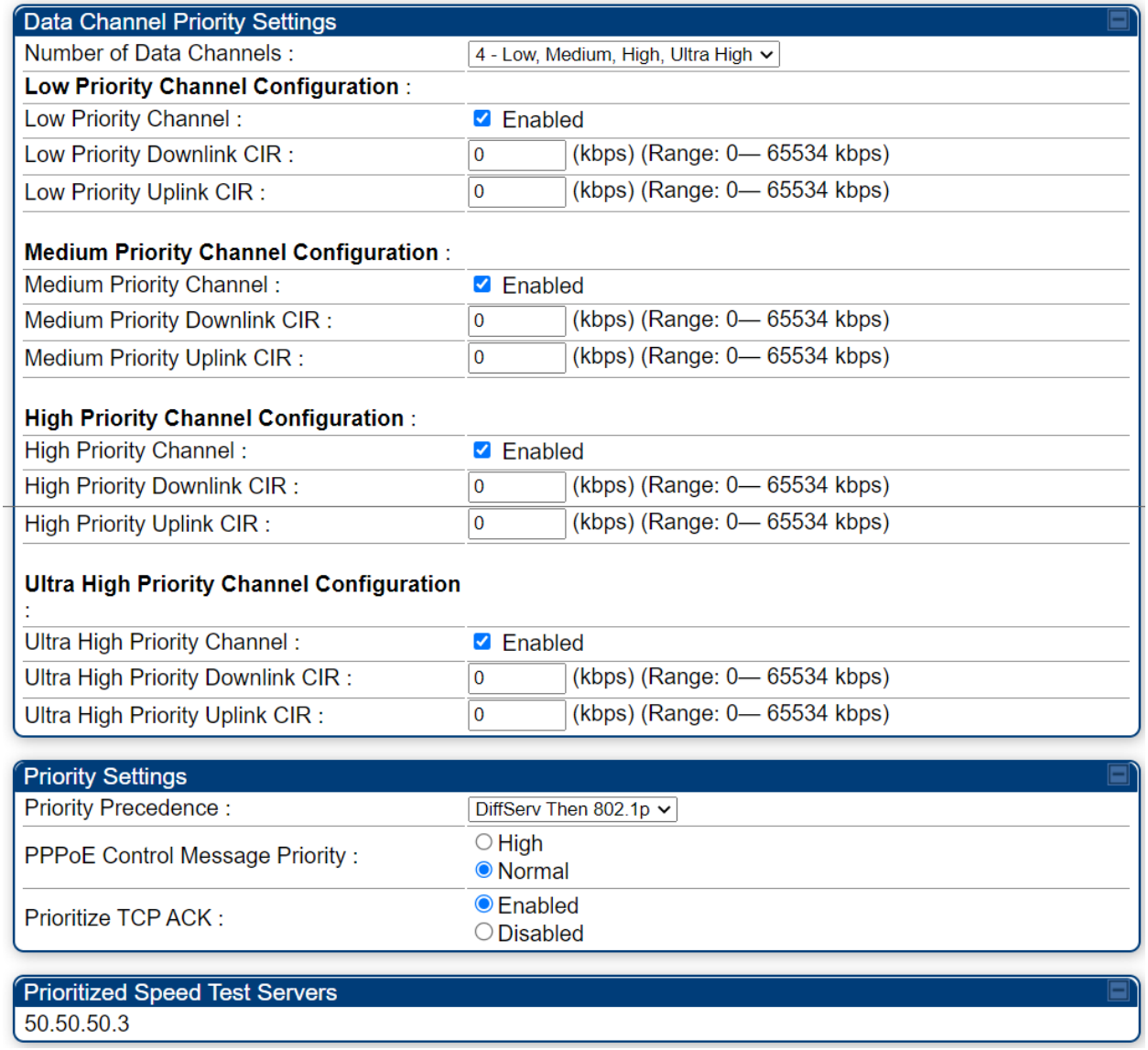


Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHM to utilize the high priority channel for PPPoE control messages. Configuring the BHM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to Disabled.
Management Data Priority Level	This parameter allows to set the priority level of the VC used by Management data. Low: Management data uses low priority VC. High: Management data uses highest priority VC
Speed Test Server IP	This feature allows BHM to prioritize traffic from a unique IP address. BHM prioritizes any packets from a unique IP address in the downlink direction.

Quality of Service (QoS) page of BHS

The QoS page of BHS is explained in below table.

Table 86: QoS page attributes - BHS



Attribute	Meaning
Number of Data Channels	This parameter allows the operator to specify the number of priority channels to be used for data transmission which is configurable from 1 to 4. • 1: Select 1 to enable Low Priority channel. • 2: Select 2 to enable Low and High Priority channels. • 3: Select 3 to enable Low, Medium, and High Priority channels. • 4: Select 4 to enable all channels. For each enabled channel, configure the respective Downlink CIR and Uplink CIR.

Attribute	Meaning
Low Priority Channel	This parameter shows whether low priority data channel is enabled or not. Its value is derived based on the number of data channels selected. This parameter is enabled by default.
Low Priority Downlink CIR	This field indicates the minimum rate at which low priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note**: CIR values are not applicable for proportional scheduler.
Low Priority Uplink CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note**: CIR values are not applicable for proportional scheduler.
Medium Priority Channel	This parameter shows whether medium priority data channel is enabled or not. Its value is derived based on the number of data channels selected.
Medium Priority Downlink CIR	This field indicates the minimum rate at which medium priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note:** CIR values are not applicable for proportional scheduler.
Medium Priority Uplink CIR	This field indicates the minimum rate at which medium priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note:** CIR values are not applicable for proportional scheduler.
High Priority Channel	This parameter shows whether high priority data channel is enabled or not. Its value is derived based on the number of data channels selected.
High Priority Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note**: CIR values are not applicable for proportional scheduler.
High Priority Uplink CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) **Note**: CIR values are not applicable for proportional scheduler.

Attribute	Meaning
Ultra High Priority Channel	This parameter allows the operator to enable or disable one of the data channels with the highest priority bandwidth.
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the BHS to utilize the high priority channel for PPPoE control messages. Configuring the BHS in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to Disabled.
Prioritized Speed Test Servers	This feature allows BHS to prioritize traffic to a unique IP address. BHS prioritizes any packets to a unique IP address in the uplink direction. BHS learn the Speed Test server's IP address from the BHM.

Citizens Broadband Radio Service (CBRS)

Citizens Broadband Radio Service subscription for the CBRS-compliant devices in 3.6 GHz band (3550 MHz to 3700 MHz).

Note

Assuming the user follows the Cambium recommended procedures for using the CBRS cnMaestro Management tool and then syncing those parameters to the radio, nothing at all needs to be set by the operator directly on this Configuration CBRS radio page. All of this will be pushed or pulled from cnMaestro. Definitions are being included for completeness.

PMP 450 Series AP/BHM - CBRS configuration

PMP 450 series CBRS configuration page of AP/BHM is explained in the below table:

Table 87: PMP 450Series AP/BHM - CBRS Configuration

Attribute	Meaning
Citizen Broadband Radio Service	Enable/Disable the CBRS operation until the device is valid.
Log Level	Log level can be increased to Debug or decreased to Error level accordingly and logs will appear. • Debug: Logs used to help in debugging. • Info:Logs the message correspond to normal applicationbehavior. • Error:Logs the issues thataffect the usage orperformance ofthesystem.
Reboot for Channel Bandwidth Change	This attribute applies only the 450m AP. System Release 20.2's multigrant feature supports automatic bandwidth changes as individual multigrants are terminated or suspended or authorized. Disabling this flag will prevent the 450m from automatically making these bandwidth changes on the fly. The 450m is the only Cambium AP that requires a reboot to apply a bandwidth change.
Alternate Channel Selection	This CBRS feature flag enables the AP to automatically search for new channels for the sector to operate on when the existing channels are suspended due to DPA activation, or terminated without a suggested EIRP to use from the SAS.

Attribute	Meaning
	For PMP 450m operators that wish to avoid unexpected reboots due to grant terminations or suspensions, this feature flag could be left enabled, while the **Reboot for Channel Bandwidth Change** flag is disabled. Then, if some or all of the multigrants held by the AP are suspended or terminated, an alternate channel selection (channel hunt) is triggered, but only to channels of the same operating bandwidth. This avoids the potential of an unexpected reboot, but at the possible risk of no such channel being found, in which case the AP will remain off the air until a suspension is automatically cleared or operator action is taken. Additionally, a channel hunt to a channel of the same bandwidth may result in poorer performance than a channel hunt to a cleaner channel of smaller bandwidth.
Change Channel if Only SMs are Impacted	When enabled, this feature allows the AP to automatically find and move to a new channel or decrease the bandwidth, when more than the **SM Percentage Threshold for Channel Change** percentage of SMs have been impacted by termination or suspension, even though the AP itself has not been impacted. Not applicable for PTP configurations.
SM Percentage Threshold for Channel Change	Displays the percentage of SMs that need to be impacted by termination or suspension for the feature to be invoked, even though the AP itself has not been impacted. Note that the **Alternate Channel Selection** feature must also be enabled for the AP to hunt for a new channel due to the **Change Channel if SMs are Impacted** feature. If an operator elects to run with **Alternate Channel Selection** enabled but **Change Channel if SMs are impacted** feature is disabled, the AP still performs automatic channel selection, but only in cases where the AP is directly impacted by terminations or suspensions. If the **Alternate Channel Selection** feature is disabled, but the **Change Channel if SMs are Impacted** feature is enabled, if enough SMs are impacted by terminations or suspensions, the AP still reduces the Bandwidth if authorized grants are available, but it will not hunt for a new channel. Not applicable for PTP configurations.
Original Channel Restore Time	When this feature is triggered via SM suspensions, the AP continues to heartbeat the original channels for itself and all the SMs, while operating on the temporary channels or reduced bandwidth for at least this length of a period after moving to these temporary channels or reducing bandwidth. When this timer expires, the AP can move back to the original channels and/or bandwidth if enough suspended SMs have become authorized on the original channels. Not applicable for PTP configurations.
User ID	User ID assigned by SAS is part of the Registration request message
Include User ID	For operators using Federated Wireless or Commscope SAS, this option will be available and set to Enabled by default. By appending it to the Co-Existence parameters sent to the SAS, it seperates and allows the SAS to handle the possibility of 2 operators accidently picking the same CoExistence parameters. If an operator wishes to frequency coordinate on the same channel with another operator or between PMP and LTE technology, this parameter can be disabled and the Co-Existence group parameters set the same - coordinated. For Google, these parameters are unique to an organization, so this parameter is not available for operators using Google SAS. See Cambium 20.3 training slides for more information.

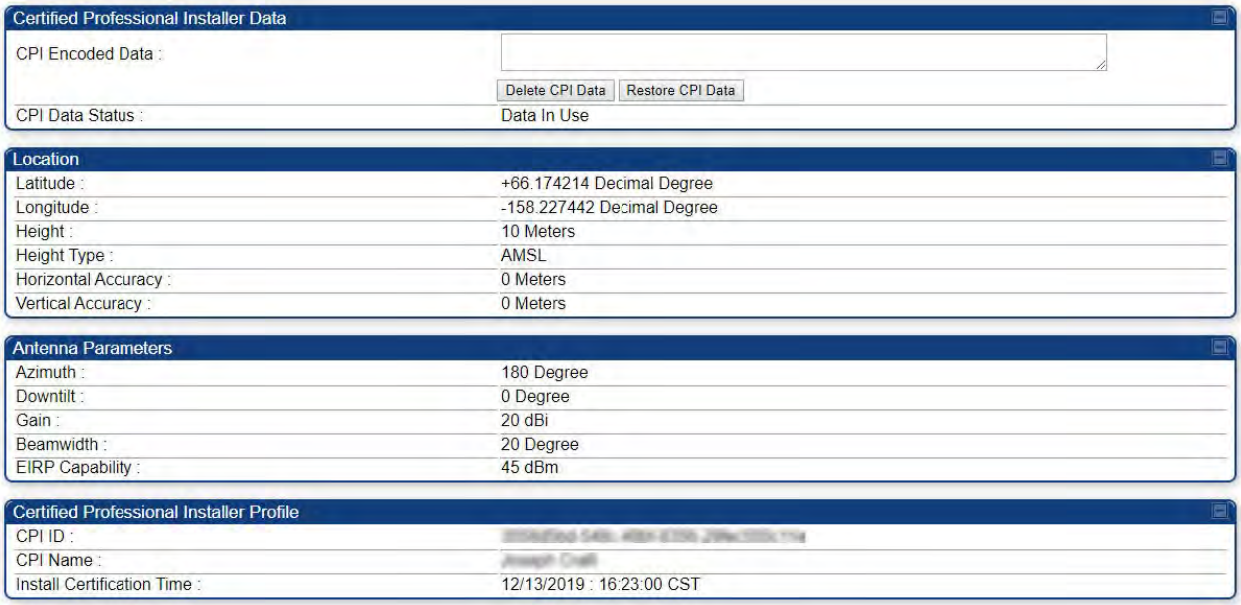
Attribute	Meaning
Coexistence Sector ID	This parameter is also known as the identifier of a Common Channel Group (CCG) in CBRS Alliance or Principal Subordinate Single Frequency Group (SFG) in WinnForum Release 2 . The Google SAS portal currently calls it "Same Frequency" in the Frequency Management subsection of the per-device Configuration Tab as well as at the top of the per-device Coex tab. Although this can be edited, it defaults to the MAC address of the AP/BHM of this sector. The purpose of the sector ID is, it helps the SAS identify which SM's are grouped with a particular AP (same frequency and bandwidth as the AP).
Coexistence Spectrum Reuse ID	This parameter defines a CBRS interference coordination group. It is called Spectrum Reuse in WInnForum Release 2, or Interference Coordination Group (ICG) in CBRS Alliance. The Google SAS portal urrently calls it "Frequency Reuse" in the Frequency Management subsection of the per-device Configuration tab as well as at the top of the per-device Coex tab. Multiple sectors can be assigned the same Reuse ID. ASAS will not attempt to coordinate interference between devices using the same Reuse ID. For example, an operator using 2 non-overlapping center frequencies in what is typically called an ABAB deployment could assign 1 Reuse ID to all sectors using center frequency "A", and a second Reuse ID to all sectors using center frequency "B".
CPI Encoded Data	CPI information is the set of encoded installation parameters by CPI and the signed installation parameter provided by the CPI. It receives the parameter with a registration message from the SAS. • Delete CPI Data: CPI data can be deleted by selecting the Delete CPI Data. • Restore CPI Data: CPI data can be restored by selecting the Restore CPI Data.
CPI Data Status	Displays the status of the CPI data is in use or unchanged.
Latitude	Displays latitude of the device location in degrees.
Longitude	Displays longitude of the CBSD antenna location in degrees.
Height	Displays device antenna height in meters.
Height Type	Should be AGL or AMSL as follows: • AGL height is measured relative to the ground level. • AMSL height is measured relative to the mean sea level.
Horizontal Accuracy	Displays positive number in meters to indicate the accuracy of the device antenna horizontal location.
Vertical Accuracy	Displays positive number in meters to indicate the accuracy of the device antenna vertical location.
Azimuth	Displays Boresight direction of the horizontal plane of the antenna in degrees with respect to true north.
Downtilt	Displays the antenna down tilt in degrees.
Gain	Integrated antenna gain: Peak gain of the integrated antenna. External antenna gain: peak gain of the external antenna connected to a device.

Attribute	Meaning
Beamwidth	Displays the beamwidth of the antenna in the horizontal plane in degrees.
EIRP Capability	Display max Effective Isotropic Radiated Power (EIPR) capability of the device.
CPI ID	The assigned CPI ID unique to the installer that is certifying the CBRS installation.
CPI Name	The entered name of the Certified professional installer.
Install Certification Time	Thetime of thecertifiedinstallation for this radio.

PMP 450 Series SM/BHS-CBRS configuration

PMP 450 series CBRS configuration page of SM/BHS is explained in the below table:

Table 88: PMP 450 Series SM/BHS_CBRS Configuration

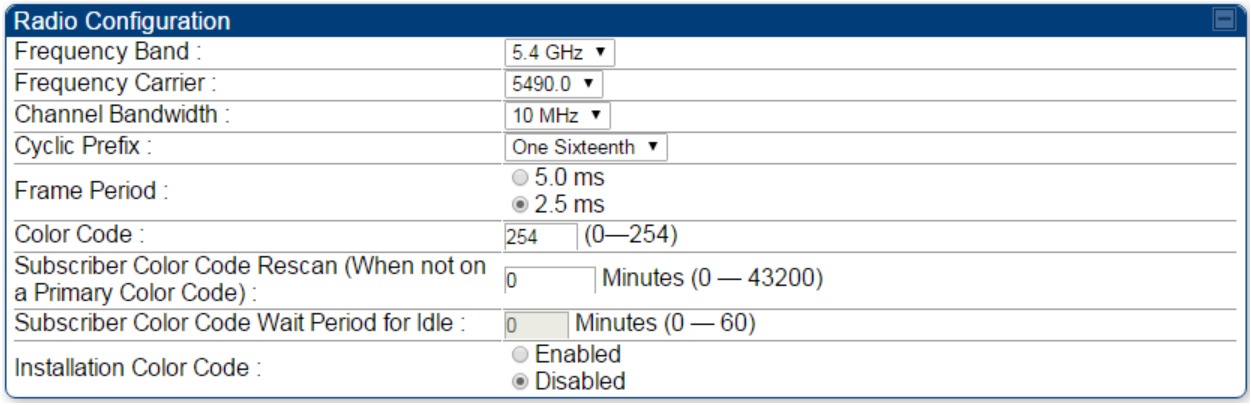


Attribute	Meaning
CPI Encoded Data	Refer table PMP 450Series AP/BHM – CBRS Configuration for parameter descriptions
CPI Data Status	
Latitude	
Longitude	
Height	
Height Type	
Horizontal Accuracy	
Vertical Accuracy	
Azimuth	
Downtilt	
Gain	
Beamwidth	
EIRP Capability	
CPI ID	
CPI Name	
Install Certification Time	

Installation Color Code

With this feature enabled on the AP and SM, operators may install and remotely configure SMs without having to configure matching color codes between the modules. While the SM is accessible for configuration from above the AP (for remote provisioning) and below the SM (for local site provisioning), no user data is passed over the radio link. When using the Installation Color Code feature, ensure that the SM is configured with the factory default Color Code configuration (Color Code 1 is “0”, Color Code 2-10 set to “0” and “Disable”). The status of the Installation Color Code can be viewed on the AP Eval web GUI page, and when the SM is registered using the Installation Color Code the message “SM is registered via ICC – Bridging Disabled!” is displayed in red on every SM GUI page. The Installation Color Code parameter is configurable without a radio reboot for both the AP and SM. If an SM is registered via Installation Color Code and the feature is then disabled, operators will need to reboot the SM or force it to reregister (i.e. using the Rescan APs functionality on the AP Eval page).

Figure 54: *Installation Color Code of AP*



Zero Touch Configuration Using DHCP Option 66

This feature allows an SM to get its configuration via DHCP option 66. This can be used for the initial configuration of an SM as well as managing the configuration of SMs on an ongoing basis. Here is how it works in brief:

- When the SM boots up, if it is set to use DHCP client, it will send out a DHCP Discover packet which includes a request for DHCP Option 66.
- In case of a brand new SM out of the box, the DHCP Discover packet is sent out if the SM connects to an AP using Installation Color Code (ICC), even though DHCP client is not enabled in factory default config.
- An appropriately configured DHCP server will respond with a DHCP Offer and include a URL in response to the Option 66 request. The URL should point to the configuration file.
- The device will download the configuration file and apply it. The device will reboot automatically if needed. (Note: this requires “rebootIfRequired” flag to be added to the config file. See Creating a Golden config file

Configuration Steps

Procedure 15 Zero Touch Configuration steps:

1	Create the golden config file(s)
2	Host it on an TFTP/FTP/HTTP/HTTPS server
3	Configure the DHCP server to return the URL of the golden config file in option 66

When the SM boots up, it will get the URL for the golden config from the DHCP server via option 66, download it and apply it.

If all the SMs are configured exactly the same, then you can create just new golden config file that can be used with all SMs.

If the SMs are not configured the same, see if it is possible to group the SMs such that SMs with the same configuration are served by the same DHCP pool. User can then create multiple golden config files and configure the DHCP server to use the appropriate config file for each pool.

User can also create one config file per SM. This provides the most flexibility, but is practical only if you have a software tool/script to generate the config files for each MAC address. The files should be named

<mac>.cfg where <mac> is the MAC address of the SM, and stored in the same directory on the file server. The DHCP server should be configured to return the directory name ending with a '/' in option 66. The SM will automatically add "<mac>.cfg" to the path and get its config file.

If some configuration is unique per SM, but rest of the configuration is common, the SMs can be staged with the unique part, and use option 66 to manage the common part. For example, if each SM needs to have its coordinates set, don't include the coordinates in the golden config file. Instead, configure the coordinates for each SM manually. Manage the rest of the configuration using DHCP option 66.

Creating a Golden config file

The easiest way to create the golden config file is to configure an SM, export its configuration and edit it. To export the configuration file from the GUI of the SM, go to "Configuration > Unit Settings" tab, go to the "Download Configuration File" section and click on the "<mac>.cfg" link. This will give you a text file in JSON format. You can edit this file in a text editor but it's easier to use a JSON editor like https://www.jsoneditoronline.org/.

Strip down the config file to remove sections and entries that don't care about, and keep only the items that require changes. If there are many required changes, it can easily get confusing. To identify the exact items changes, first reset the SM to factory default, export the config file, make the necessary changes, export a second config file, then use a tool like WinMerge (http://winmerge.org/) to identify the differences.

The config file contains the following informational entries at the top level.

"cfgUtcTimestamp": "cfgUtcTimestamp",

"swVersion": "CANOPY 15.1 SM-AES",

"cfgFileString": "Canopy configuration file",

"srcMacAddress": "0a-00-3e-a2-c2-74",

"deviceType": "5.4/5.7GHz MIMO OFDM - Subscriber Module",

"cfgFileVersion": "1.0"

The "cfgUtcTimestamp", "swVersion", "srcMacAddress" and "deviceType" lines can be deleted. Do not delete the "cfgFileString" and "cfgFileVersion" entries.

Next, create an object named "configFileParameters" at the top level. Under that, add a parameter called "rebootIfRequired" and set it to true. This tells the SM to reboot automatically if a reboot is needed to apply the new configuration.

A sample configuration file that has been edited for use via DHCP option 66 is given below.

```
{
 "userParameters": {
  "smNetworkConfig": {
   "networkAccess": 1
  },
  "location": {
   "siteName": "Test site"
  },
  "smRadioConfig": {
```

```
    "frequencyScanList": [
      5475000,
      5480000
    ],
    "colorCodeList": [
      {
        "colorCode": 42,
        "priority": 1
      }
    ]
  },
  "networkConfig": {
    "lanDhcpState": 1
  }
},
"cfgFileVersion": "1.0",
"cfgFileString": "Canopy configuration file",
"configFileParameters": {
  "rebootIfRequired": true
}
}
```


When configuration is imported, only the items that exist in the configuration file are modified. Parameters that are not in the imported file are not changed. If user wish to revert those settings to their factory default values, please add a "setToDefaults" item under "configFileParameters" section with a value of true.


```
"cfgFileVersion": "1.0",
"cfgFileString": "Canopy configuration file",
"configFileParameters": {
  "rebootIfRequired": true,
  "setToDefaults": true
}
```


In case, the SM needs to fetch the configuration file on each boot up even when not connecting to AP via ICC, set "Network Accessibility" to "Public" and "DHCP State" to "Enabled" in the "Configuration > IP" page before exporting the configuration.

Hosting the config file

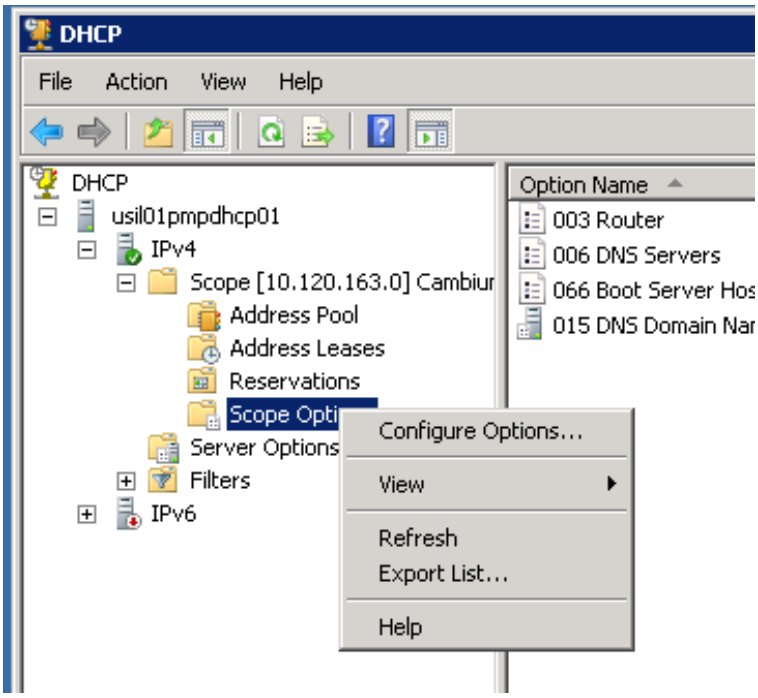
Copy the golden configuration file to an FTP, TFTP, HTTP or HTTPS server. This location can be password protected; you just have to include the user name and password in the URL.

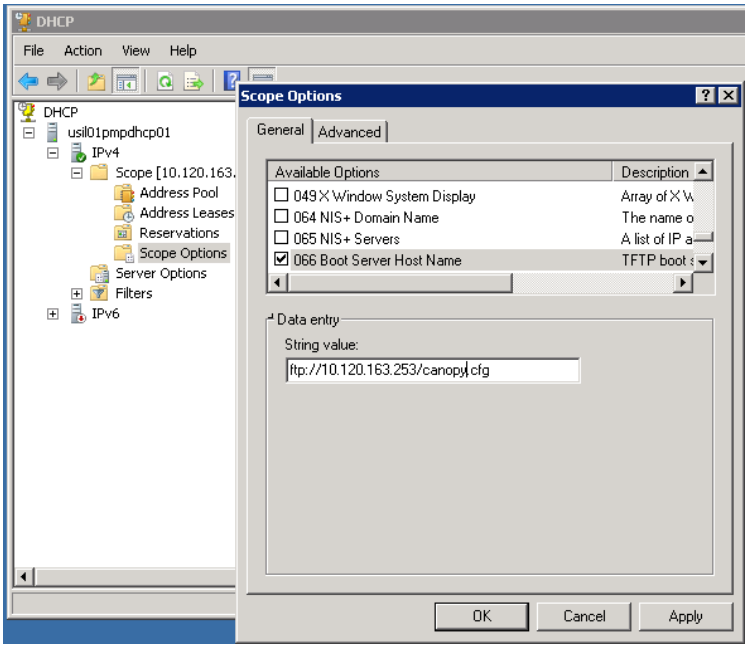
DHCP server configuration

Configure DHCP server to return the full URL to the golden config file as the value of DHCP option 66.

The following example explains how to make the change for Windows Server 2008. Adapt it to your specific DHCP server.

Procedure 16 DHCP server configuration

1	Click “Start > Administrative Tools > DHCP”
2	If you have multiple “Scopes” defined, identify the correct “Scope” that will serve IP addresses for the SMs
3	Right click on “Scope Option” under the correct “Scope” and select “Configure Options” 
4	In the “Scope Options” dialog, scroll down to “066 Boot Server Host Name”, select the checkbox and enter the full URL to the golden config file as the “String value”. Then click “OK”.

	
5	In the DHCP snap-in window, right click and “Refresh” to see the DHCP option 66 in the list of DHCP options

Supported URL Formats

FTP, TFTP, HTTP and HTTPS URLs are supported. Some examples are given below.

- ftp://10.120.163.253/canopy.cfg
- ftp://admin:admin123@10.120.163.253/canopy.cfg (login as admin with password admin123)
- tftp://10.120.163.253/canopy.cfg
- http://10.120.163.253/golden-config.cfg
- https://10.120.163.253/smconfig/golden-config.cfg

User can also specify the URL pointing to a directory and not a specific file. Terminate the URL with a ‘/’ to indicate that it is a directory and not a file. Use this format when each SM has its own individual config file. The directory should contain files named “<mac>.cfg”, one for each SM.

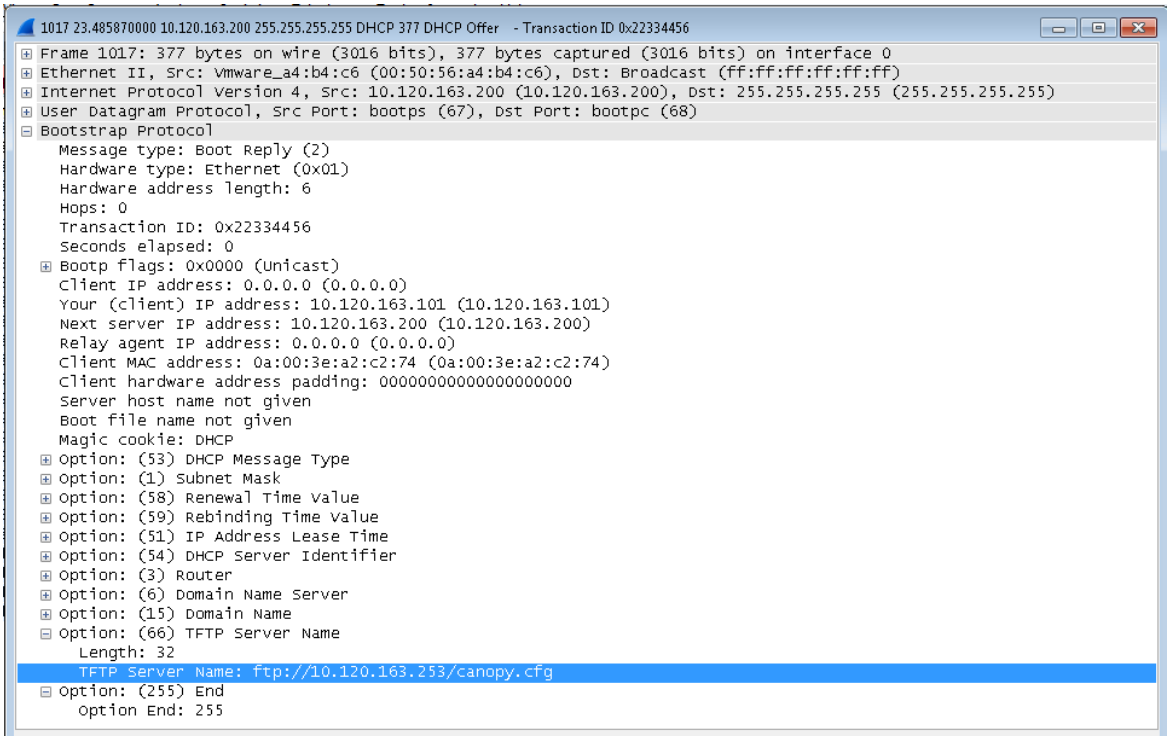
For example:

ftp://10.120.163.253/smconfig/

In this case, the SM will append “<mac>.cfg” to the path and try to get that file. For example, if the SM’s MAC address is 0a-00-3e-a2-c2-74, it will request for ftp://10.120.163.253/smconfig/0a003ea2c274.cfg. This mechanism can be used to serve individual config file for each SM.

Troubleshooting

1	Ensure that the___14 SM is running 13.3 or newer version of software.

2	If the SM has factory default config, confirm ICC is enabled on the AP, so the SM can connect to it.
3	If the SM is connecting to the AP using a color code other than ICC, make sure the SM has “Network Accessibility” set to “Public” and “DHCP State” set to “Enabled” in the “Configuration > IP” page.
4	Make sure the golden config file does not turn off “Network Accessibility” or “DHCP State”. If it does, the SM will no longer request the config file when it is rebooted.
5	Check the event log of the SM to see the status of the configuration file import including any errors that prevented it from importing the file.
6	Capture the DHCP Offer packet from the DHCP server to the SM and verify that Option 66 has the expected URL. 

```
1017 23.485870000 10.120.163.200 255.255.255.255 DHCP 377 DHCP Offer  - Transaction ID 0x22334456
⊞ Frame 1017: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface 0
⊞ Ethernet II, Src: vmware_a4:b4:c6 (00:50:56:a4:b4:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 10.120.163.200 (10.120.163.200), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x22334456
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 10.120.163.101 (10.120.163.101)
    Next server IP address: 10.120.163.200 (10.120.163.200)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 0a:00:3e:a2:c2:74 (0a:00:3e:a2:c2:74)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type
  ⊞ Option: (1) Subnet Mask
  ⊞ Option: (58) Renewal Time Value
  ⊞ Option: (59) Rebinding Time Value
  ⊞ Option: (51) IP Address Lease Time
  ⊞ Option: (54) DHCP Server Identifier
  ⊞ Option: (3) Router
  ⊞ Option: (6) Domain Name Server
  ⊞ Option: (15) Domain Name
  ⊟ Option: (66) TFTP Server Name
      Length: 32
      TFTP Server Name: ftp://10.120.163.253/canopy.cfg
  ⊟ Option: (255) End
      Option End: 255
```

Configuring Radio via config file

The 450 Platform Family supports export and import of a configuration file from the AP or SM as a text file. The configuration file is in JSON format.

To export or import the configuration file, the logged in user needs to be an ADMINISTRATOR and it must not be a “read-only” account.

The exported configuration file contains the complete configuration including all the default values. To keep a backup of the current configuration, the file can be saved as-is and imported later.

While importing a configuration file, it can be either imported the full configuration or a sparse configuration containing only the items that need to be changed. If a sparse configuration file is imported, only the items in the file will be imported. Other configuration will remain unchanged. There could also be used a special flag in the configuration file to tell the device to apply the configuration starting from factory default (ReferProcedure 19 Special Headers for configuration file).

Import and Export of config file

The config file import and export is supported in Configuration > Unit Settings page. The procedure for importing and exporting config file is explained below.

Figure 55: *Configuration File upload and download page*

The DHCP server configuration procedure is as follows:

Procedure 17 DHCP server configuration

1	Login to the GUI and go to Configuration > Unit Settings.
2	Under Download Configuration File tab, click on the “<mac>.cfg” link, where <mac> is the MAC address of the device (for example, “01003ea2c274.cfg”).
3	Save the file to the local disk.

The below procedure is to be followed for Importing a config file

Procedure 18 Import the configuration from the GUI

1	Login to the GUI and go to Configuration → Unit Settings.
2	Click on “Browse” button under “Upload and Apply Configuration File” tab and select the configuration file from disk.
3	Click “Upload” followed by “Apply Configuration File” button click.
4	The “Status of Configuration File” section will show the results of the upload.
5	Review it to make sure there are no errors. Then click on “Reboot” to reboot with the imported configuration

The special headers for config file is explained below:

Procedure 19 Special Headers for configuration file

1	A “configFileParameters” section can be added to the header to control the behavior of the device when importing configuration.

2	The “setToDefaults” when set to “true” tell the device to reset to factory default configuration and apply the configuration in the file on top of that. So any attribute not in the configuration file will be set to its factory default value. By default, the configuration in the file is merged with the existing configuration on the device.
	
	The “rebootIfRequired” flag when set to “true” tell the device to reboot automatically if needed to apply the configuration change. By default, the device will not reboot automatically.
	
	{
	“cfgFileString”: “Canopy configuration file”,
	“cfgFileVersion”: “1.0”,
	“configFileParameters”: {
	“setToDefaults”:true,
	“rebootIfRequired”:true,
	}
	}

Configuring cnMaestro™ Connectivity

450 Platform Family network can be onboarded, configured and managed using cnMaestro™ Cloud or On Premises Server.

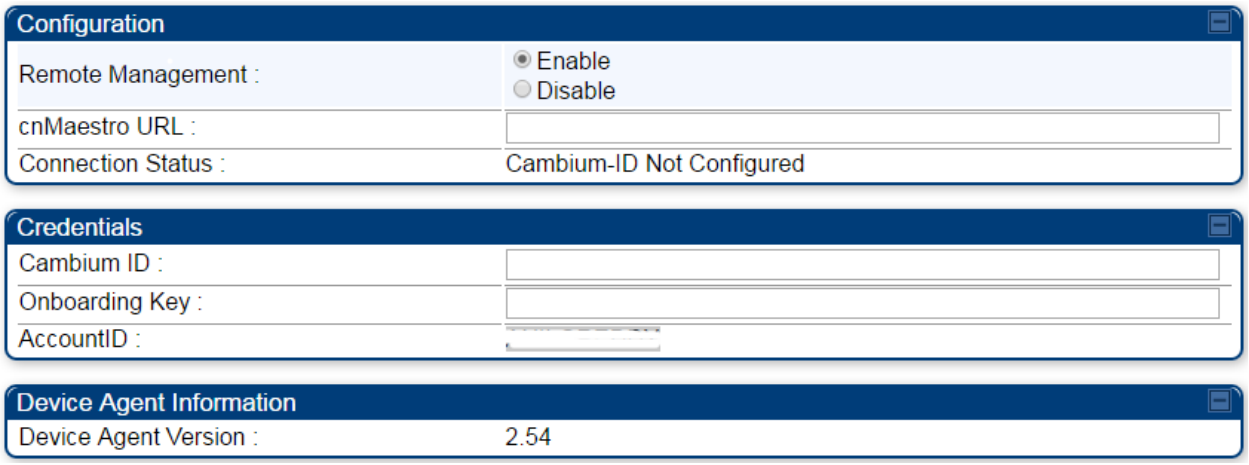
Onboarding

Onboarding can be done in one of several ways:

- Using Cambium ID and Onboarding key
- Using Manufacturer’s Serial Number (Only if it starts with an “M” and is 12 characters long)
- On Premises Zero Touch onboarding of AP/SM using DHCP option 43 and 15
- PMP SM Zero touch onboarding to the cnMaestro server where PMP AP is onboarded.

To configure the PMP devices, enable Remote Management under Configuration->cnMaestro as shown in below figure.

Figure 56: *Configuring cnMaestro*

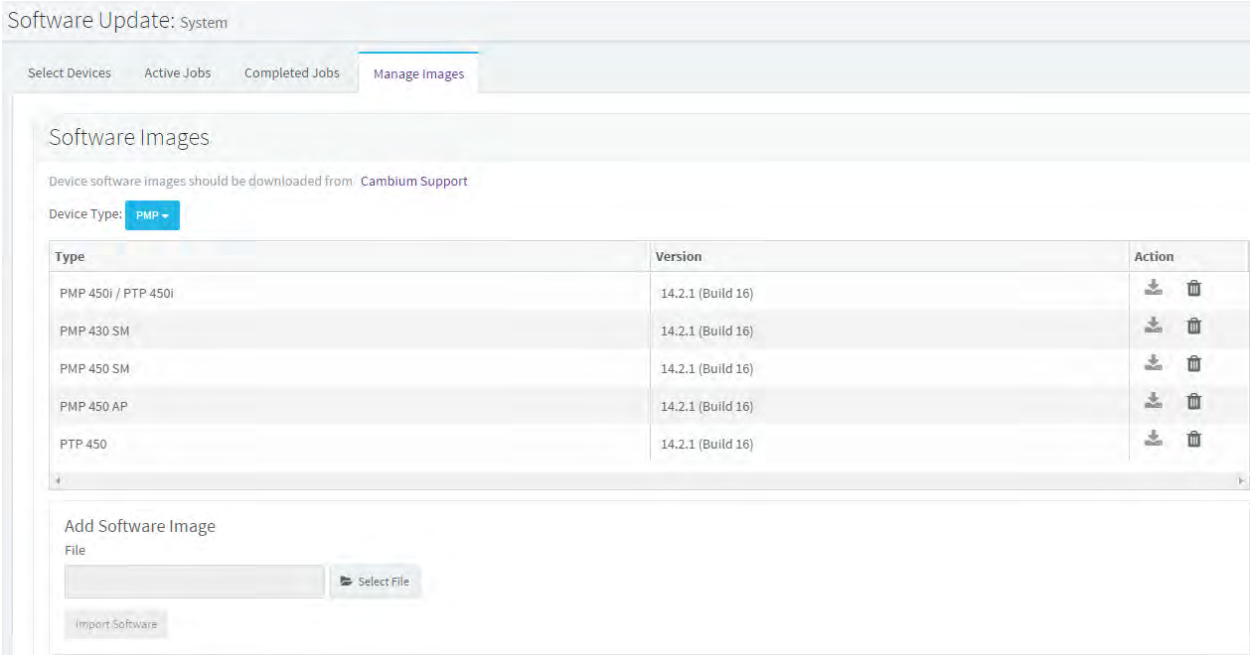


Attribute	Meaning
Remote Management	This field enables/disables remote management of 450 Platform Family products.
cnMaestro URL	This field allows to enter cnMaestro URL e.g. https://cloud.cambiumnetworks.com Or cnMaestro on premises URL
Connection Status	This field indicates cnMaestro connectivity status.
Cambium ID	This field allows to enter Cambium ID for onboarding 450 Platform devices.
Onboarding Key	This field allows to enter Onboarding Key for onboarding.
AccountID	This field indicates Account ID of the customer.
Device Agent Version	This field shows device agent version.

Prerequisites for onboarding to cnMaestro™

- Devices types must be PMP 450m Series, PMP/PTP 450 Series, PMP/PTP 450i/450b Series or PMP 430 Series SMs (interoperability mode only).
- Minimum required software version of 14.2.1. Device software images can be downloaded from http://support.cambiumnetworks.com or from the On Premises cnMaestro server by navigating to Operate >Software Update->Manage Images. Select
- Device type to display the available images and then click the download icon as shown in below figure.

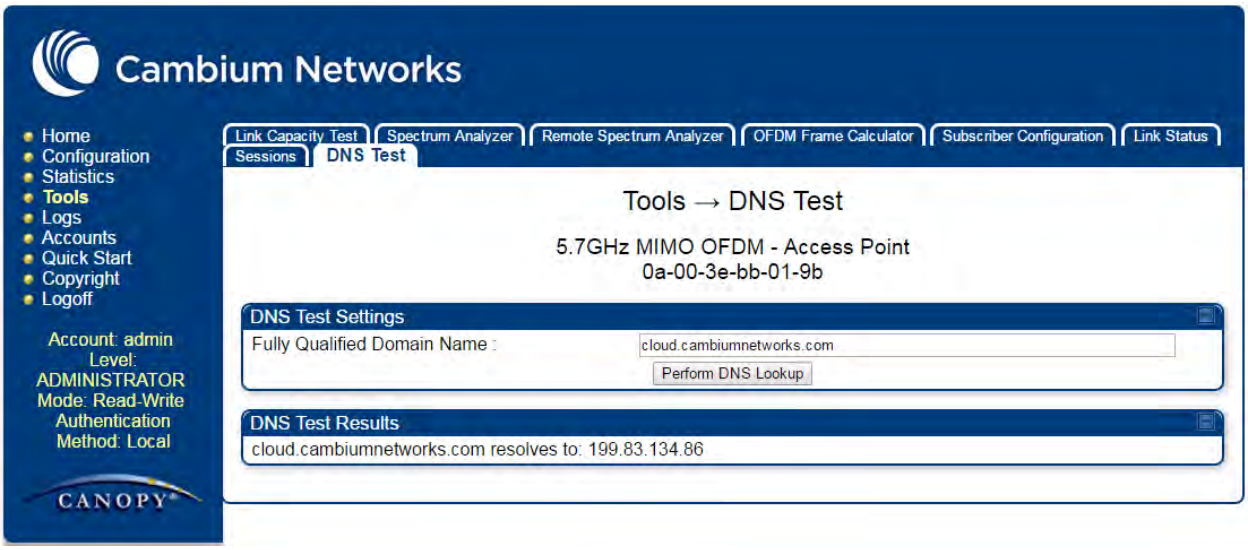
Figure 57: *Software Upgrade from cnMaestro™*



- IP connectivity between PMP Device and the cnMaestro server is established. Ensure Port 443 is open in the firewall as this port is used for secure communication between the PMP device and the cnMaestro server through web sockets. In addition, if the PMP device and cnMaestro™ server are on different subnets, proper routes should be established for communication.

- For PMP AP, a valid DNS setting is required so that the AP will be able to resolve the cnMaestro URL. DNS settings can be verified by performing a DNS lookup under Tools->DNS Test on the AP as shown in below figure.

Figure 58: *DNS Test for cnMaestro™ connectivity*



- If the SM is in Bridge mode, then LAN1 must have public equestility with a public IP assigned and corresponding DNS setting.
- If the SM is in NAT mode, then Remote Management should be enabled with the standalone configuration option and DNS settings.

Knowledge Based articles for onboarding

For onboarding the devices to cloud server and troubleshooting the onboarding issues in cloud server please see the following link:

http://community.cambiumnetworks.com/t5/cnMaestro/Device-On-boarding/td-p/51484

For onboarding the devices to on Premises server and configuring the DHCP server options for on boarding please see the following link:

http://community.cambiumnetworks.com/t5/cnMaestro/Device-Onboarding-and-Linux-DHCP-Options-for-cnMaestro-On/m-p/55187#U55187

Order of Device Onboarding

The device discovery order is as follows in On Permises cnMaestro™ Server. If any of the options is not configured, the discovery method will fallback to the next option:

1. Static cnMaestro URL
2. Zero Touch token (on boarding of PMP SMs when the corresponding AP is on boarded)
3. DHCP Option 43
4. DHCP Option 15
5. https://cloud.cambiumnetworks.com

Device Agent Logs

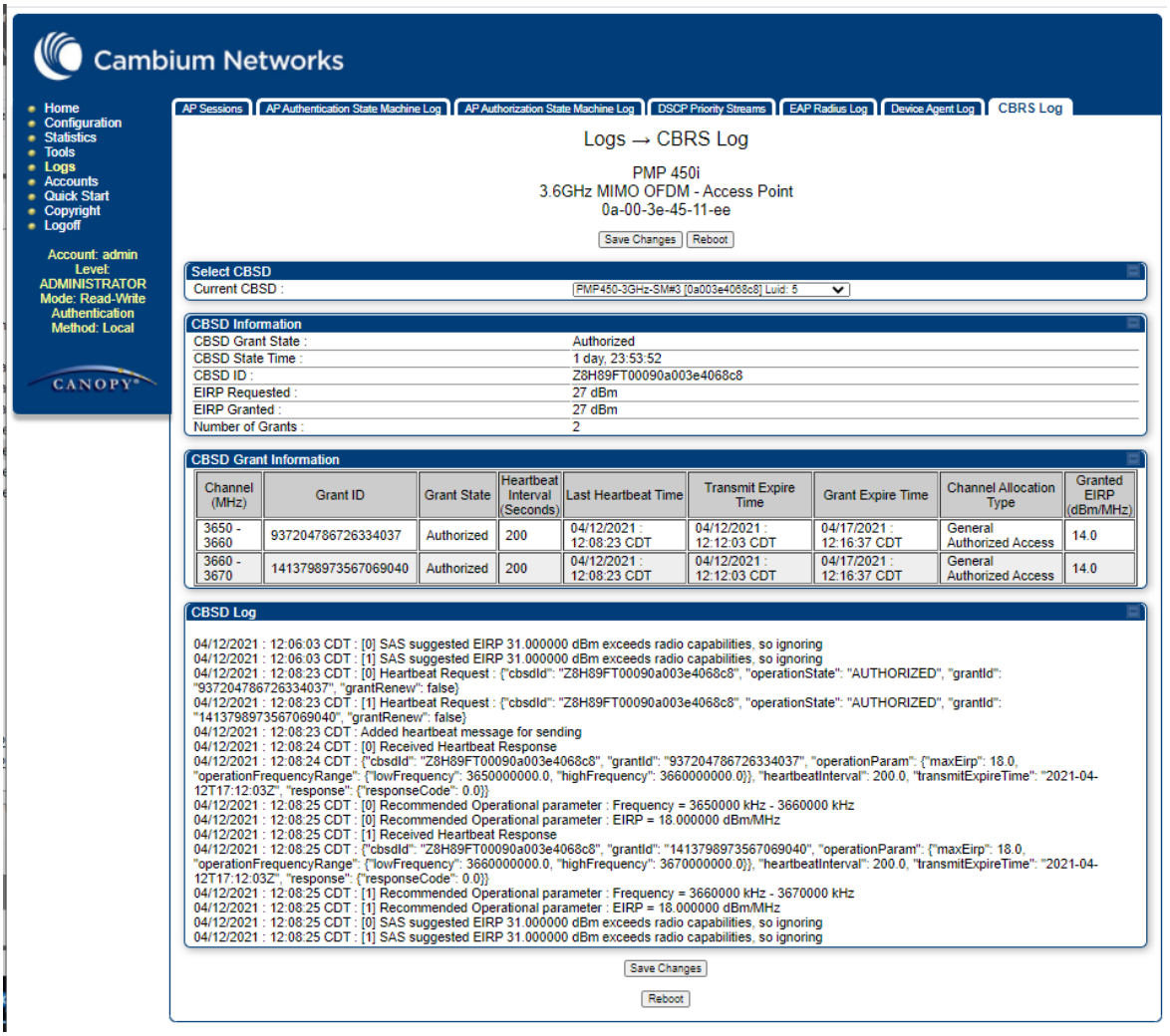
For debugging any onboarding issues please check the device agent logs by navigating to Logs->Device Agent Logs on the PMP device GUI as shown in Device Agent Logs. In addition, a tech support dump can for the PMP device can be obtained from cnMaestro™ by navigating to Monitor->Tools menu after selecting the particular PMP device in the tree and clicking the tech support file icon. This can be send to Cambium support for further troubleshooting.

Figure 59: *Device Agent Logs*

CBRS Log

The CBRS Log page shows detailed information on each CBRS grant per device. Only 1 device is shown on the page at a time. The device can be selected in the "Current CBSD" pull down as shown in the figure below.

Figure 60: *CBRS Log*



Monitoring Tools for PMP Devices on cnMaestro™

cnMaestro™ as of this release offers several debugging tools for PMP devices. Some examples are:

- Pictorial view of network hierarchy
- Device status
- Tech support file
- Throughput
- Alarms

- Reboot
- Debug Logs
- Network connectivity – ping and DNS lookup

Figure 61: *Example cnMaestro™ screenshot*

For more information on these tools please see

http://community.cambiumnetworks.com/t5/cnMaestro/How-to-use-the-cnMaestro-Tools-for-Troubleshooting-Device-or/m-p/54503#U54503

Zero Touch on boarding of the PMP SMs when the corresponding AP is on boarded

First a link should be established between the PMP AP and SM either by configuring manually or using the ICC. Once the AP and SM link is established, the AP must be onboarded to cnMaestro™ using one of several ways detailed above under the Onboarding section. Once the AP is onboarded to cnMaestro™ Cloud or On premises cnMaestro™server, the SMs under the AP will automatically onboard to cnMaestro™ using a Zero touch token that is communicated between the AP and SMs. This is applicable to existing SMs registered to the AP as well as new SMs registering to the AP for the first time. The SMs appear on the onboarding queue of cnMaestro™ and the operator must "Approve" the devices in order to manage them.

The following operations for PMP Devices are available on cnMaestro™:

- Monitor the device details in the Dashboard page by navigating to the Monitor > Dashboard menu and selecting the PMP AP/SM in the tree.
- Monitor notifications related to the PMP AP/SM by navigating to the Monitor > Notifications Menu and selecting the PMP AP/SM in the tree.
- Monitor device statistics on the statistics page by navigating to the Monitor > Statistics menu and selecting the PMP AP/SM in the tree, then selecting the PMP AP or PMP SM in the Device type dropdown.
- Monitor Performance graphs related to the PMP AP/SM by navigating to the Monitor > Performance menu and selecting the required performance graph (i.e Throughput, SMs,

Modulation) and selecting the PMP AP/SM in the tree.

- Troubleshoot the device on the Troubleshooting page by navigating to the Monitor > Tools menu and selecting the PMP AP/SM in the tree.
- Configure the devices by navigating to the Configure >Devices menu and selecting the PMP AP/SM in the tree and selecting the config template that needs to be pushed to the device. Configuration templates need to be created before the configuration can be pushed to the device. The template can be created by copying the existing configuration from the view device configuration link provided in the same page and then modifying the template as needed and then pushing to the same device or other similar devices. Template needs to be properly reviewed for IP Address and other critical parameters to avoid stranding SMs (resulting in a truck roll) by pushing an incorrect configuration. Configuration templates can be created by navigating to the Configure->Templates page and selecting the PMP device type while creating the template.
- Once on 14.2.1, PMP devices can be upgraded to future supported versions from cnMaestro™ by navigating to the Operate > Software Update page and selecting the “PMP Sectors” option from the device type drop-down and the version to which the device needs to be upgraded. It is recommended to upgrade the AP first, then the SMs.
- PMP Device Inventory details can be reviewed by navigating to the Monitor > Inventory page.

Configuring a RADIUS server

Configuring a RADIUS server in a PMP 450 Platform network is optional, but can provide added security, increase ease of network management and provide usage-based billing data.

Understanding RADIUS for PMP 450 Platform Family

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

RADIUS Functions

RADIUS protocol support provides the following functions

- SM Authentication allows only known SMs onto the network (blocking “rogue” SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to “rogue” APs). RADIUS authentication is used for SMs, but is not used for APs.
- SM Configuration: Configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), Medium Priority, High Priority, and Ultra High Priority Data channels, and VLAN (Virtual LAN) parameters from the RADIUS server when a SM registers to an AP.
- User Authentication allows users to configure a separate User authentication server along with the SM authentication server. If firmware is upgraded while using this functionality and no User authentication servers are configured, then AP continues to use the SM authentication server for User authentication
- SM Accounting provides support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP.
- Centralized AP and SM user name and password management allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does not track and report specific configuration actions

performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is not the ability to perform accounting functions on the subscriber/end user/customer account.

- Framed IP allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).

Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

- FreeRADIUS, Version 2.1.8
- Aradial RADIUS, Version 5.1.12
- Microsoft RADIUS (Windows Server 2012 R2 version)
- Cisco ACS, Version 5.7.0.15

> Note
>
> Aradial 5.3 has a bug that prevents “remote device login”, so doesn’t support the user name and password management feature.

Choosing Authentication Mode and Configuring for Authentication Servers - AP

On the AP’s **Configuration > Security tab**, select the RADIUS AAA Authentication Mode. The following describes the other **Authentication Mode** options for reference, and then the RADIUS AAA option.

- **Disabled**: Requires no authentication. Any SM (except a SM that itself has been configured to require RADIUS authentication by enabling Enforce Authentication as described below) is allowed to register to the AP.

- **Authentication Server**: Authentication Server in this instance refers to Wireless Manager in BAM-only mode. Authentication is required for a SM to register to the AP. Only SMs listed by MAC address in the Wireless Manager database is allowed to register to the AP.

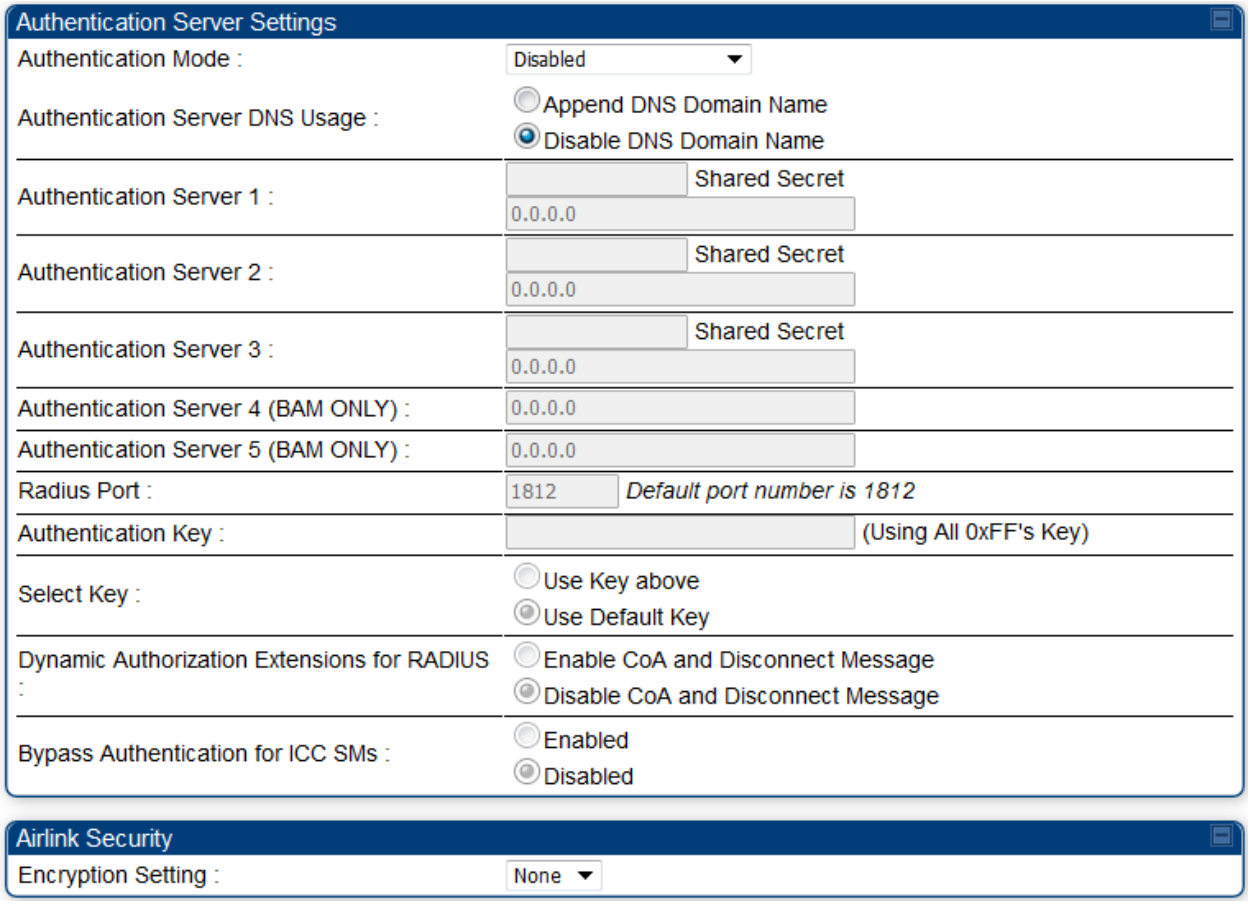
- **AP Pre-Shared Key**: Canopy offers a pre-shared key authentication option. In this case, an identical key must be entered in the Authentication Key field on the AP’s Configuration > Security tab and in the Authentication Key field on each desired SM’s Configuration > Security tab.

- **RADIUS AAA**: To support RADIUS authentication of SMs, on the AP’s Configuration > Security tab select RADIUS AAA. Only properly configured SMs with a valid certificate is allowed to register to the AP.

When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers.

The default IP address is 0.0.0.0. The default Shared Secret is “CanopySharedSecret”. The Shared Secret can be up to 32 ASCII characters (no diacritical marks or ligatures, for example).

Figure 62: *Security tab attributes*



AP Evaluation Configuration

SM Display of AP Evaluation Data :	○ Disable Display ◉ Enable Display

Session Timeout

Web, Telnet, FTP Session Timeout :	600 Seconds

IP Access Filtering

IP Access Control :	○ IP Access Filtering Enabled - Only allow access from IP addresses specified below ◉ IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0 / 32 Network Mask (set to 32 to disable)

Security Mode

Web Access :	HTTP Only
SNMP :	SNMPv2c Only
Telnet :	◉ Enabled ○ Disabled
FTP :	◉ Enabled ○ Disabled
TFTP :	◉ Enabled ○ Disabled
NTP server :	◉ Enabled ○ Disabled

Attribute	Meaning
Authentication Mode	Operators may use this field to select the following authentication modes: Disabled—the AP requires no SMs to authenticate. Authentication Server —the AP requires any SM that attempts registration to be authenticated in Wireless Manager before registration. AP PreShared Key - The AP acts as the authentication server to its SMs and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP and all SMs desired to register to that AP. There is also an option of leaving the AP and SMs at their default setting of using the “Default Key”. Due to the nature of the authentication operation, if you want to set a specific authentication key, then you MUST configure the key on all of the SMs and reboot them BEFORE enabling the key and option on the AP. Otherwise, if you configure the AP first, none of the SMs is able to register. RADIUS AAA - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address (s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn’t respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network and does not progress trying the other servers.
Authentication Server DNS Usage	The management DNS domain name may be toggled such that the name of the authentication server only needs to be specified and the DNS domain name is automatically appended to that name.
Authentication Server 1	Enter the IP address or server name of the authentication server (RADIUS or WM) and the Shared Secret configured in the authentication server. When Authentication Mode RADIUS AAA is selected, the default value of Shared Secret is “CanopySharedSecret”. The Shared Secret may consist of up to 32 ASCII characters.
Authentication Server 2	
Authentication Server 3	
Authentication Server 4 (BAM Only)	
Authentication Server 5 (BAM Only)	
Radius Port	This field allows the operator to configure a custom port for RADIUS server communication. The default value is 1812.
Authentication Key	The authentication key is a 32-character hexadecimal string used when Authentication Mode is set to AP Pre-Shared Key. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.
Selection Key	This option allows operators to choose which authentication key is used:

Attribute	Meaning
	Use Key above means that the key specified in Authentication Key is used for authentication Use Default Key means that a default key (based off of the SM's MAC address) is used for authentication
Encryption Key	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. None provides no encryption on the air link. AES (Advanced Encryption Standard): An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
SM Display of AP Evaluation Data	You can use this field to suppress the display of data about this AP on the AP Evaluation tab of the Tools page in all SMs that register.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the AP.
IP Access Control	You can permit access to the AP from any IP address (IP Access Filtering Disabled) or limit it to access from only one, two, or three IP addresses that you specify (IP Access Filtering Enabled). If you select IP Access Filtering Enabled, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted from any IP address
Allowed Source IP 1	If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the AP from any IP address. You may populate as many as all three.
Allowed Source IP 2	If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.
Allowed Source IP 3	
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop-down list: • HTTP Only – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • HTTPS Only – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • HTTP and HTTPS – If enabled, the radio can be accessed via bothHTTP and HTTPS..
SNMP	This option allows to configure SNMP agent protocol version. It can be selected from drop-down list :

Attribute	Meaning
	• Disable SNMP - To disable SNMP agent. • SNMPv2c Only – Enables SNMP v2c protocol. • SNMPv3 Only – Enables SNMP v3 protocol. It is secured communication protocol. • SNMPv2c and SNMPv3 – It enables both the protocols.
Telnet	This option allows to Enable and Disable Telnet access to the Radio.
FTP	This option allows to Enable and Disable FTP access to the Radio.
TFTP	This option allows to Enable and Disable TFTP access to the Radio.
NTP server	This option allows to Enable and Disable NTP server access to the Radio.

SM Authentication Mode – Require RADIUS or Follow AP

If it is desired that a SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set Enforce Authentication to AAA. With this enabled, SM does not register to an AP that has any Authentication Mode other than RADIUS AAA selected.

If it is desired that a SM use the authentication method configured on the AP it is registering to, set Enforce Authentication to Disabled. With Enforce Authentication disabled, a SM will attempt to register using whichever Authentication Mode is configured on the AP it is attempting to register to.

Note

Having SMs to use RADIUS by enabling Enforce Authentication avoids the security issue of SMs possibly registering to "rogue" APs, which have authentication disabled.

Table 89: SM Security tab attributes

Authentication Key Settings

Authentication Key :	(Using All 0xFF's Key)
Select Key :	○ Use Key above ◉ Use Default Key

AAA Authentication Settings

Enforce Authentication :	Disable
Phase 1 :	eapttls
Phase 2 :	MSCHAPv2
Identity/Realm :	○ Enable Realm ◉ Disable Realm Identity anonymous @ Realm canopy.net
Username :	0a-00-3e-a0-00-6c Use Default Username
Password :	••••••••
Confirm Password :	

RADIUS Certificate Settings

Upload Certificate File

File: Choose File No file chosen

Import Certificate

Use Default Certificates

This will delete all current certificates

Certificate 1

C =US
S =Illinois
O =Motorola Solutions, Inc.
OU =Canopy Wireless Broadband
CN =Canopy AAA Server Demo CA
E =technical-support@canopywireless.com
Valid From: 01/01/2001 00:00:00
Valid To: 12/31/2049 23:59:59

Delete

Certificate 2

Certificate 2 deleted.

Airlink Security

Encryption Setting :	DES

Session Timeout

Web, Telnet, FTP Session Timeout :	600000 Seconds

SM Management Interface Access via Ethernet Port

Ethernet Access :	◉ Enabled ○ Disabled

IP Access Filtering

IP Access Control :	○ IP Access Filtering Enabled - Only allow access from IP addresses specified below ◉ IP Access Filtering Disabled - Allow access from all IP addresses		
Allowed Source IP 1 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0	/ 32	Network Mask (set to 32 to disable)

Security Mode

Web Access :	HTTP Only
SNMP :	SNMPv2c Only
Telnet :	◉ Enabled ○ Disabled
FTP :	◉ Enabled ○ Disabled
TFTP :	◉ Enabled ○ Disabled

Attribute	Meaning
Authentication Key	The authentication key is a 32-character hexadecimal string used when Authentication Mode is set to AP PreShared Key. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.
Select Key	This option allows operators to choose which authentication key is used: Use Key above means that the key specified in Authentication Key is used for authentication Use Default Key means that a default key (based off of the SM's MAC address) is used for authentication
Enforce Authentication	The SM may enforce authentication types of AAA and AP Pre-sharedKey. The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM locks out the AP for 15 minutes). Enforce Authentication default setting is Disable.
Phase 1	The protocols supported for the Phase 1 (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).
Phase 2	Select the desired Phase 2 (Inside Identity) authentication protocol from the Phase 2 options of PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), and MSCHAP (Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.
Identity/Realm	If Realms are being used, select Enable Realm and configure an outer identity in the Identity field and a Realm in the Realm field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default Identity is "anonymous". The Identity can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default Realm is "canopy.net". The Realm can also be up to 128 non-special alphanumeric characters. Configure an outer Identity in the Username field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity Username is "anonymous". The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Username	Enter a Username for the SM. This must match the username configured for the SM on the RADIUS server. The default Username is the SM's MAC address. The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password	Enter the desired password for the SM in the Password and Confirm Password fields. The Password must match the password configured for the SM on the RADIUS server. The default Password is "password". The Password can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Confirm Password	

Attribute	Meaning
Upload Certificate File	To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a Delete button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on Choose File, browse to the location of the certificate, and click the Import Certificate button, and then reboot the radio to use the new certificate. When a certificate is in use, after the SM successfully registers to an AP, an indication of In Use will appear in the description block of the certificate being used. The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system. Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the Delete button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the Use Default Certificates button in the RADIUS Certificate Settings parameter block and reboot the radio.
Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. None provides no encryption on the air link. AES (Advanced Encryption Standard): An over-the-air link encryption option that uses the Rijndael algorithm and 128-bit keys to establish a higher level of security. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.
Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP, telnet or ftp access to the AP.
Ethernet Access	If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select Ethernet Access Disabled. This selection disables access through this port to via HTTP (the GUI), SNMP, telnet, FTP, and TFTP. With this selection, management access is available through only the RF interface via either an IP address (if Network Accessibility is set to Public on the SM) or the Session Status or Remote Subscribers tab of the AP. See IP Access Control below. If you want to allow management access through the Ethernet port, select Ethernet Access Enabled. This is the factory default setting for this parameter.
IP Access Control	You can permit access to the AP from any IP address (IP Access Filtering Disabled) or limit it to access from only one, two, or three IP addresses that you specify (IP Access Filtering Enabled). If you select IP Access Filtering Enabled, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted from any IP address

Attribute	Meaning
Allowed Source IP 1	If you selected IP Access Filtering Enabled for the IP Access Control parameter, then you must populate at least one of the three Allowed Source IP parameters or have no access permitted to the AP from any IP address. You may populate as many as all three. If you selected IP Access Filtering Disabled for the IP Access Control parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.
Allowed Source IP 2	
Allowed Source IP 3	
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop-down list: • HTTP Only – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • HTTPS Only – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • HTTP and HTTPS – If enabled, the radio can be accessed via both HTTP and HTTPS.
SNMP	This option allows to configure SNMP agent protocol version. It can be selected from drop-down list : • Disable SNMP - To disable SNMP agent. • SNMPv2c Only – Enables SNMP v2c protocol. • SNMPv3 Only – Enables SNMP v3 protocol. It is secured communication protocol. • SNMPv2c and SNMPv3 – It enables both the protocols.
Telnet	This option allows to Enable and Disable Telnet access to the Radio.
FTP	This option allows to Enable and Disable FTP access to the Radio.
TFTP	This option allows to Enable and Disable TFTP access to the Radio.

SM - Phase 1 (Outside Identity) parameters and settings

The protocols supported for the Phase 1 (Outside Identity) phase of authentication are

eapttls (Extensible Authentication Protocol Tunneled Transport Layer Security) and eapMSChapV2 (Extensible Authentication Protocol – Microsoft Challenge-Handshake Authentication Protocol).

Configure an outer Identity in the Username field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity Username is “anonymous”. The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters. If Realms are being used in the RADIUS system (eapttls only), select Enable Realm and configure an outer identity in the Identity field and a Realm in the Realm field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default Identity is “anonymous”. The Identity can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default Realm is “canopy.net”. The Realm can also be up to 128 non-special alphanumeric characters.

SM - Phase 2 (Inside Identity) parameters and settings

If using eapttls for Phase 1 authentication, select the desired Phase 2 (Inside Identity) authentication protocol from the Phase 2 options of PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), and MSCHAPv2 (Microsoft's version of CHAP). The protocol must be consistent with the authentication protocol configured on the RADIUS server. Enter a Username for the SM. This must match the username configured for the SM on the RADIUS server. The default Username is the SM's MAC address. The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Enter the desired password for the SM in the Password and Confirm Password fields. The Password must match the password configured for the SM on the RADIUS server. The default Password is "password". The Password can be up to 128 non-special (no diacritical markings) alphanumeric characters.

Handling Certificates

Managing SM Certificates via the SM GUI

The default public Canopy certificates are loaded into SMs upon factory software installation. The default certificates are not secure and are intended for use during lab and field trials as part of gaining experience with the RADIUS functionalities or as an option during debug. For secure operation, an operator will want to create or procure their own certificates. Resetting a SM to its factory defaults will remove the current certificates and restore the default certificates.

Up to two certificates can be resident on a SM. An installed certificate can be deleted by clicking the Delete button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the Use Default Certificates button in the RADIUS Certificate Settings parameter block and reboot the radio.

To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a Delete button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on Choose File, browse to the location of the certificate, and click the Import Certificate button, and then reboot the radio to use the new certificate.

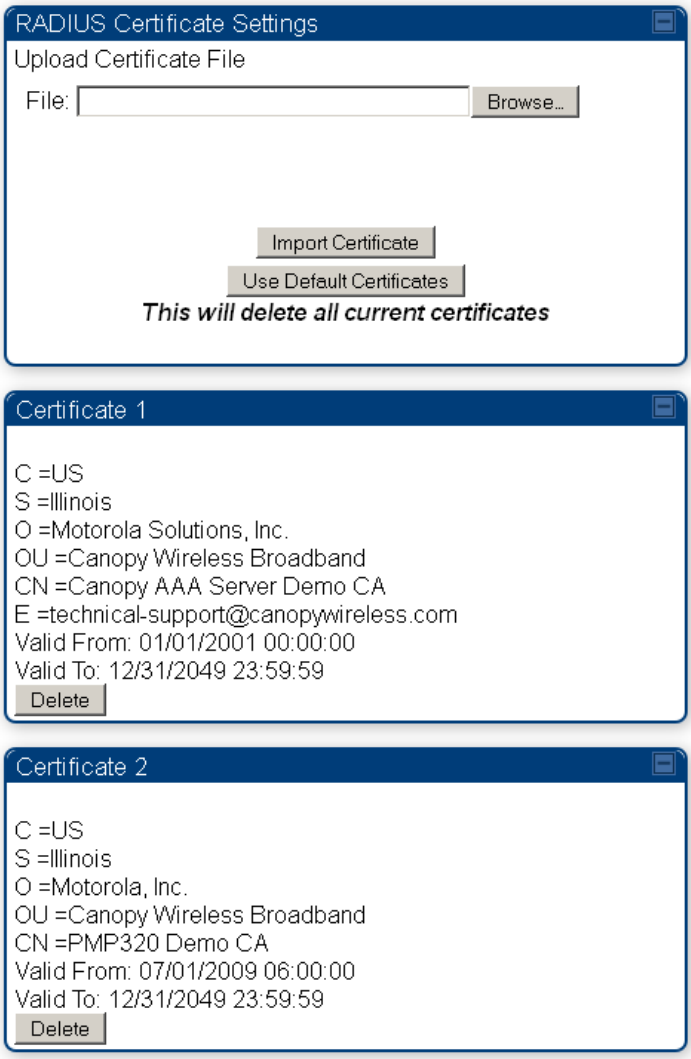
When a certificate is in use, after the SM successfully registers to an AP, an indication of In Use will appear in the description block of the certificate being used.

The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system.

Note

Root certificates of more than one level (Example - a certificate from someone who received their CA from Verisign) fails. Certificates must be either root or self-signed.

Figure 63: *SM Certificate Management*



Configuring RADIUS servers for SM authentication

Your RADIUS server must be configured to use the following:

- EAPTTLS or MSCHAPv2 as the Phase 1/Outer Identity protocol.
- If **Enable Realm** is selected on the SM's **Configuration > Security** tab, then the same Realm appears there (or access to it).
- The same Phase 2 (Inner Identity) protocol as configured on the **SM's Configuration > Security** tab under Phase 2 options.
- The username and password for each SM configured on each SM's **Configuration > Security** tab.
- An IP address and NAS shared secret that is the same as the IP address and Shared Secret configured on the AP's **Configuration > Security** tab for that **RADIUS server**.

- A server private certificate, server key, and CA certificate that complement the public certificates distributed to the SMs, as well as the Canopy dictionary file that defines Vendor Specific Attributes (VSAa). Default certificate files and the dictionary file are available from the software site: https://support.cambiumnetworks.com/files/pmp450 after entering your name, email address, and either Customer Contract Number or the MAC address of a module covered under the 12 month warranty.

Optionally, operators may configure the RADIUS server response messages (Accept or Reject) so that the user has information as to why they have been rejected. The AP displays the RADIUS Authentication Reply message strings in the Session Status list as part of each SM's information. The SM will show this string (listed as Authentication Response on the SM GUI) on the main Status page in the Subscriber Module Stats section.

Note

Aradial AAA servers only support operator-configurable Authentication Accept responses, not Authentication Reject responses.

Assigning SM management IP addressing via RADIUS

Operators may use a RADIUS AAA server to assign management IP addressing to SM modules (framed IP address). SMs now interpret attributes Framed-IP-Address, Framed-IP-Netmask, and Cambium-Canopy-Gateway from RADIUS. The RADIUS dictionary file has been updated to include the Cambium-Canopy-Gateway attribute and is available on the Cambium Software Support website.

In order for these attributes to be assigned and used by the SM, the following must be true:

- The system is configured for AAA authentication
- The SM is not configured for DHCP on its management interface. If DHCP is enabled and these attributes are configured in the RADIUS server, the attributes is ignored by the SM.
- The SM management interface must be configured to be publically accessible. If the SM is configured to have local accessibility, the management interface will still be assigned the framed addressing, and the SM iscome publicly accessible via the assigned framed IP addressing.
- When using these attributes, for the addressing to be implemented by the SM operators must configure Framed-IP-Address in RADIUS. If Framed-IP-Address is not configured but Framed-IP-Netmask and/or Cambium-Canopy-Gateway is configured, the attributes is ignored. In the case where only the Framed-IP-Address is configured, Framed-IP-Netmask defaults to 255.255.0.0 (NAT disabled) / 255.255.255.0 (NAT enabled) and Cambium-Canopy-Gateway defaults to 0.0.0.0.

Configuring RADIUS server for SM configuration

Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details are listed in RADIUS Vendor Specific Attributes (VSAs). The associated SM GUI page, tab and parameter are listed to aid cross-referencing and understanding of the VSAs.

A RADIUS dictionary file is available from the software site:

https://support.cambiumnetworks.com/files/pmp450

The RADIUS dictionary file defines the VSAs and their values and is usually imported into the RADIUS server as part of server and database setup.

Note

Beginning with System Release 12.0.2, two RADIUS dictionary files are available on the Cambium website – “RADIUS Dictionary file – Cambium” and “RADIUS Dictionary file – Motorola”.

In addition to a renaming of attributes, the Cambium-branded dictionary file contains two new VSAs for controlling uplink and downlink Maximum Burst Data Rate (these VSAs are listed below in RADIUS Vendor Specific Attributes (VSAs)).

If you are transitioning from the Motorola-branded dictionary file to the Cambium-branded dictionary file, ensure that all RADIUS profiles containing Motorola-Canopy attribute references are updated to include Cambium-Canopy attribute references (for all applicable VSAs listed in RADIUS Vendor Specific Attributes (VSAs)). Also, ensure that all RADIUS configuration files reference the new dictionary file (as an alternative, operators may rename the Cambium-branded dictionary file to the filename currently in use by the RADIUS server). Once the profiles are updated and the new Cambium-branded dictionary file is installed on the RADIUS server, restart the RADIUS server to ensure that the new VSAs and attribute names are enabled.

Table 90: RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Required	Value	
Cambium-Canopy-LPULCIR	26.161.1	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-LPDLCIR	26.161.2	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Downlink CIR				0 kbps	32 bits
Cambium-Canopy-HPULCIR	26.161.3	integer	N	0-65535 kbps	
Configuration > Quality of Service > High Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-HPDLCIR	26.161.4	integer	N	0-65535 kbps	
Configuration > Quality of Service > High Priority Downlink CIR				0 kbps	32 bits
Cambium-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable	
Configuration > Quality of Service > High Priority Channel Enable/Disable				0	32 bits
Cambium-Canopy-ULBR	26.161.6	integer	N	0-100000 kbps	

Name	Number	Type	Required	Value	
Configuration > Quality of Service > Sustained Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-ULBL	26.161.7	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-DLBR	26.161.8	integer	N	0-100000 kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-DLBL	26.161.9	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-VLLEARNEN	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Cambium-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Cambium-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Cambium-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Cambium-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Cambium-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits

Name	Number	Type	Required	Value	
Cambium-Canopy-VLSMMGPASS	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Cambium-Canopy-BCASTMIR	26.161.24	integer	N	0-100000 kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-Gateway	26.161.25	ipaddr	N	-	
Configuration > IP > Gateway IP Address				0.0.0.0	-
Cambium-Canopy-ULMB	26.161.26	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Uplink Data Rate				0	32 bits
Cambium-Canopy-DLMB	26.161.27	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Downlink Data Rate				0	32 bits
Cambium-Canopy-BCASTMIRUNITS	26.161.28	integer	N		
Configuration > QoS > Broadcast Downlink CIR				0	32 bits
Cambium-Canopy-ConfigFileImportUrl	26.161.29	string	N		
Configuration > Unit Settings				0	32 bits
Cambium-Canopy-ConfigFileExportUrl	26.161.30	string	N		
Configuration > Unit Settings				0	32 bits
Cambium-Canopy-DHCP-State	26.161.31	integer	N	1-Enable	
Configuration > IP > DHCP state				1	32 bits
Cambium-Canopy-SMPrioritizationGroup	26.161.32	integer	N	0-Low, 1-High	32 bits

Name	Number	Type	Required	Value	
Configuration > Quality of Service > Prioritization Group				0	
Cambium-Canopy-DATACHANCOUNT	26.161.35	integer	N	1 - 4	
Configuration > Quality of Service > Number of Data Channels				1	32 bits
Cambium-Canopy-MPULCIR	26.161.36	integer	N	0 - 65534 Kbps	
Configuration > Quality of Service > Medium Priority Uplink CIR				0	32 bits
Cambium-Canopy-MPDLCIR	26.161.37	integer	N	0 - 65534 Kbps	
Configuration > Quality of Service > Medium Priority Downlink CIR				0	32 bits
Cambium-Canopy-UHPULCIR	26.161.39	integer	N	0 - 65534 Kbps	
Configuration > Quality of Service > Ultra High Priority Uplink CIR				0	32 bits
Cambium-Canopy-UHPDLCIR	26.161.40	integer	N	0 - 65534 Kbps	
Configuration > Quality of Service > Ultra High Priority Downlink CIR				0	32 bits
Cambium-Canopy-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Cambium-Canopy-UserMode	26.161.51	integer	N	1=Read-Only 0=Read-Write	
Account > Add User > User Mode				0	32 bits
Cambium-Canopy-PortMap-Priority	26.161.52	integer	N	0 - 7	
Configuration > VLAN > Port VID MAC Address Mapping -> Priority				0	32 bits
Cambium-Canopy-PortMap-VLANID	26.161.53	integer	N	1 - 4094	32 bits
Configuration > VLAN > Port VID MAC Address Mapping -> VID				1	

Name	Number	Type	Required	Value	
Cambium-Canopy-PortMap-MacAddr	26.161.54	string	N	12 - 17	
Configuration > VLAN > Port VID MAC Address Mapping -> MAC Address				00-00-00-00-00-00	-
Cambium-Canopy-RatePlan-DL	26.161.55	integer	N	1 — 310000 kbps	
Configuration > Quality of Service > Downlink Plan				0	32 bits
Cambium-Canopy-RatePlan-UL	26.161.56	integer	N	1 — 310000 kbps	
Configuration > Quality of Service > Uplink Plan				0	32 bits
Cambium-Canopy-RatePlan-Weight	26.161.57	integer	N	0.1 - 9.9	
Configuration > Quality of Service > Weight				0	32 bits
Cambium-Canopy-RatePlan-UserLckMod	26.161.58	integer	N	0-Disabled, 1-Enabled, 2-Enable below threshold	
Configuration > Quality of Service > User Lock Modulation				0	32 bits
Cambium-Canopy-RatePlan-LockMod	26.161.59	integer	N	8=8x,6=6x,4=4x,3=3x,2=2x,1=1x	
Configuration > Quality of Service > Locked Modulation				8	32 bits
Cambium-Canopy-RatePlan-ThreMod	26.161.60	integer	N	8=8x,6=6x,4=4x,3=3x,2=2x	
Configuration > Quality of Service > Threshold Modulation				8	32 bits
Cambium-Canopy-SMVlan8021pSupport	26.161.61	integer	N	0-disable, 1-enable	
Configuration > VLAN > Support 802.1p Frames (VID 0)				0	32 bits
Cambium-Canopy-UserLevel-AP	26.161.62	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Cambium-Canopy-UserMode-AP	26.161.63	integer	N	1=Read-Only 0=Read- Write	

Name	Number	Type	Required	Value	
Account > Add User > User Mode				25 mins	32 bits
Cambium-Canopy-UserLevel-SM	26.161.64	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				1	32 bits
Cambium-Canopy-UserMode-SM	26.161.65	integer	N	1=Read-Only 0=Read- Write	
Account > Add User > User Mode				1	32 bits

(*) Contains key for encrypting packets sent by the NAS to the remote host (for Microsoft Point-to-Point Encryption Protocol).

Note

VSA numbering:

- 26 connotes Vendor Specific Attribute, per RFC 2865
- 26.311 is Microsoft Vendor Code, per IANA

Configuring RADIUS server for SM configuration using Zero Touch feature

The RADIUS VSA (Vendor Specific Attributes) is updated for Zero Touch feature. This feature enables the ability for a SM to get its configuration via RADIUS VSA. The RADIUS VSA is updated for an URL which points to the configuration file of SM (see RADIUS Vendor Specific Attributes (VSAs) for list of VSA).

The RADIUS will push the vendor specific attribute to SM after successful authentication. The VSA contains URL of config file which will redirect SM to download configuration. If there is any change in SM confirmation, the SM will reboot automatically after applying the configuration.

The RADIUS VSA attributes concerning Zero Touch are as follows:

```
VSA                                    Type       String


Cambium-Canopy-ConfigFileImportUrl (29) string  Maximum Length 127 characters.
Cambium-Canopy-ConfigFileExportUrl (30) string  Maximum Length 127 characters.
```

The updated RADIUS dictionary can be downloaded from below link:

https://support.cambiumnetworks.com/files/pmp450/

Note

The feature is not applicable to the AP.

Using RADIUS for centralized AP and SM user name and password management

AP – Technician/Installer/Administrator Authentication

To control technician, installer, and administrator access to the AP from a centralized RADIUS server:

Procedure 20 Centralized user name and password management for AP

1	Set Authentication Mode on the AP's Configuration > Security tab to RADIUS AAA
2	Set User Authentication Mode on the AP's Account > User Authentication tab (the tab only appears after the AP is set to RADIUS authentication) to Remote or Remote then Local. • Local: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • Remote: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has RADIUS AAA Authentication Mode selected. For up to 2 minutes a test pattern is displayed until the server responds or times out. • Remote then Local: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of Allow Local Login after Reject from AAA determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.

User administration and authentication separation

On the AP, it is possible to configure up to three User Authentication servers, along with their Shared Secret. If none of the User Authentication servers are configured, the AP continues to use SM Authorization servers for User Authentication.

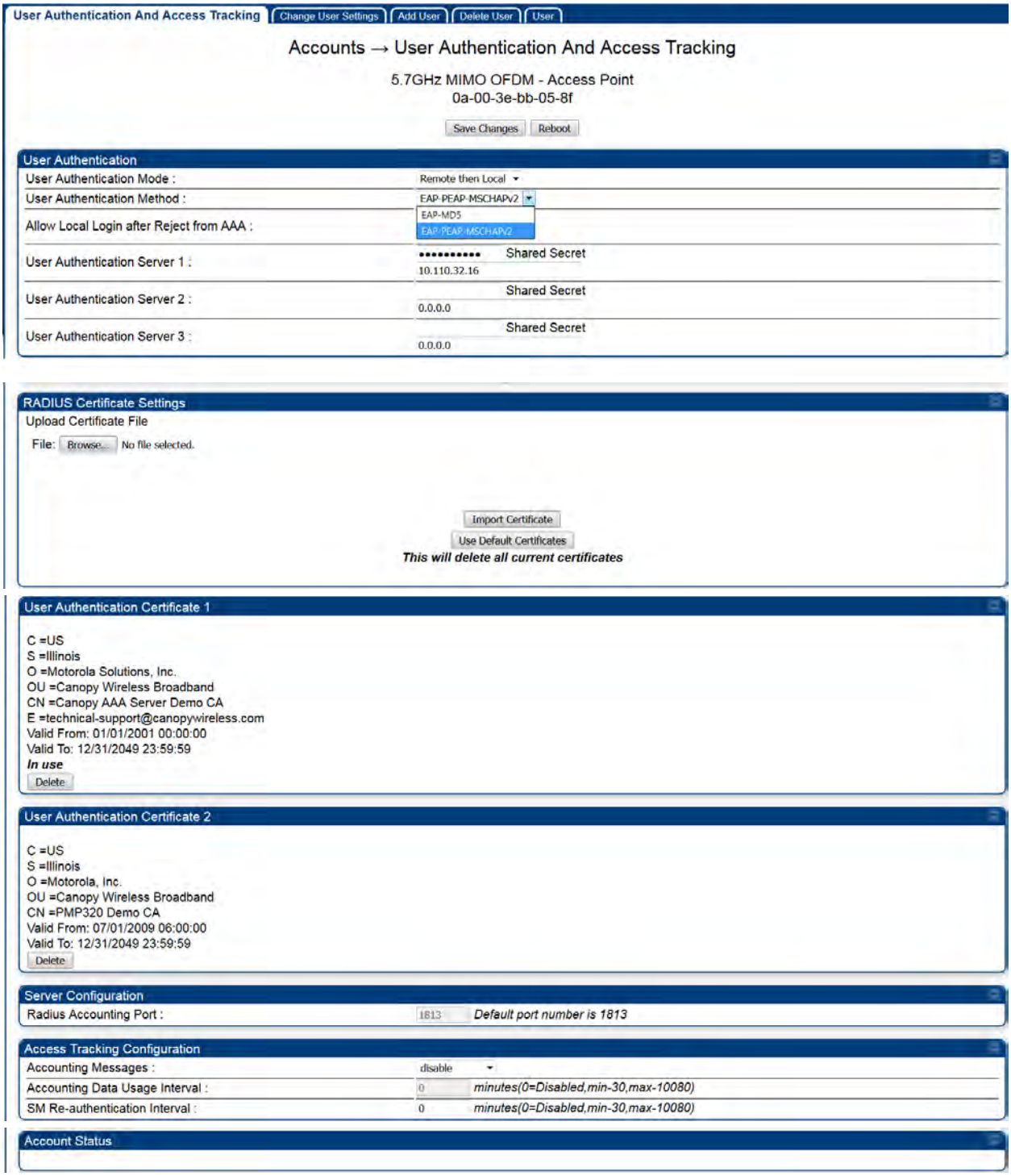
If at least one of the IP addresses is configured, all Authentication, Authorization, and Accounting requests now follow the newly configured User Authorization server.

To configure separate User Authentication and SM Authentication:

Procedure 21 User administration and authentication separation

1	Go to the AP's Account > User Authentication And Access Tracking tab
2	Set User Authentication Mode to Remote or Remote then Local.
3	Set User Authentication Method to EAP-MD5 or EAP-PEAP-MSCHAPv2
4	Configure the Shared Secrets and IP Addresses of: User Authentication Server 1 User Authentication Server 2 User Authentication Server 3 Note: If none of the above User Authentication servers are configured, only SM authentication will be performed.
5	Under RADIUS Certificate Settings, click Browse to upload the RADIUS Certificate files.

Figure 64: *User Authentication and Access Tracking attributes*



Attribute	Meaning
User Authentication Mode	• Local: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • Remote: Authentication by the centralized RADIUS server is required to gain access to the AP. For up to 2 minutes a test pattern is displayed until the server responds or times out. • Remote then Local: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of Allow Local Login after Reject from AAA determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the AP.
User Authentication Method	The user authentication method employed by the radios: • EAP-MD5 • EAP-PEAP-MSCHAPv2
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user is allowed to login locally to the radio's management interface.
User Authentication Server 1	The IP address and the shared secret key of the User authentication RADIUS server 1.
User Authentication Server 2	The IP address and the shared secret key of the User Authentication Server 2 configured in RADIUS Server.
User Authentication Server 3	The IP address and the shared secret key of the User Authentication Server 3 configured in RADIUS Server.
RADIUS Certificate Settings	Import Cetificate – browse and select the file to be uploaded and click on "Import Certificate" to import a new certificate. Use Default Certificates – use the preloaded default certificates.
User Authentication Certificate 1	Cerificate provided by default for User authentication.
User Authentication Certificate 2	Cerificate provided by default for User authentication.
Radius Accounting Port	The destination port on the AAA server used for Radius accounting communication.
Accounting Messages	Disable – no accounting messages are sent to the RADIUS server.

Attribute	Meaning
	deviceAccess – accounting messages regarding device access are sent to the RADIUS server (see Device data accounting RADIUS attributes). DataUsage – accounting messages regarding data usage are sent to the RADIUS server (see Device data accounting RADIUS attributes). All – accounting messages regarding device access and data usage are sent to the RADIUS server.
Accounting Data Usage Interval	The interval for which accounting data messages are sent from the radio to the RADIUS server. If 0 is configured for this parameter, no data usage messages are sent.
SM Re-authentication Interval	The interval for which the SM will re-authenticate to the RADIUS server.
Account Status	Displays the account status.

SM – Technician/Installer/Administrator Authentication

The centralized user name and password management for SM is same as AP. Follow AP – Technician/Installer/Administrator Authentication on page AP – Technician/Installer/Administrator Authentication procedure.

Note

Remote access control is enabled only after the SM registers to an AP that has Authentication Mode set to RADIUS AAA. Local access control will always be used before registration and is used after registration if the AP is not configured for RADIUS.

Figure 65: *User Authentication and Access Tracking tab of the SM*

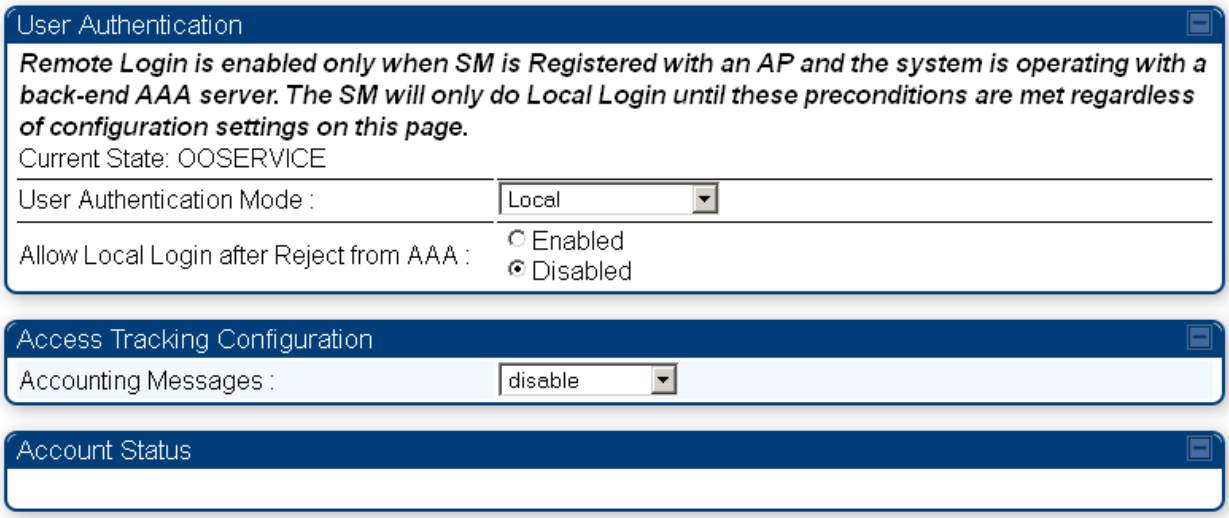
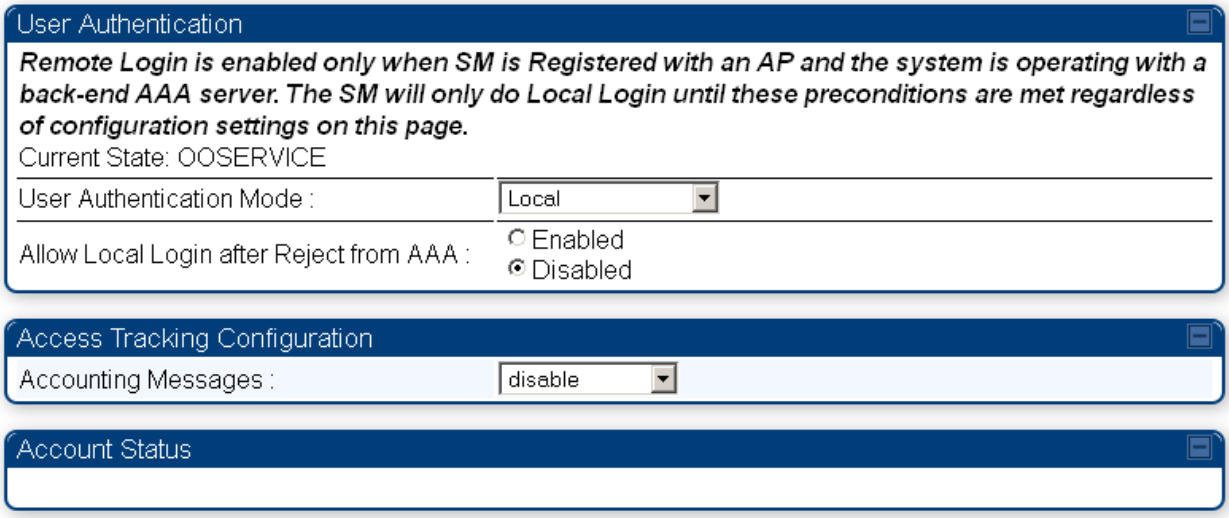


Table 91: SM User Authentication and Access Tracking attributes



Attribute	Meaning
User Authentication Mode	• Local: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • Remote: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has RADIUS AAA Authentication Mode selected. For up to 2 minutes a test pattern is displayed until the server responds or times out. • Remote then Local: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of Allow Local Login after Reject from AAA determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user is allowed to login locally to the radio's management interface. It is applicable ONLY when the User Authentication Mode is set to "Remote then Local". Note When the radio User Authentication Mode is set to "Local" or "Remote", the Allow Local Login after Reject from AAA does not any effect.
Accounting Messages	• disable – no accounting messages are sent to the RADIUS server • deviceccess – accounting messages are sent to the RADIUS server regarding device access (see Device data accounting RADIUS attributes).

Access Tracking

To track logon and logoff times on individual radios by technicians, installers, and administrators, on the AP or SM's Account > User Authentication and Access Tracking tab under Accounting (Access Tracking)

set Accounting Messages to “deviceAccess”.

Device Access Tracking is enabled separately from User Authentication Mode. A given AP or SM can be configured for both, either, or neither.

RADIUS Device Data Accounting

PMP 450 Platform systems include support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP. The attributes included in the RADIUS accounting messages are shown in the table below.

Table 92: Device data accounting RADIUS attributes

Sender	Message	Attribute	Value	Description
AP	Accounting-Request	Acct-Status-Type	1 - Start	This message is sent every time a SM registers with an AP, and after the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Event-Timestamp	UTC time the event occurred on the AP	

Sender	Message	Attribute	Value	Description
AP	Accounting-Request	Acct-Status-Type	2 - Stop	This message is sent every time a SM becomes unregistered with an AP, and when the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets received at the SM over the Low Priority data channel as well as any Medium, High, and Ultra High Priority data channels configured.. Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets sent from the SM over the Low Priority data channel as well as any Medium, High, and Ultra High Priority data channels configured..	
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the Low Priority data channel as well as any Medium, High, and Ultra High Priority data channels configured..	
		Acct-Session-Time	Uptime of the SM session.	
		Acct-Terminate-Cause	Reason code for session termination	

Sender	Message	Attribute	Value	Description
AP	Accounting-Request	Acct-Status-Type	3 - Interim-Update	This message is sent periodically per the operator configuration on the AP in seconds. Interim update counts are cumulative over the course of the session
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets sent to the SM over the Low Priority data channel as well as any Medium, High, and Ultra High Priority data channels configured.. Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets set from the SM over the Low Priority data channel as well as any Medium, High, and Ultra High Priority data channels configured.	
		Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Output-Gigawords	Number of times the Acct-Output-Octets counter has wrapped around 2^32 over the course of the session	
		Acct-Session-Time	Uptime of the SM session.	
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data channel and the high priority data VC (if enabled). It will not include broadcast.	
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the regular data VC and the high priority data VC (if enabled).	

The data accounting configuration is located on the AP's Accounts > User Authentication and Access Tracking GUI menu, and the AP's Authentication Mode must be set to Radius AAA for the menu to appear. The accounting may be configured via the AP GUI as shown in the figures below. By default accounting messages are not sent and the operator has the choice of configuring to send only Device Access accounting messages (when a user logs in or out of the radio), only Data Usage messages, or both. When Data Accounting is enabled, the operator must specify the interval of when the data accounting messages are sent (0 – disabled, or in the range of 30-10080 minutes). The default interval is 30 minutes.

Figure 66: *RADIUS accounting messages configuration*

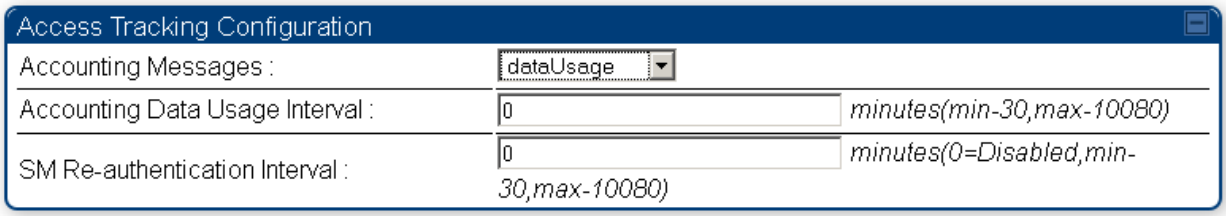
The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify the AAA of the change.

If an operator clears the VC statistics on the device through the management GUI, a RADIUS stop message and data start message is issued for each device affected. The start and stop messages will only be sent once every 5 minutes, so if an operator clears these statistics multiple times within 5 minutes, only one set of data stop/start messages is sent. This may result in inaccurate data accumulation results.

RADIUS Device Re-authentication

PMP 450 Platform systems include support for periodic SM re-authentication in a network without requiring the SM to re-register (and drop the session). The re-authentication may be configured to occur in the range of every 30 minutes to weekly.

Figure 67: *Device re-authentication configuration*



The re-authentication interval is only configurable on the AP. When this feature is enabled, each SM that enters the network will re-authenticate each the interval time has expired without dropping the session. The response that the SM receives from the AAA server upon re-authentication is one of the following:

- Success: The SM continues normal operation
- Reject: The SM de-registers and will attempt network entry again after 1 minute and then if rejected will attempt re-entry every

  minutes
- Timeout or other error: The SM remains in session and attempt 5 times to re-authenticate with the RADIUS-REQUEST message. If these attempts fail, then the SM will go out of session and proceed to re-authenticate after 5 minutes, then every 15 minutes.

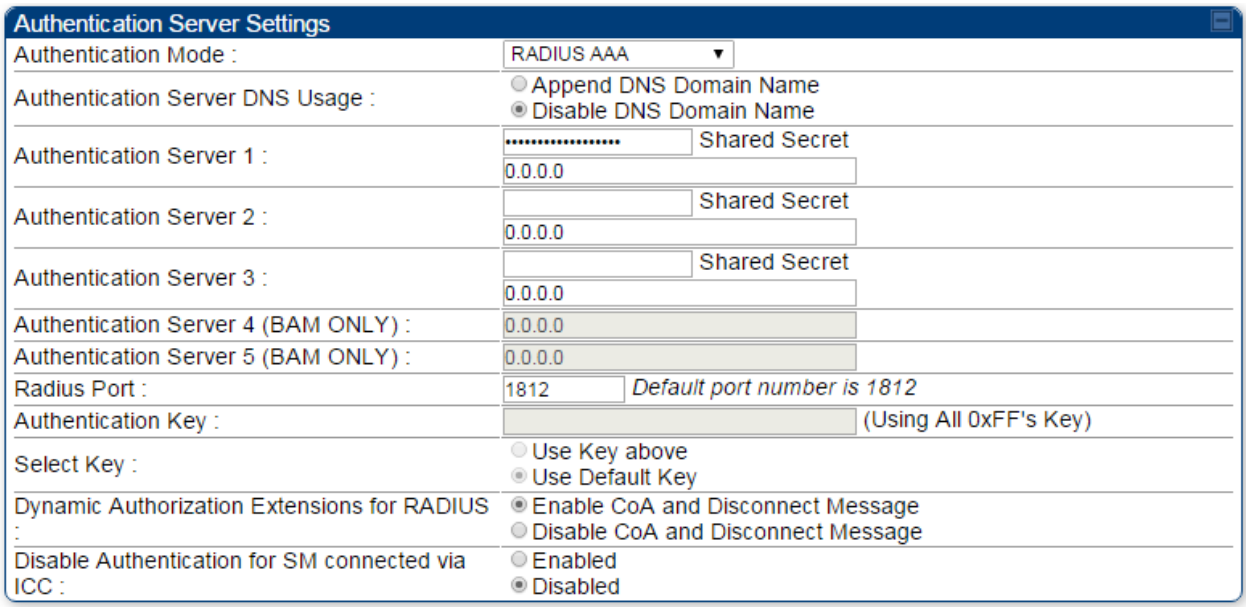
Although re-authentication is an independent feature, it was designed to work alongside with the RADIUS data usage accounting messages. If a user is over their data usage limit the network operator can reject the user from staying in the network. Operators may configure the RADIUS 'Reply-Message' attribute with an applicable message (i.e. "Data Usage Limit Reached") that is sent to the subscriber module and displayed on the general page.

RADIUS Change of Authorization and Disconnect Message

Prior to this feature, SM will get configuration parameters from a RADIUS server during authentication process. This feature allows an administrator to control configuration parameters in the SM while SM is in session. The configuration changes in SM are done using RADIUS Change of Authorization method (RFC

3576) on the existing RADIUS authentication framework for AP and SM. A typical use case could be changing the QOS parameters after a certain amount of bandwidth usage by a SM.

Figure 68: *RADIUS CoA configuration for AP*



The RADIUS CoA feature enables initiating a bi-directional communication from the RADIUS server(s) to the AP and SM.

The AP listens on UDP port 3799 and accepts CoA requests from the configured RADIUS servers. This CoA request should contain SM MAC address in 'User-Name' attribute as identifier and all other attributes which control the SM config parameters. For security reasons, a timestamp also needs to be added as 'Event-Timestamp' attribute. Hence the time should also be synchronized between the RADIUS server(s) and the AP to fit within a window of 300 seconds.

Once the configuration changes are applied on the SM, CoA-ACK message is sent back to RADIUS server. If the validation fails, the AP sends a CoA-NACK response to the RADIUS server with proper error code.

A Disconnect-Message is sent by the RADIUS server to NAS in order to terminate a user session on a NAS and discard all associated session context. It is used when the authentication AAA server wants to disconnect the user after the session has been accepted by the RADIUS.

In response of Disconnect-Request from RADIUS server, the NAS sends a Disconnect-ACK if all associated session context is discarded, or a Disconnect-NACK, if the NAS is unable to disconnect the session.

Note

The RADIUS CoA feature will only enabled if Authentication mode is set to RADIUS AAA.

Microsoft RADIUS support

This feature allows to configure Microsoft RADIUS (Network Policy and Access Services a.k.a NPS) as Authentication server for SM and User authentication.

- For SM Authentication, SM will user PEAP-MSCHAPv2 since NPS doesn't support TTLS protocol.
- For User Authentication, the Canopy software will use EAP-MD5 but the user has to do certain configuration in order to enable EAP-MD5 on NPS.

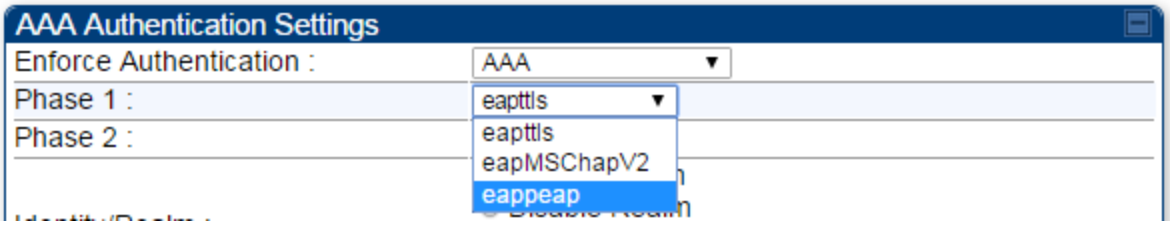
> **Note**
>
> All this configuration has been tested on Windows Server 2012 R2 version.
>
> This feature is not supported on hardware board type P9 or lower platforms.

SM Authentication Configuration

There are no new configurations on AP. However, SM has to be configured for PEAP authentication protocol.

1. Go to **Configuration > Security** page
2. Select "eappeap" for Phase 1 attribute under tab AAA Authentication Settings.

Figure 69: *EAPPEAP settings*



The Phase 2 will change automatically to MSCHAPv2 on select of Phase 1 attribute as EAP-PEAP. Other parameters of Phase 2 protocols like PAP/CHAP will be disabled.

Windows Server Configuration

Import Certificate

The SM certificate has to be imported to Windows Server for certificate authentication.

- Copy the certificate which is configured in SM under Configuration > Security -> Certificate1 to Windows Server machine.
- Right click and select 'Install Certificate'. This will install the certificate and it's ready for use. This certificate will be used while configuring PEAP-MSCHAPv2 in NPS.

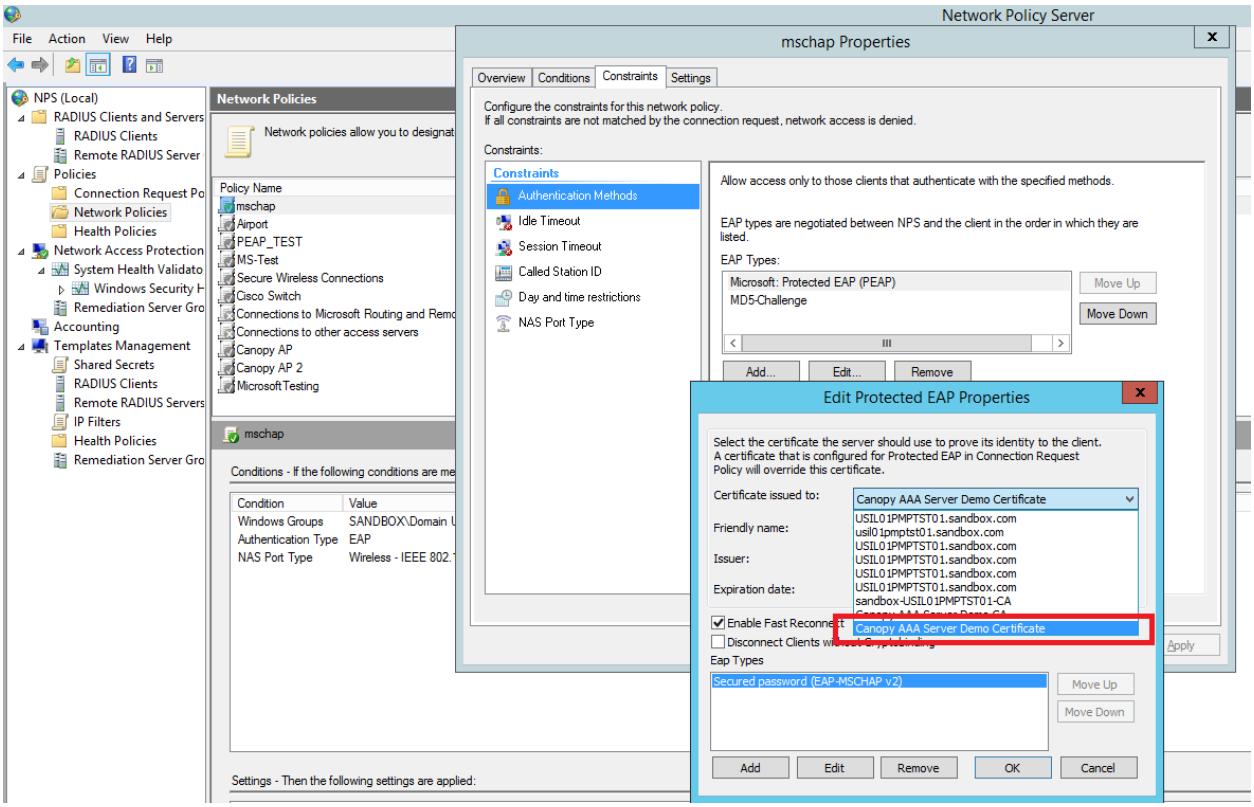
NPS Configuration (https://technet.microsoft.com/en-us/network/bb545879.aspx)

Following **items** should be configured in NPS Console:

- RADIUS Client
- https://technet.microsoft.com/en-us/library/cc732929
- Connection Request Policies
- https://technet.microsoft.com/en-us/library/cc730866
- Choose 'Wireless-Other' in NAS-Port-Type

- Network Policy
- https://technet.microsoft.com/en-us/library/cc755309
- Choose 'Wireless-Other' in NAS-Port-Type.
- While configuring PEAP, select the above imported certificate.

Figure 70: *Importing certificate in NPS*



User Authentication Configuration

Enabling EAP-MD5

As mentioned earlier, Microsoft has deprecated the support for MD5 from versions of Windows. To enable MD5, the following steps to be followed:

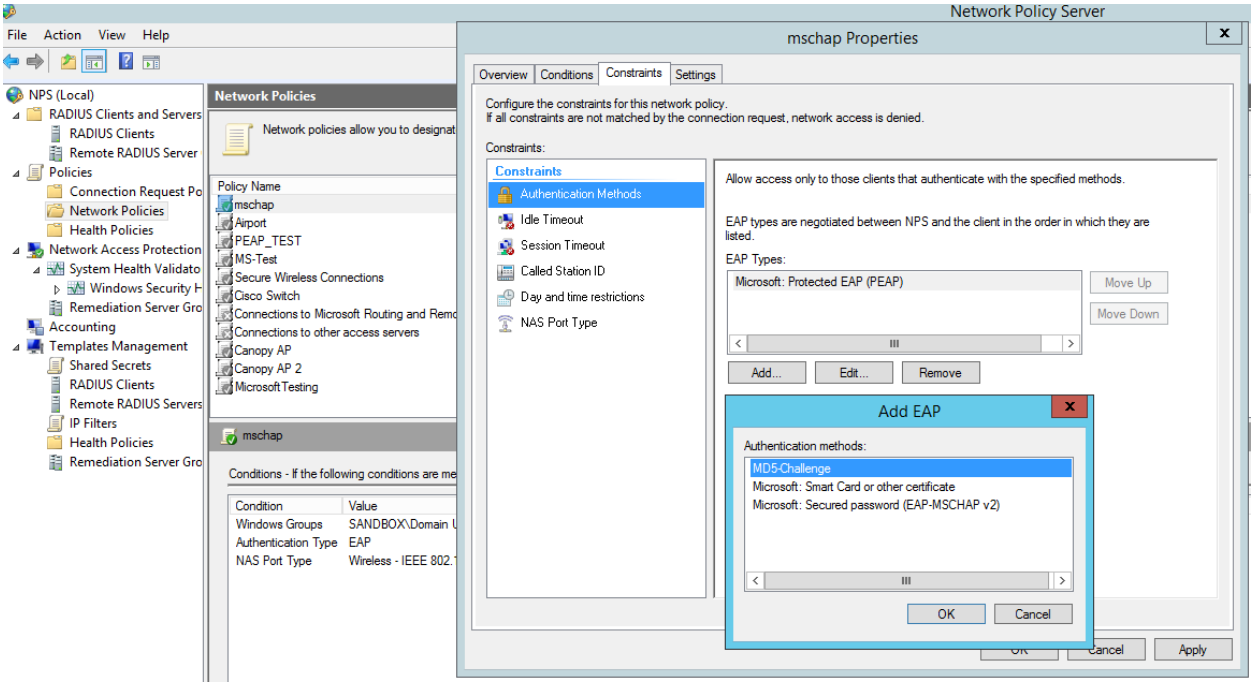
1. Follow the instructions:

   Optionally, the registry file can be downloaded. It can be installed by double-click it in Windows Registry.

   https://support.microsoft.com/en-us/kb/922574/en-us?wa=wsignin1.0

2. From NPS Console Network Policy > <Policy Name> > Properties > Constrains > Authentication Method and click Add. Select MD5 and click OK.

Figure 71: *Selecting MD5 from NPS console*

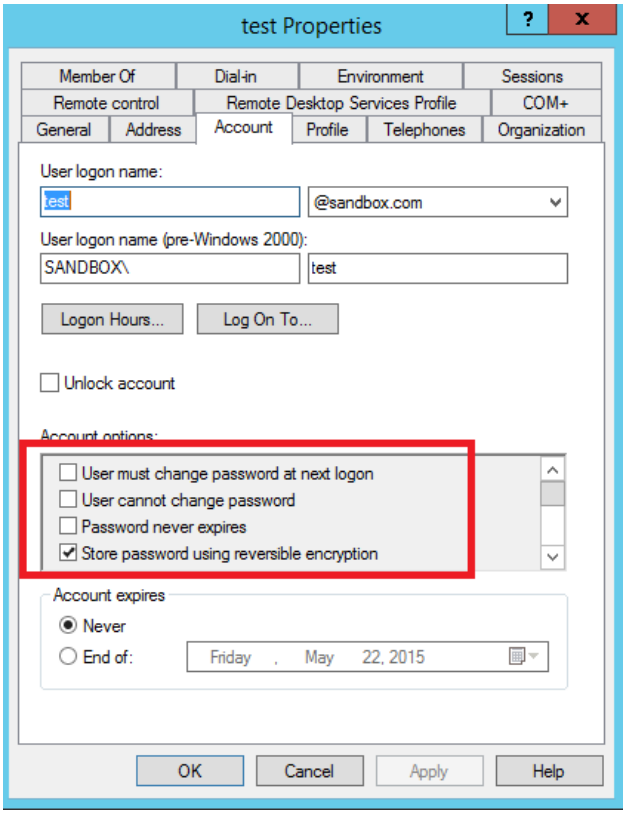


User Configuration in Active Directory

Next open '**Active Directory Users and Computers**' and create user.

Make sure user property is configured as shown below.

Figure 72: *User configuration*



RADIUS VSA Configuration

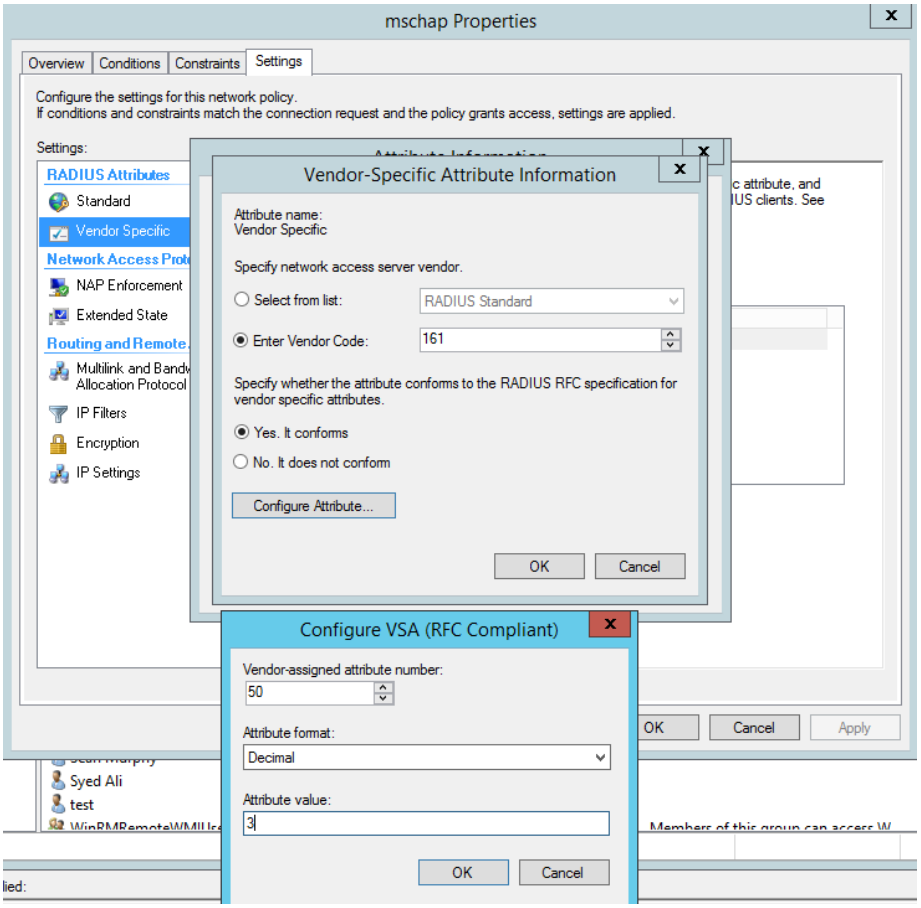
Before using VSA, the **Cambium-Canopy-UserLevel(50)** VSA must be configured with some access level say ADMIN(3).

Follow below link for configuring VSA:

https://technet.microsoft.com/en-us/library/cc731611

The Cambium's vendor code is 161.

Figure 73: *RADIUS VSA configuration*



Accounting

User can enable accounting in NPS under **NPS Console > Accounting > Configure Accounting.**

For more details refer https://technet.microsoft.com/library/dd197475

Cisco ACS RADIUS Server Support

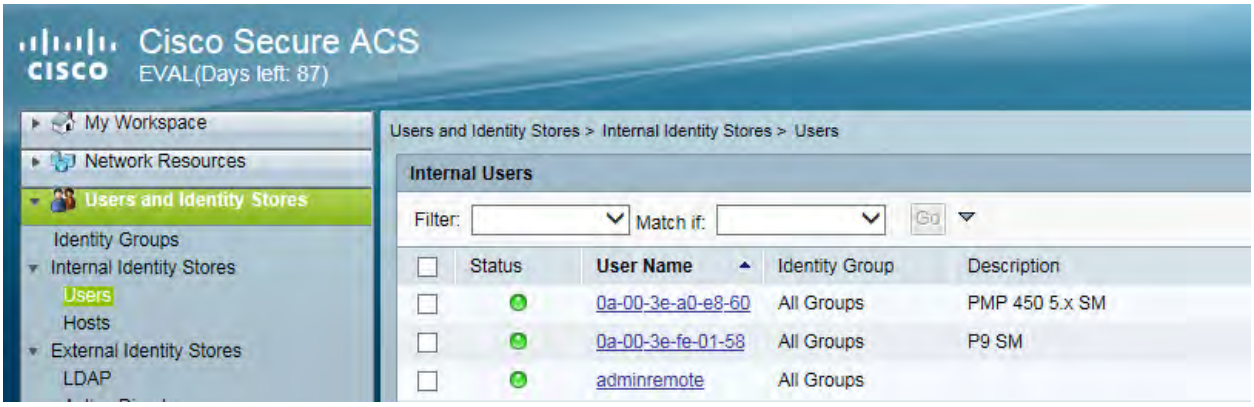
This briefly explains how to configure Cisco ACS RADIUS server for PEAP-MSCHAPv2 authentication. The configuration had been tested on CISCO ACS Version : 5.7.0.15

Adding RADIUS client

Figure 74: *Adding RADIUS client*

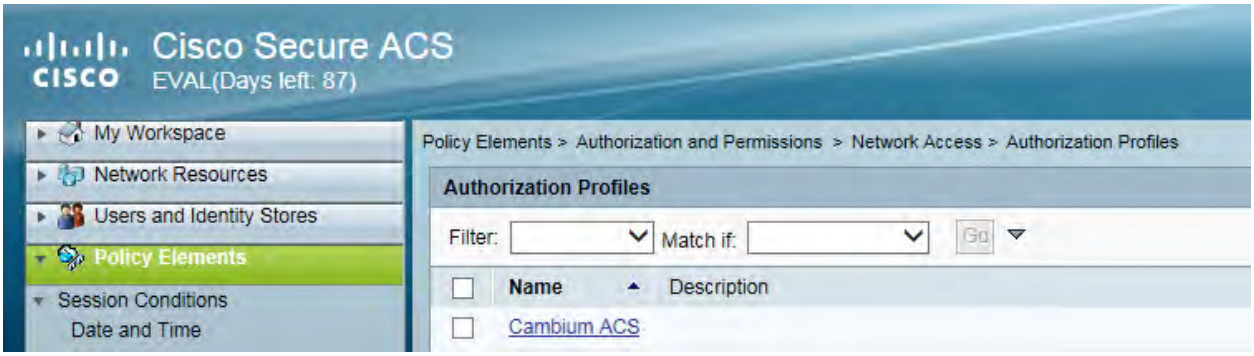
Creating Users

Figure 75: *Creating users*



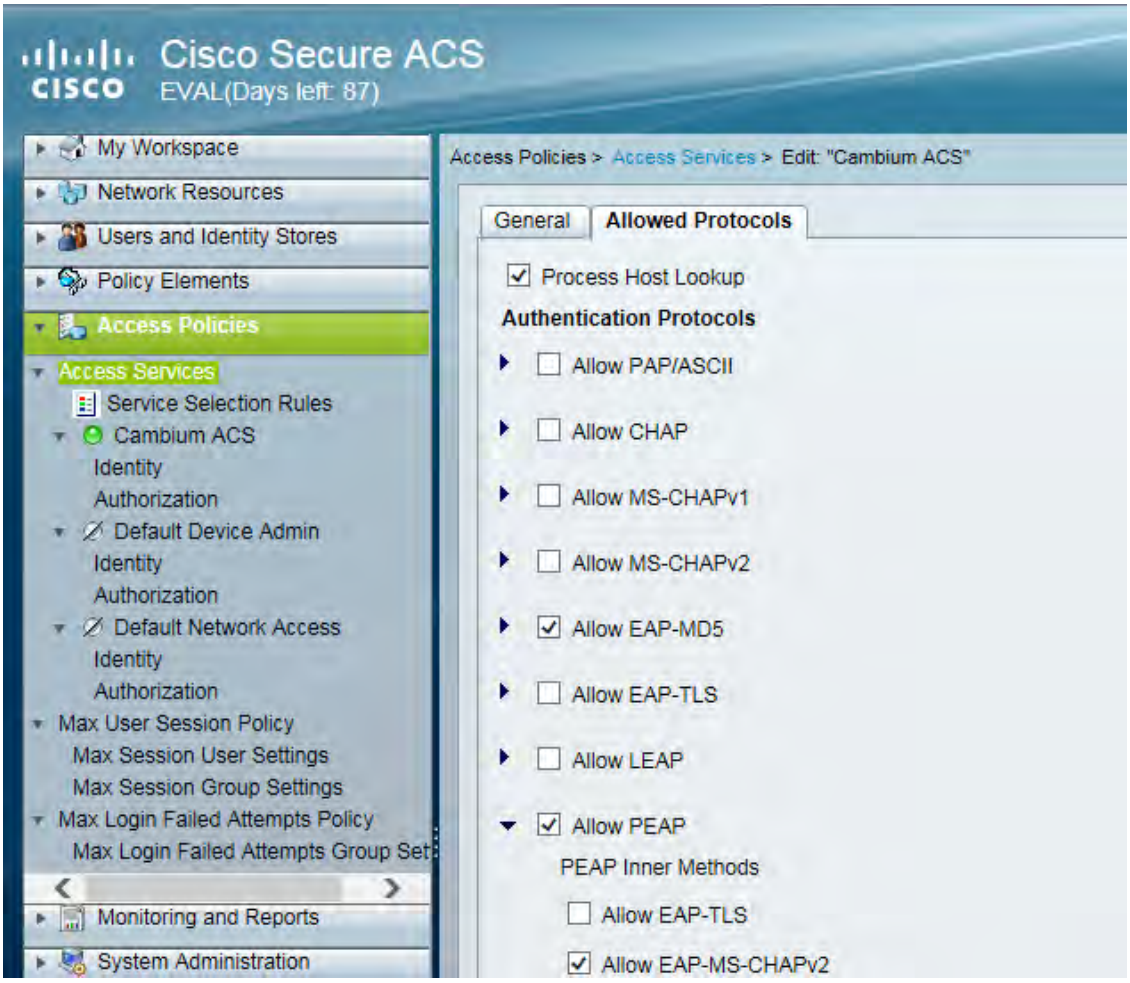
Creating RADIUS instance

Figure 76: *Creating RADIUS instance*



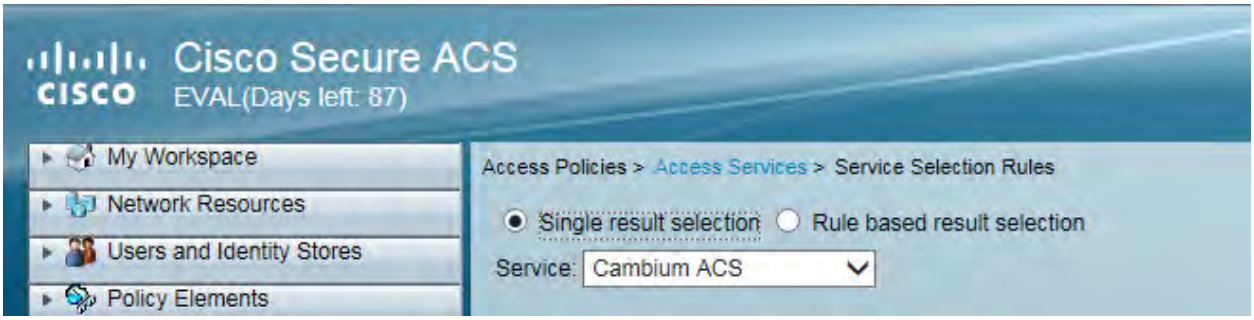
RADIUS protocols

Figure 77: *RADIUS protocols*



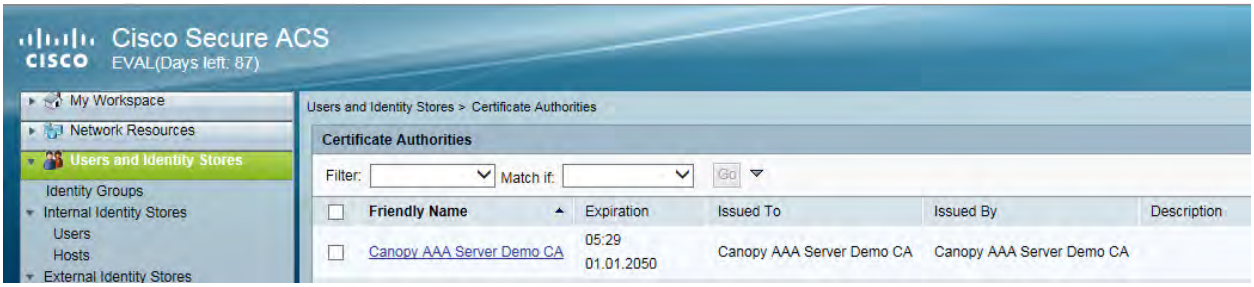
Service selection

Figure 78: *Service selection*



Adding Trusted CA

Figure 79: *Adding Trusted CA*



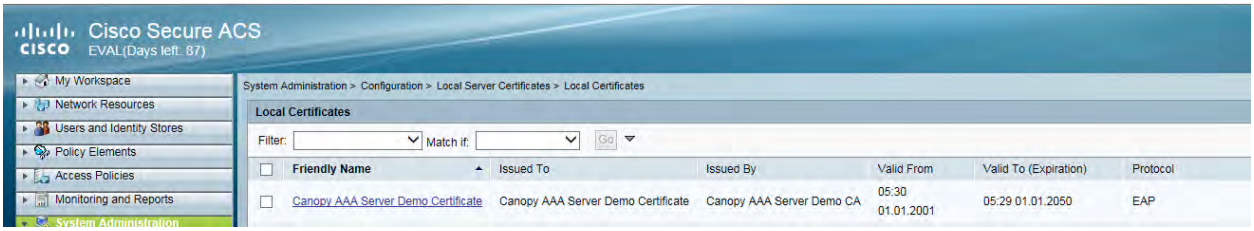
Note that certificate has to be in DER form, so if you have in PEM format convert using openssl.

Openssl.exe x509 -in <path-to->/cacert_aaasvr.pem -outform DER -out <path-to>/cacert_aaasvr.der

Installing Server Certificate

After installing trusted CA, you need to add a server certificate which will be used for TLS tunnel. Generally you have to install same certificate which is installed in your AP, so that AP can trust the radius server.

Figure 80: *Installing Server Certificate*



Monitoring Logs

Figure 81: *Monitoring logs*

Configuring VSA

Before using VSA , user has to add Cambium Vendor Specific Attribute

Navigate to **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > Motorola**

If Motorola is not present you can create Vendor with ID 161 and add all the VSA one by one.

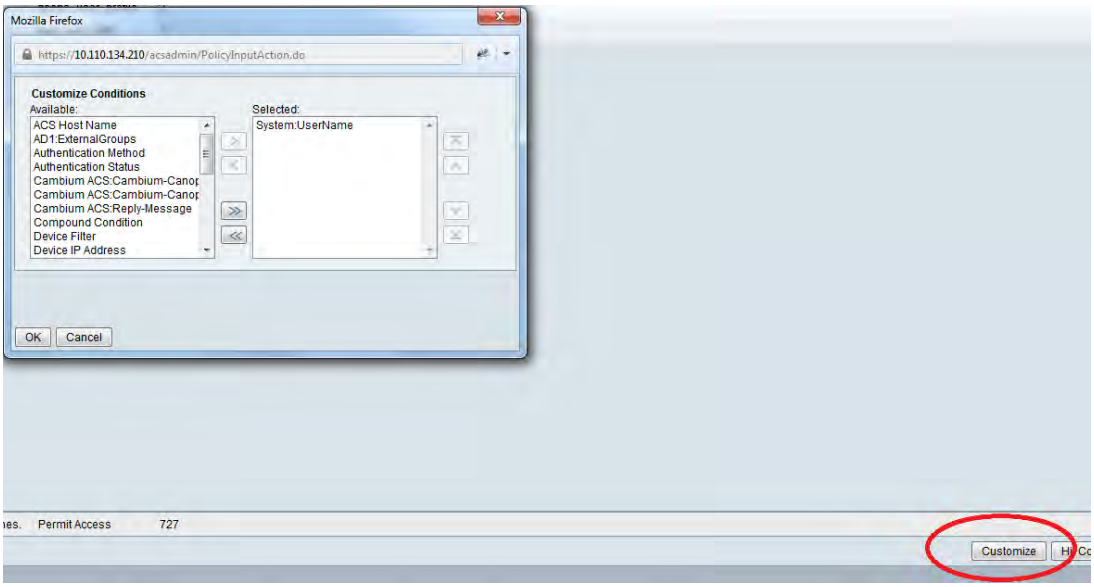
Figure 82: *VSA list*

Attribute	ID	Type	Direction	Multiple Allowed
Cambium-Canopy-BCASTMIR	24	Unsigned Integer 32	BOTH	false
Cambium-Canopy-DLBL	9	Unsigned Integer 32	BOTH	false
Cambium-Canopy-DLBR	8	Unsigned Integer 32	BOTH	false
Cambium-Canopy-DLMB	27	Unsigned Integer 32	BOTH	false
Cambium-Canopy-Gateway	25	IP Address	BOTH	false
Cambium-Canopy-HPDLCIR	4	Unsigned Integer 32	BOTH	false
Cambium-Canopy-HPENABLE	5	Unsigned Integer 32	BOTH	false
Cambium-Canopy-HPULCIR	3	Unsigned Integer 32	BOTH	false
Cambium-Canopy-LPDLCIR	2	Unsigned Integer 32	BOTH	false
Cambium-Canopy-LPULCIR	1	Unsigned Integer 32	BOTH	false
Cambium-Canopy-ULBL	7	Unsigned Integer 32	BOTH	false
Cambium-Canopy-ULBR	6	Unsigned Integer 32	BOTH	false
Cambium-Canopy-ULMB	26	Unsigned Integer 32	BOTH	false
Cambium-Canopy-UserLevel	50	Unsigned Integer 32	BOTH	false
Cambium-Canopy-UserMode	51	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLAGETO	20	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLFRAMES	15	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLIDSET	16	Unsigned Integer 32	BOTH	true
Cambium-Canopy-VLIGVID	21	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLLEARNEN	14	Unsigned Integer 32	BOTH	false
Cambium-Canopy-VLMGVID	22	Unsigned Integer 32	BOTH	true
Cambium-Canopy-VLSMMGPASS	23	Unsigned Integer 32	BOTH	false

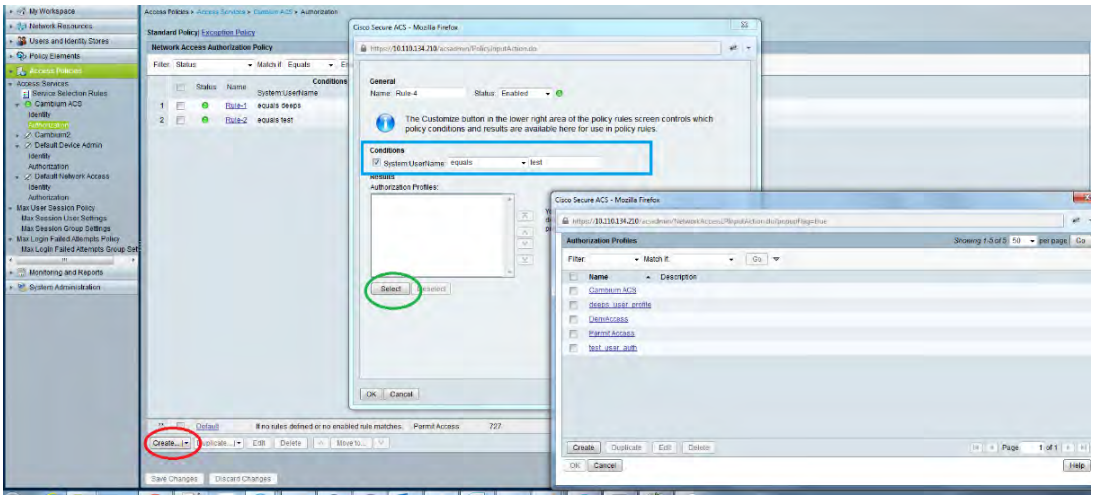
Using VSA for users

Navigate to **Access Policies > Access Services > Cambium ACS > Authorization**

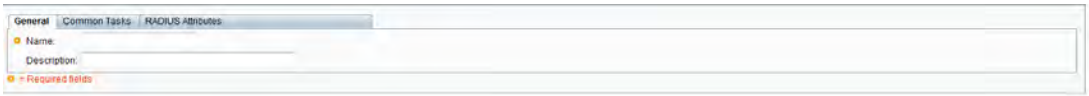
1. Change condition to User name



2. Next click Create and then click Select see diagram below

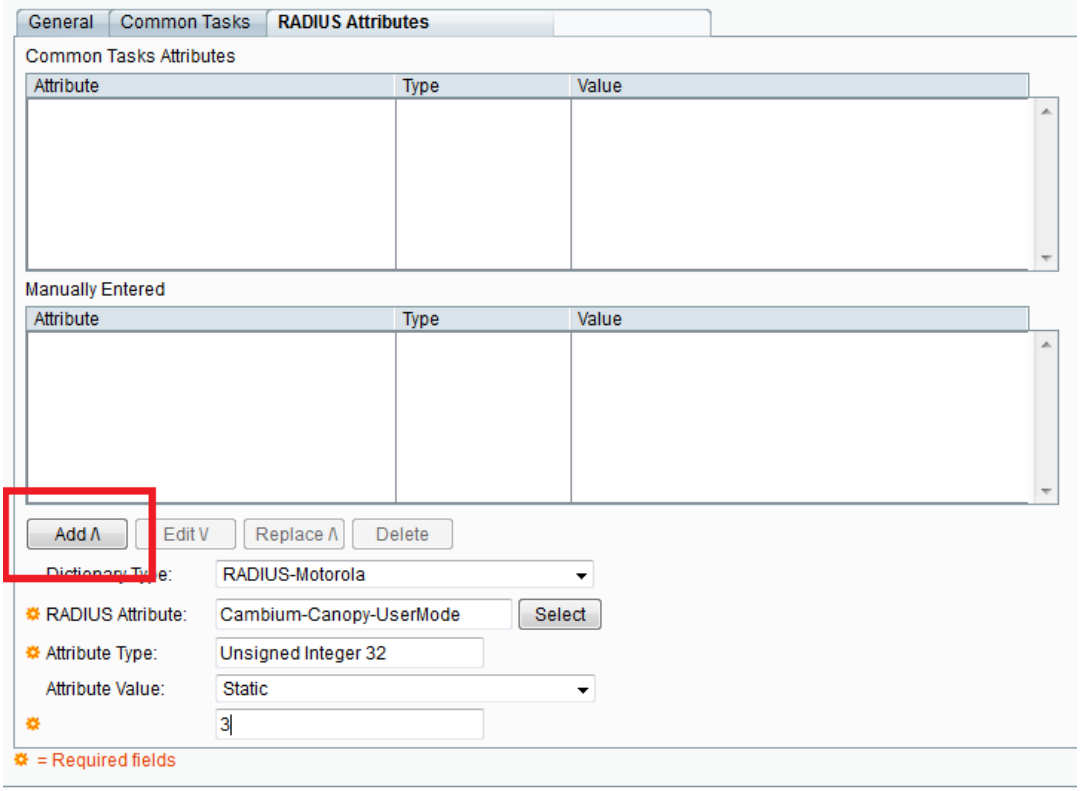


3. Click **Create** from the screen you get following screen



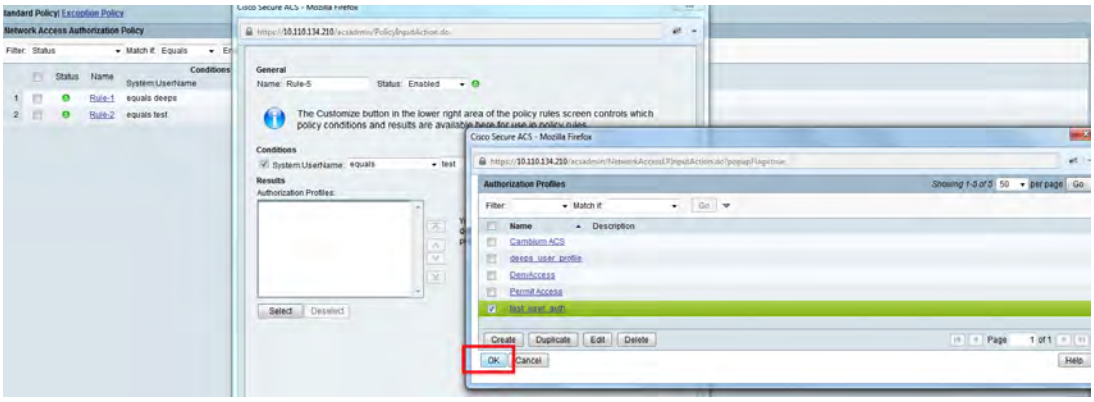
Chose some name and then move to RADIUS Attributes tab

4. Fill attribute which all you want for that particular user



Important: Click Add for each attribute and when done click Submit.

5. Now you are ready to use this Authorization profile for the use Select and Press OK.



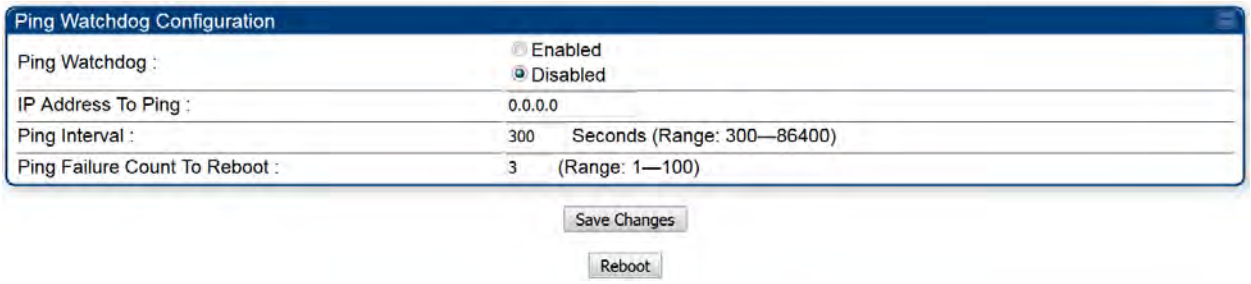
6. Finally press Save Changes and you are ready to use it.

Configuring Ping Watchdog

This feature allows administrator to automatically reboot an AP/SM when there is a network issue to avoid power on reset of radios. This feature is disabled by default.

To enable Ping Watchdog feature, select the menu option Configuration > Ping Watchdog, and configure the parameters listed in the following table.

Table 93: Ping Watchdog attributes



Attribute	Meaning
Ping Watchdog	This filed enables or disbales Ping Watchdog feature.
IP Address To Ping	This field specifies the IPV4 address of the device which needs to be pinged.
Ping Interval	This field specifies the time interval at which ping needs to be initiated. The time interval needs to be specified in seconds.
Ping Failure Count To Reboot	This field specifies the count of ping failures at which reboot needs to be initiated.

Chapter 2: Tools

The AP and SM GUIs provide several tools to analyze the operating environment, system performance and networking, including:

- Using Spectrum Analyzer tool
- Using the Alignment Tool
- Using the Link Capacity Test tool
- Using AP Evaluation tool
- Using BHM Evaluation tool
- Using the OFDM Frame Calculator tool
- Using the Subscriber Configuration tool
- Using the Link Status tool
- Using BER Results tool
- Using the Sessions tool
- Using the Ping Test tool

Using Spectrum Analyzer tool

The integrated spectrum analyzer can be very useful as a tool for troubleshooting and RF planning, but is not intended to replicate the accuracy and programmability of a high-end spectrum analyzer, which sometime can be used for other purposes.

The AP/BHM and SM/BHS perform spectrum analysis together in the Sector Spectrum Analyzer tool.

Caution

On start of the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. When choosing Start Timed Spectrum Analysis, the scan is run for time specified in the Duration configuration parameter. When choosing Start Continuous Spectrum Analysis, the scan is run continuously for 24 hours, or until stopped manually (using the Stop Spectrum Analysis button).

Caution

On start of the Spectrum Analyzer on a module, it enters a scan mode and drops any RF connection it may have had. When choosing Start Timed Spectrum Analysis, the scan is run for time specified in the Duration configuration parameter. When choosing Start Continuous Spectrum Analysis, the scan is run continuously for 24 hours, or until stopped manually (using the Stop Spectrum Analysis button).

Any module can be used to see the frequency and power level of any detectable signal that is within, just above, or just below the frequency band range of the module.

> **Note**
>
> Vary the days and times when you analyze the spectrum in an area. The RF environment can change throughout the day or throughout the week.

> **Caution**
>
> If the **Perform Spectrum Analysis on Boot Up for One Scan** option is enabled on the AP (accessible under **Tool** > **Spectrum Analyzer**), and the AP undergoes a reboot (whether due to a Channel Bandwidth change or any other reason) the SMs may switch from the Last known primary AP scan to the normal scan by the time spectrum analysis has completed. To mitigate this, operators may want to consider disabling the **Perform Spectrum Analysis on Boot Up for One Scan** option before reboot.

Mapping RF Neighbor Frequencies

The neighbor frequencies can be analyzed using Spectrum Analyzer tool. Following modules allow user to:

- Use a BHS or BHM for PTP and SM or AP for PMP as a Spectrum Analyzer.
- View a graphical display that shows power level in RSSI and dBm at 5 MHz increments throughout the frequency band range, regardless of limited selections in the Custom Radio Frequency Scan Selection List parameter of the SM/BHS.
- Select an AP/BHM channel that minimizes interference from other RF equipment.

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

Temporarily deploy a SM/BHS for each frequency band range that need to monitor and access the Spectrum Analyzer tab in the Tools web page of the module.

- Using Spectrum Analyzer tool
- Using the Remote Spectrum Analyzer tool

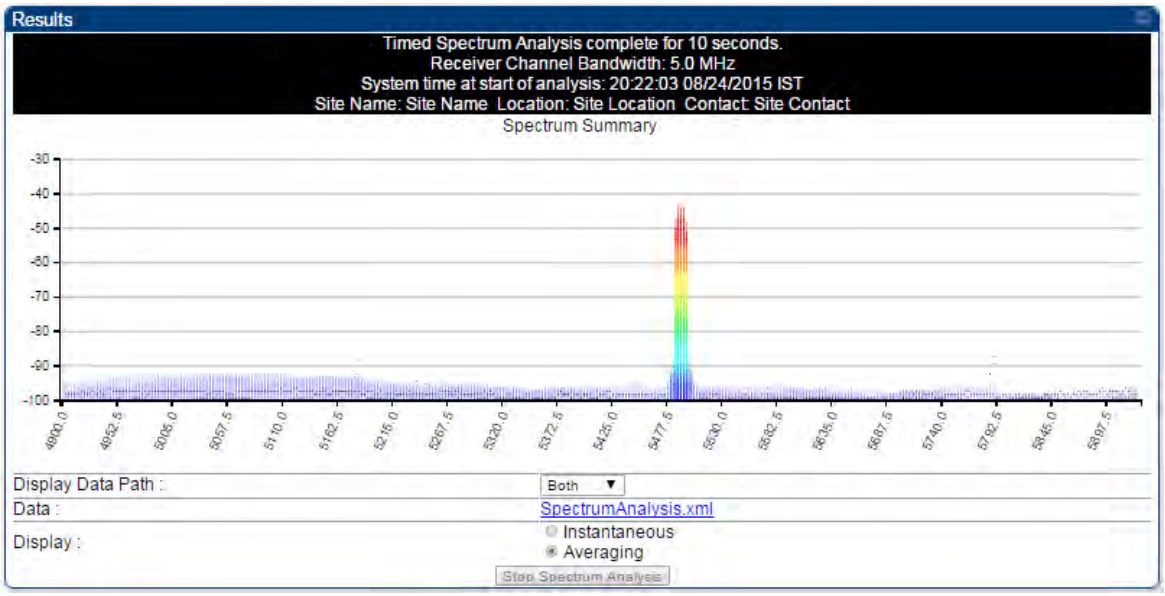
Spectrum Analyzer tool

Analyzing the spectrum

To use the built-in spectrum analyzer functionality of the AP/SM/BH, proceed as follows:

Procedure 22 Analyzing the spectrum

1	Predetermine a power source and interface that works for the AP/SM/BH in the area to be analyzed.

2	Take the AP/SM/BH, power source and interface device to the area.
3	Access the Tools > Spectrum Analyzer web page of the AP/SM/BH.
4	Enter Duration in Timed Spectrum Analyzer Tab. Default value is 10 Seconds
5	Click Start Timed Sector Spectrum Analysis
6	The results are displayed: Figure 83: *Spectrum analysis - Results*  **Note** AP/SM/BH scans for extra 40 seconds in addition to configured Duration
7	Travel to another location in the area to BHS.
8	Click Start Timed Spectrum Analysis
9	Repeat Steps 4 and 6 until the area has been adequately scanned and logged.

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

> **Note**
>
> Wherever the operator finds the measured noise level is greater than the sensitivity of the radio that is plan to deploy, use the noise level (rather than the link budget) for your link feasibility calculations.
>
> The AP/SM/BH perform spectrum analysis together in the Sector Spectrum Analyzer feature.

Graphical spectrum analyzer display

The AP/SM/BH display the graphical spectrum analyzer. An example of the Spectrum Analyzer page is shown in Spectrum analysis - Results.

The navigation feature includes:

- Results may be panned left and right through the scanned spectrum by clicking and dragging the graph left and right
- Results may be zoomed in and out using mouse

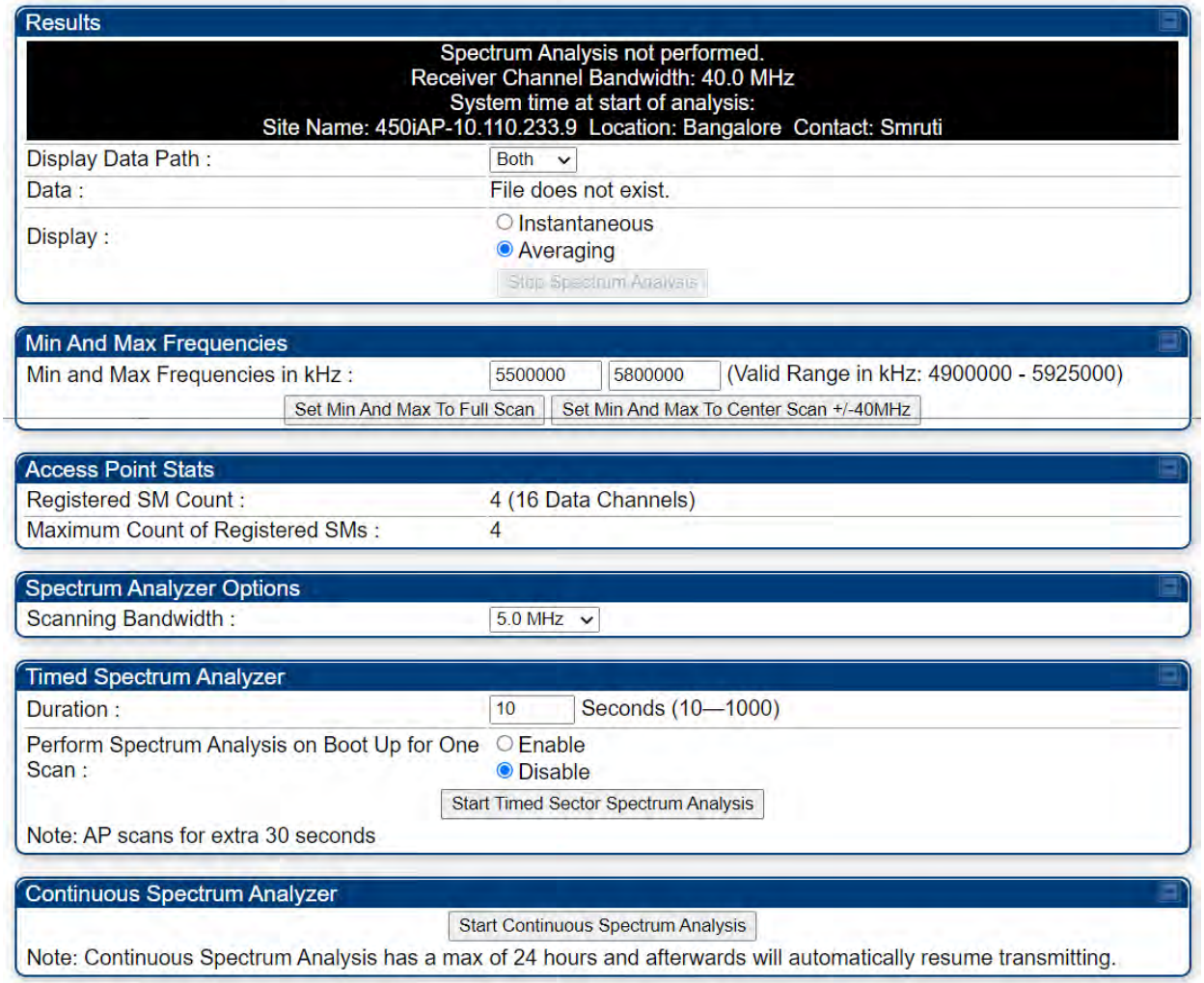
When the mouse is positioned over a bar, the receive power level, frequency, maximum and mean receive power levels are displayed above the graph

To keep the displayed data current, either set “Auto Refresh” on the module’s Configuration > General.

Spectrum Analyzer page of AP

The Spectrum Analyzer page of AP is explained in below table.

Table 94: Spectrum Analyzer page attributes - AP



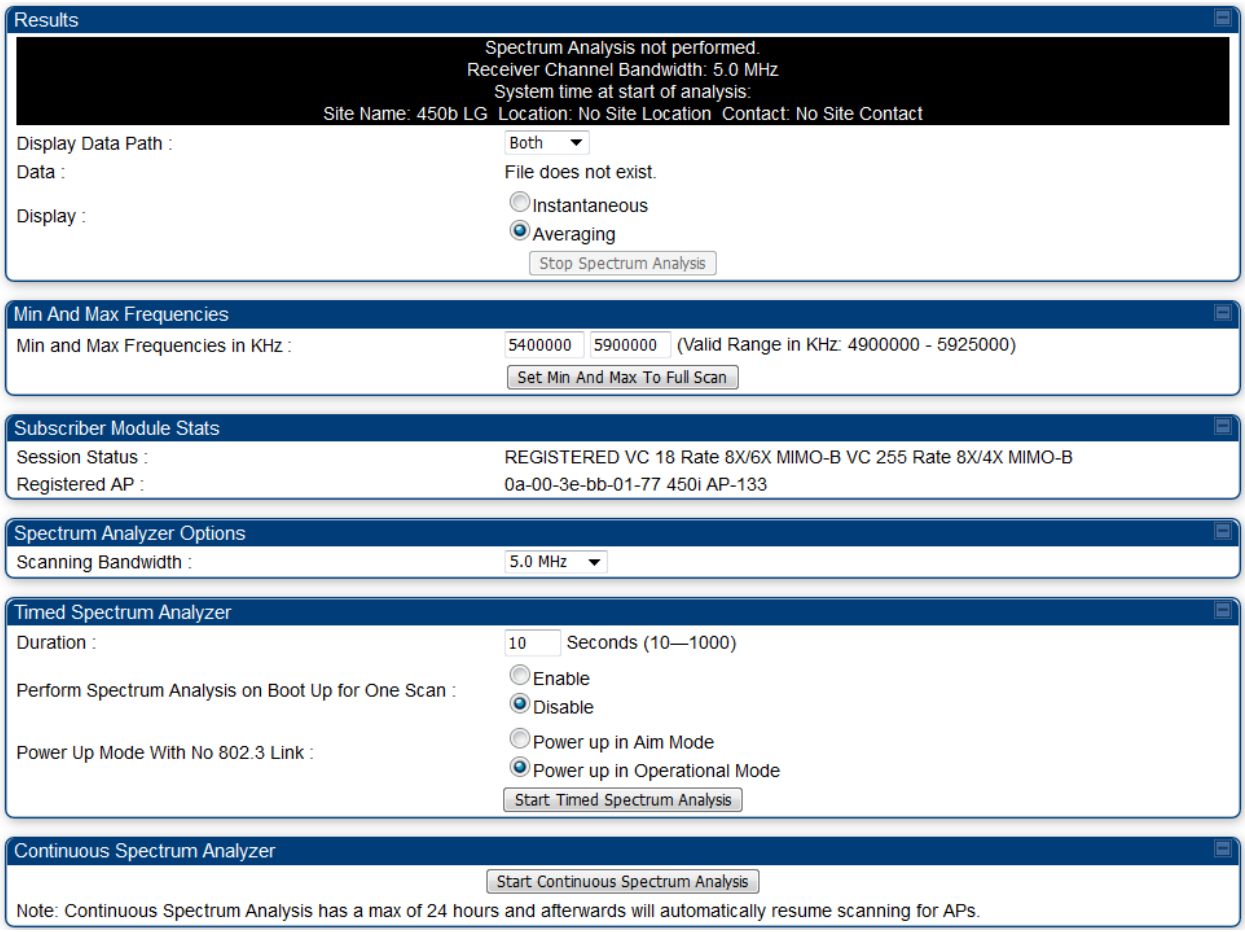
Attribute	Meaning
Display Data Path	Both means that the vertical and horizontal paths are displayed or an individual path may be selected to display only a single-path reading.
Data	For ease of parsing data and to facilitate automation, the spectrum analyzer results may be saved as an XML file. To save the results in an XML formatted file, right-click the “SpectrumAnalysis.xml” link and save the file.
Display	Instantaneous means that each reading (vertical bar) is displayed with two horizontal lines above it representing the max power level received (top horizontal line) and the average power level received (lower horizontal line) at that frequency. Averaging means that each reading (vertical bar) is displayed with an associated horizontal line above it representing the max power level received at that frequency.

Attribute	Meaning
Min and Max Frequencies in kHz	Enter minimum and maximum frequencies to be scanned.
Set Min And Max to Full Scan	On the button press, it sets minimum and maximum allowed frequencies for scanning.
Set Min And Max to Center Scan +/-40 MHz	On the button press, it sets minimum and maximum frequencies to ± 40 MHz of center frequency for scanning.
Registered SM Count	This field displays the MAC address and Site Name of the registered SM.
Maximum Count of Registered SMs	This field displays the maximum number of registered SMs.
Scanning Bandwidth	This field allows selecting scanning bandwidth for AP and all the registered SMs. **Note**: This feature is not supported in PMP 450m APs.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Perform Spectrum Analysis on Boot Up for One Scan	This field when enabled performs Spectrum Analysis on every boot up for one scan.
Continuous Spectrum Analyzer	**Start Continuous Spectrum** Analysis button ensures that when the SM is powered on, it automatically scans the spectrum for 10 seconds. These results may then be accessed via the **Tools > Spectrum Analyzer** GUI page.

Spectrum Analyzer page of SM

The Spectrum Analyzer page of SM is explained in below table.

Table 95: Spectrum Analyzer page attributes - SM



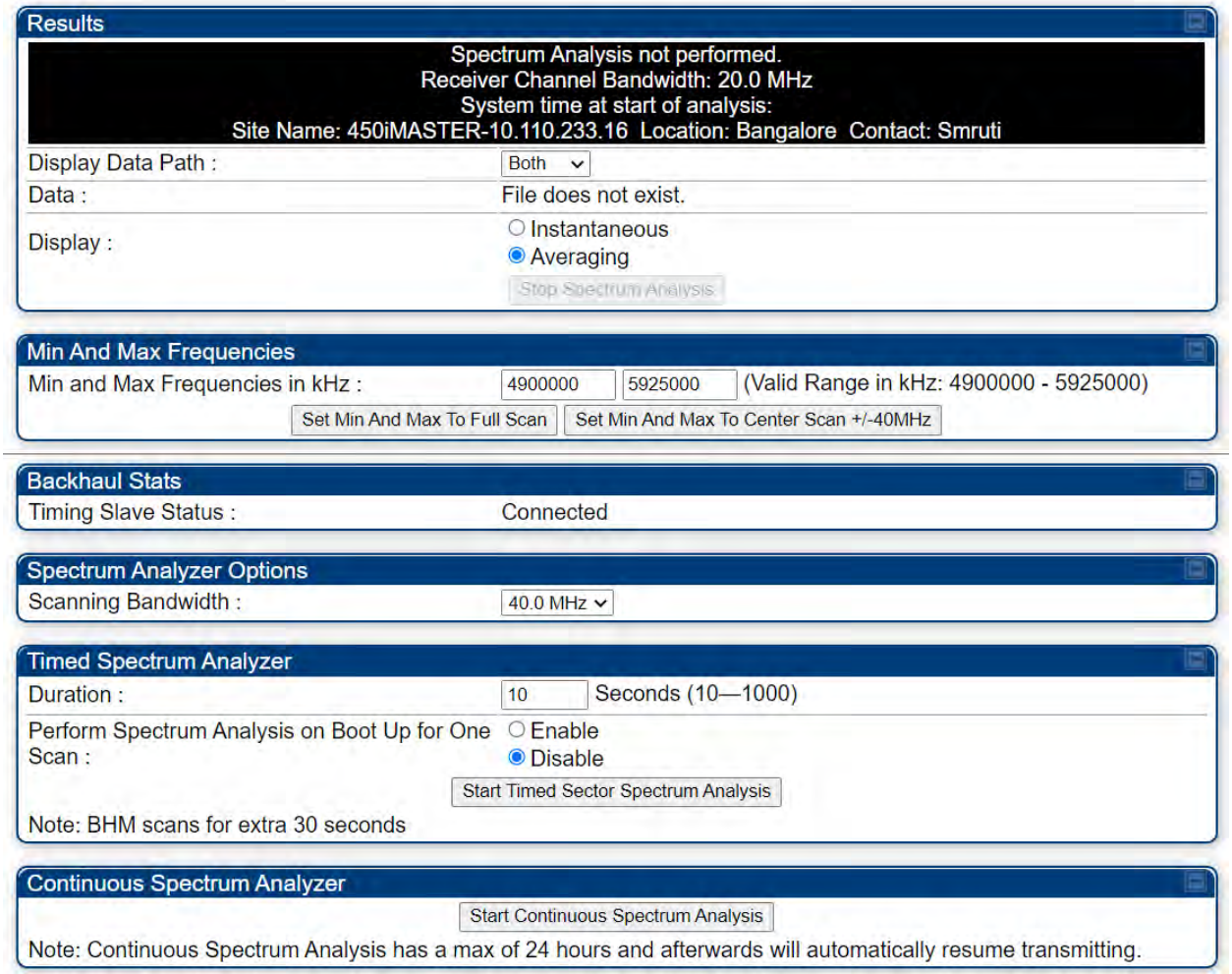
Attribute	Meaning
Display Data Path	Refer Spectrum Analyzer page attributes - AP
Data	
Display	
Min and Max Frequencies in kHz	To scan min to max range of frequencies, enter min and max frequencies in kHz and press Set Min and Max to Full Scan button. To scan +/- 40 MHz from center frequency, enter center frequency in kHz and press Set Min And Max To Center Scan +/- 40 MHz button.
Session Status	This field displays current session status and rates. The session states can be Scanning, Syncing, Registering or Registered.
Registered AP	This field displays the information of AP to which this device is registered.
Scanning Bandwidth	This field allows to select the scanning bandwidth when running Spectrum Analysis.
Duration	Refer Spectrum Analyzer page attributes - AP .

Attribute	Meaning
Perform Spectrum Analysis on Boot Up for One Scan	This field when enabled performs Spectrum Analysis on every boot up for one scan.
Power Up Mode With No 802.3 Link	This field indicates whether the link has to operate in Aim mode or in operational mode on power up.
Continuous Spectrum Analyzer	Start Continuous Spectrum Analysis button starts the SM in Spectrum Analysis until manually stopped, or it has scanned for 24 hours.

Spectrum Analyzer page of BHM

The Spectrum Analyzer page of BHM is explained in below table.

Table 96: Spectrum Analyzer page attributes - BHM

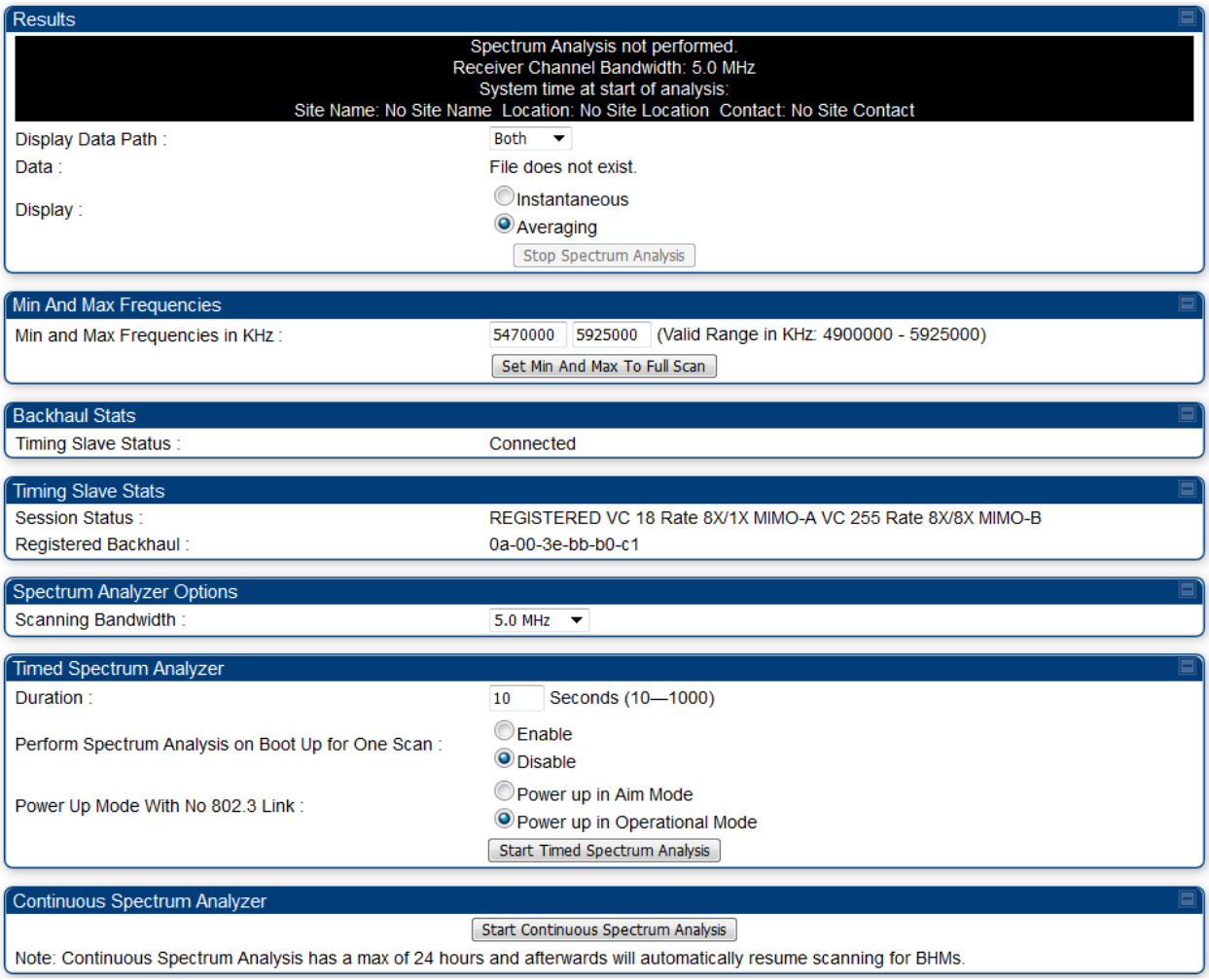


Attribute	Meaning
Data	Refer Spectrum Analyzer page attributes - AP
Display	
Duration	
Min and Max Frequencies in kHz	Enter minimum and maximum frequencies to be scanned.
Set Min And Max to Full Scan	On the button press, it sets minimum and maximum allowed frequencies for scanning.
Set Min And Max to Center Scan +/- 40 MHz	On the button press, it sets minimum and maximum frequencies to +/- 40 MHz of center frequency for scanning.
Timing Slave Status	This field displays the status of any registered Timing Slave.
Scanning Bandwidth	This field allows to select scanning bandwidth for both BHM and BHS.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Perform Spectrum Analysis on Boot Up for One Scan	This field when enabled performs Spectrum Analysis on every boot up for one scan.
Continuous Spectrum Analyzer	Start Continuous Spectrum Analysis button starts the SM in Spectrum Analysis until manually stopped, or it has scanned for 24 hours.

Spectrum Analyzer page of BHS

The Spectrum Analyzer page of BHS is explained in below table.

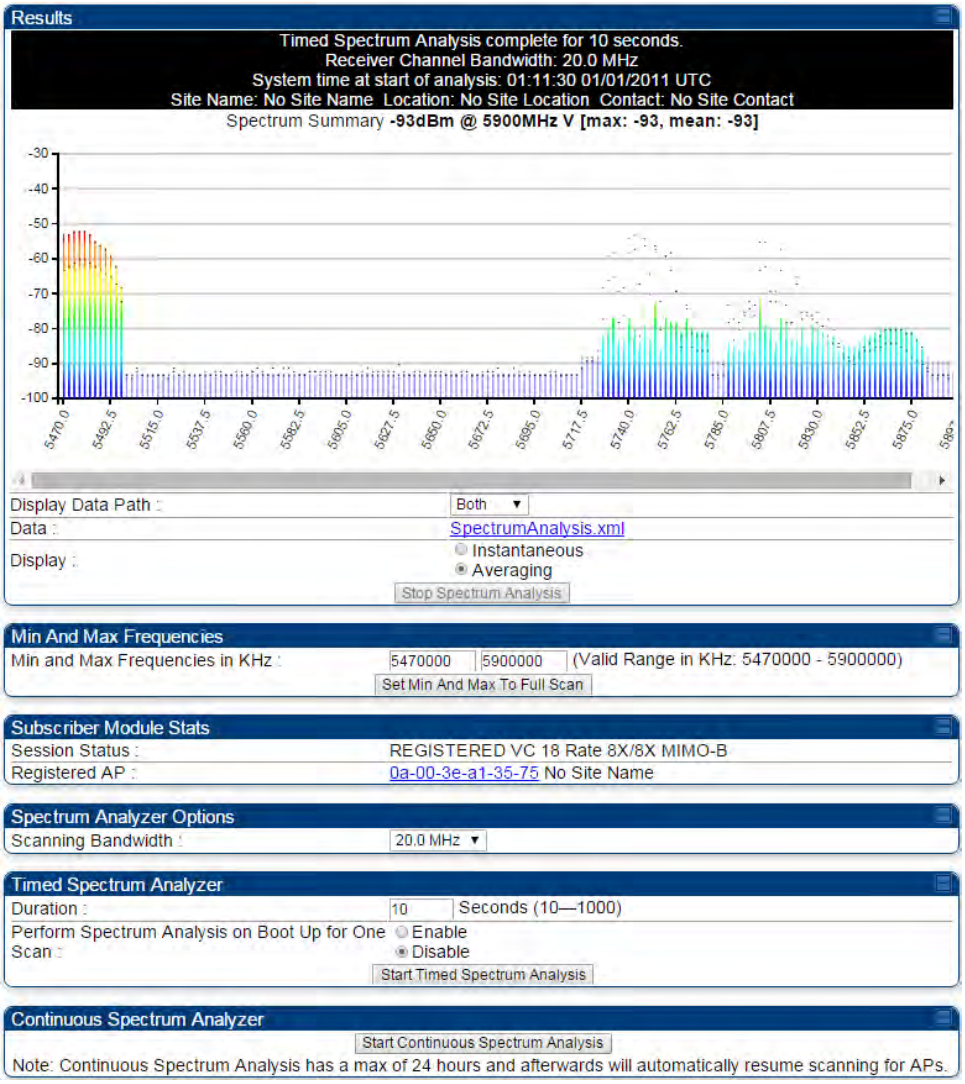
Table 97: Spectrum Analyzer page attributes - BHS



Attribute	Meaning
Data	Refer Spectrum Analyzer page attributes - AP
Display	
Session Status	This field displays current session status and rates. The session states can be Scanning, Syncing, Registering or Registered.
Registered Backhaul	This field displays MAC address of BHM and PTP model number
Duration	Refer Spectrum Analyzer page attributes - AP
Perform Spectrum Analysis on Boot Up for one scan	This field allows to Enable or Disable to start Spectrum Analysis on boot up of module for one scan.
Continuous Spectrum Analyzer	Refer Spectrum Analyzer page attributes - AP on page Spectrum Analyzer page attributes - AP

Spectrum Analyzer page result of PMP 450 SM

Figure 84: *Spectrum Analyzer page result – PMP 450 SM*



Remote Spectrum Analyzer tool

The Remote Spectrum Analyzer tool in the AP/BHM provides additional flexibility in the use of the spectrum analyzer in the SM/BHS. Set the duration of 10 to 1000 seconds, then click the Start Remote Spectrum Analysis button to launch the analysis from that SM/BHS.

In PMP configuration, a SM must be selected from the drop-down list before launching Start Remote Spectrum Analysis.

Analyzing the spectrum remotely

Procedure 23 Remote Spectrum Analyzer procedure

1	The AP/BHM de-registers the target SM/BHS.

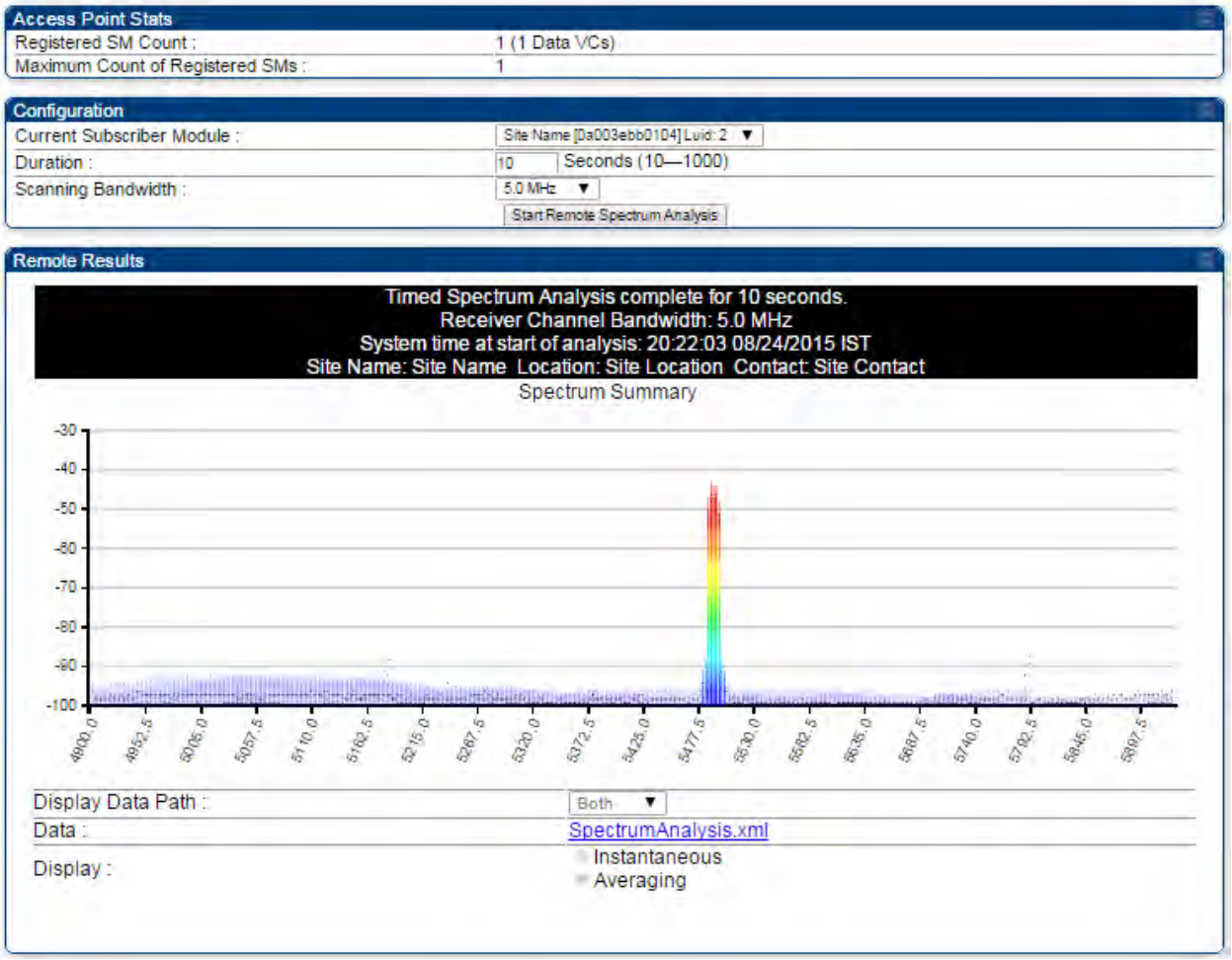
2	The SM/BHS scans (for the duration set in the AP/BHM tool) to collect data for the bar graph.
3	The SM/BHS re-registers to the AP/BHM.
4	The AP/BHM displays the bar graph.

The bar graph is an HTML file, but can be changed to an XML file, which is then easy to analyze using scripts that you may write for parsing the data. To transform the file to XML, click the "SpectrumAnalysis.xml" link below the spectrum results. Although the resulting display appears mostly unchanged, the bar graph is now coded in XML. You can now right-click on the bar graph for a Save Target As option to save the Spectrum Analysis.xml file.

Remote Spectrum Analyzer page of AP

The Remote Spectrum Analyzer page of AP is explained in below table.

Table 98: Remote Spectrum Analyzer attributes - AP

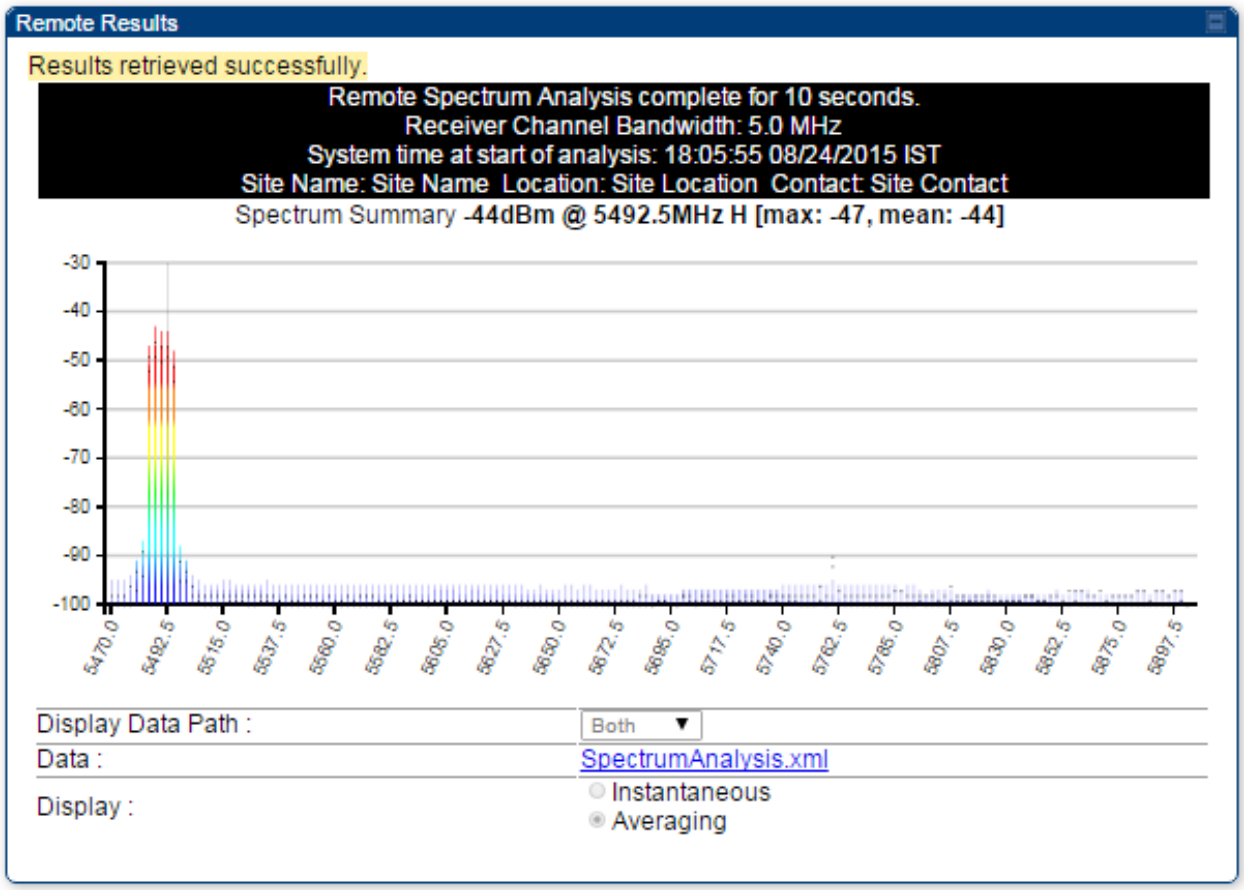


Attribute	Meaning
Registered SM Count	This field displays the number of SMs that were registered to the AP before the SA was started. This helps the user know all the SMs re-registered after performing a SA.
Maximum Count of Registered SMs	This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.
Current Subscriber Module	The currently selected SM. This is used on multiple pages.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.
Scanning Bandwidth	This parameter defines the size of the channel scanned when running the analyzer.

Remote Spectrum Analyzer page of BHM

The Remote Spectrum Analyzer page of BHM is explained in below table.

Table 99: Remote Spectrum Analyzer attributes - BHM



Attribute	Meaning
Duration	Refer Spectrum Analyzer page attributes - AP

> Note
>
> To get best performance of the link, the user has to ensure the maximum Receive Power Level during alignment by pointing correctly. The proper alignment is important to prevent interference in other cells. The achieving Receive Power Level green (>- 70 dBm) is not sufficient for the link.

Using the Alignment Tool

The SM's or BHS's Alignment Tool may be used to maximize Receive Power Level, Signal Strength Ratio and Signal to Noise Ratio to ensure a stable link. The Tool provides color coded readings to facilitate in judging link quality.

Figure 85: *Alignment Tool tab of SM – Receive Power Level > -70 dBm*

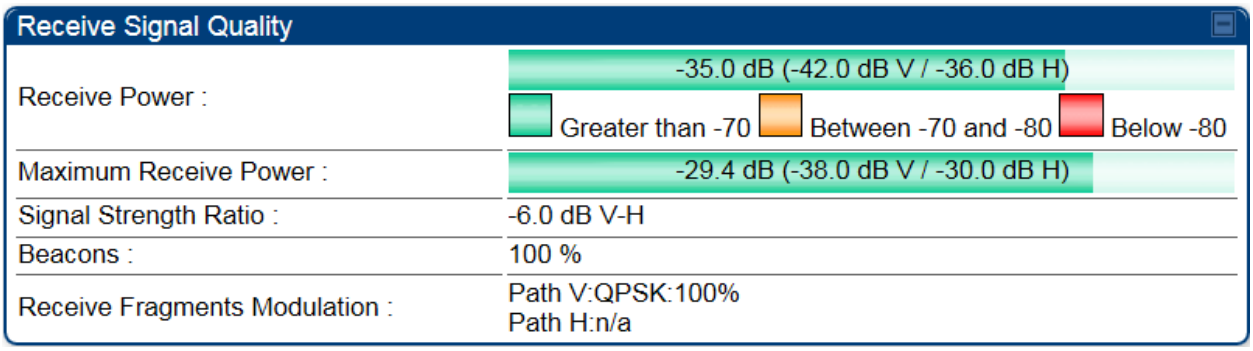


Figure 86: *Alignment Tool tab of SM – Receive Power Level between -70 to -80 dBm*

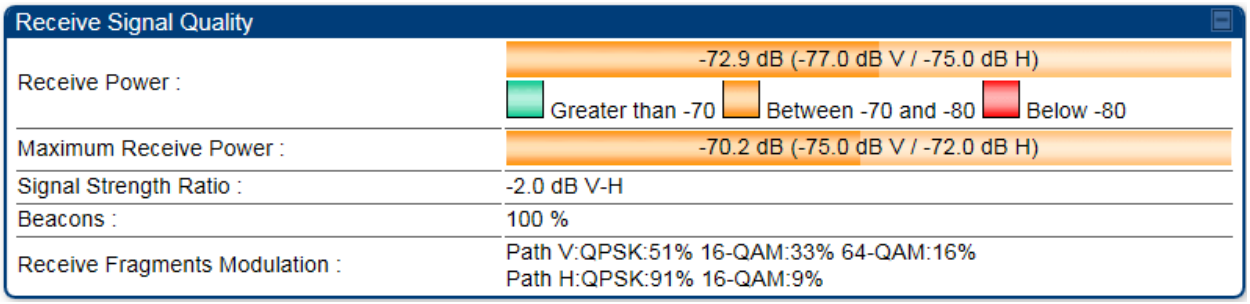
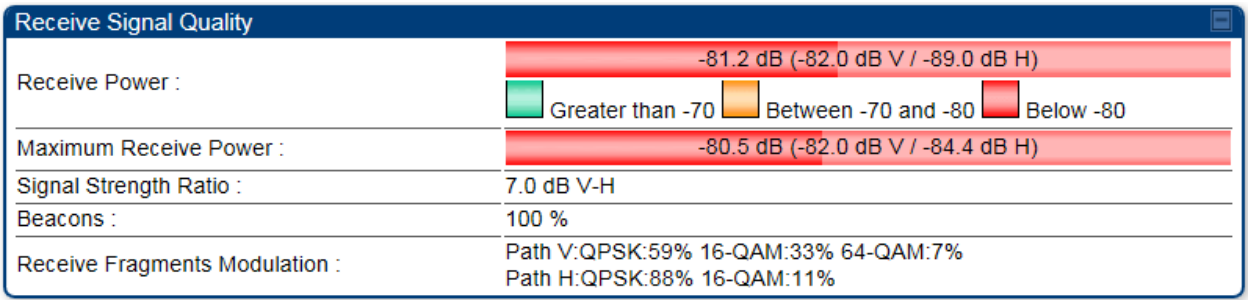


Figure 87: *Alignment Tool tab of SM – Receive Power Level < -80 dBm*



Aiming page and Diagnostic LED – SM/BHS

The SM's/BHS's Alignment Tool (located in GUI **Tools -> Aiming**) may be used to configure the SM's/BHS's LED panel to indicate received signal strength and to display decoded beacon information/power levels. The SM/BHS LEDs provide different status based on the mode of the SM/BHS. A SM/BHS in "operating" mode will register and pass traffic normally. A SM/BHS in "aiming" mode will not register or pass traffic, but will display (via LED panel) the strength of received radio signals (based on radio channel selected via **Tools ->Aiming**). See SM/BHS LEDs in Planning and Installation Guide.

> Note
>
> For accurate power level readings to be displayed, traffic must be present on the radio link.

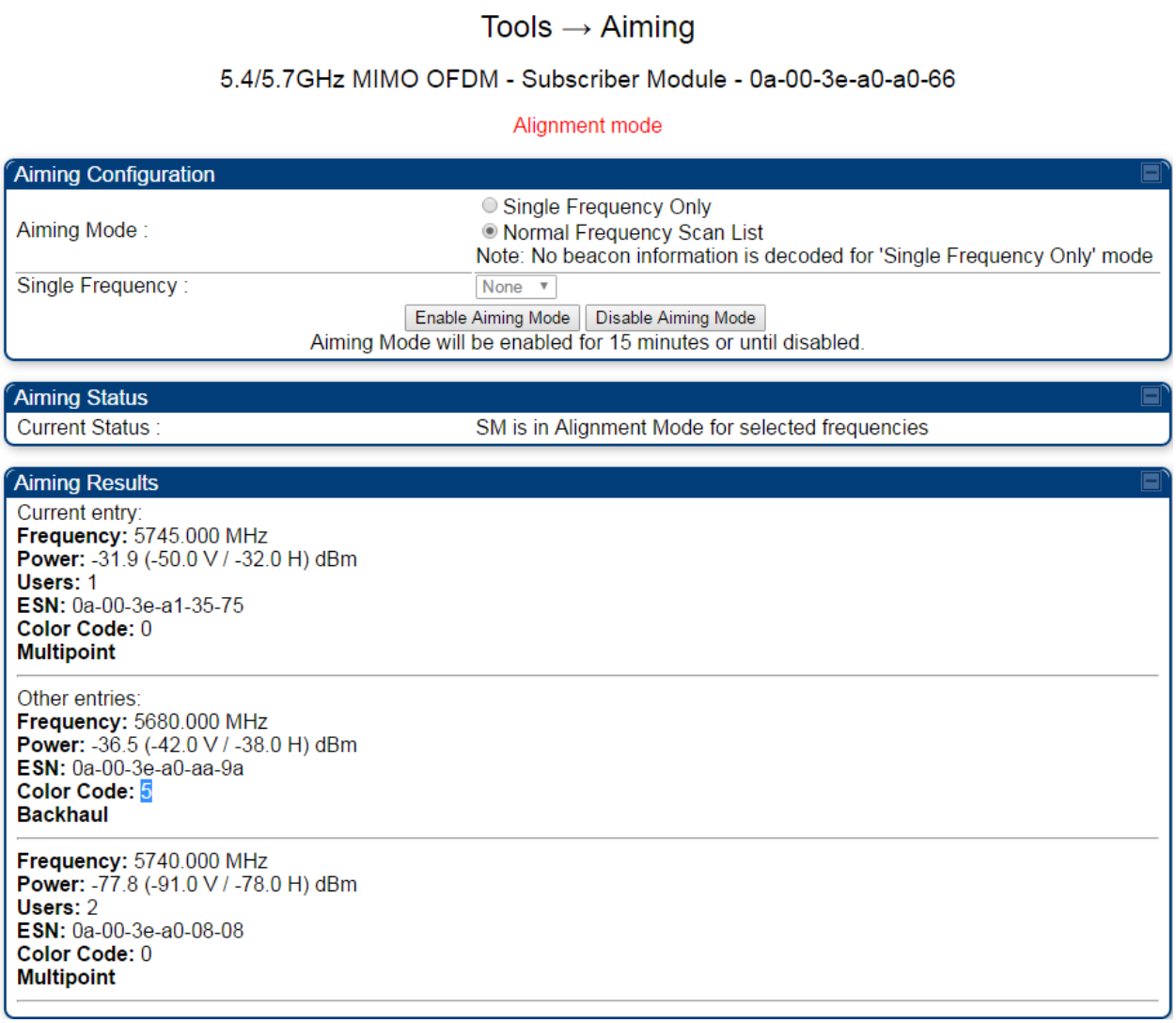
Refer SM/BHS LED description in Planning and Installation Guide for SM/BHS LED details.

Aiming page of SM

The Aiming page is similar to Spectrum Analyzer where it scans the spectrum but it does not establish any session with any APs. It has two modes – Single Frequency Only and Normal Frequency Scan List.

The Aiming page of SM is explained in below table.

Table 100: Aiming page attributes – SM



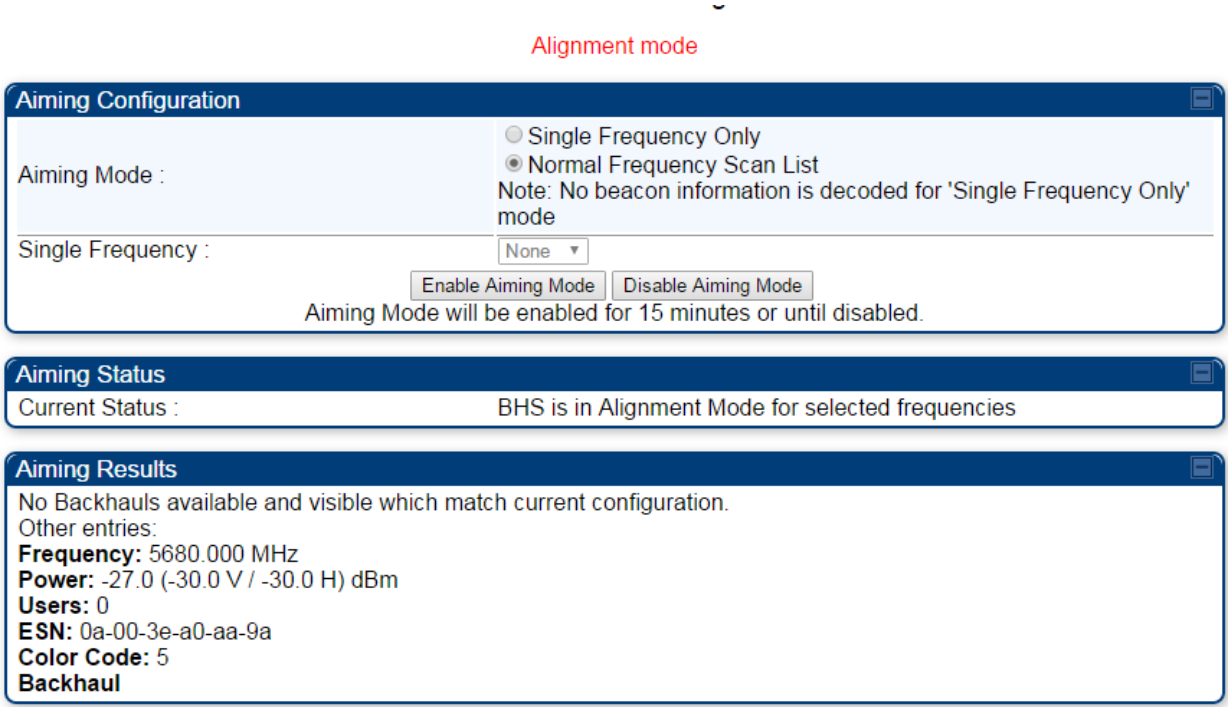
Attribute	Meaning
Aiming Mode	Single Frequency Only: scans only selected single frequency. Normal Frequency Scan List: scans: scans all frequency of scan list.
Single Frequency	Select a particular frequency from drop-down menu for scanning.
Scan Radio Frequency Only Mode	Enabled: the radio is configured to “aiming” or “alignment” mode, wherein the LED panel displays an indication of receive power level. See SM/BHS LED description in Planning and Installation Guide. Disabled: the radio is configured to “operating” mode, wherein the SM registers and passes traffic normally.
Aiming Results	The Aiming Results are displayed in two sections – Current entry and Other entries.

Attribute	Meaning
	Frequency: this field indicates the frequency of the AP which is transmitting the beacon information. Power: This field indicates the current receive power level (vertical channel) for the frequency configured in parameter Radio Frequency. Users: This field indicates the number of SMs currently registered to the AP which is transmitting the beacon information. ESN: This field indicates the MAC, or hardware address of the AP/BHM which is transmitting the beacon information. Color Code: This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes). Multipoint or Backhaul: this field indicates type of configuration - point-Multipoint (PMP) or Backhaul (PTP).

Aiming page of BHS

The Alignment page of BHS is explained in below table.

Figure 88: *Aiming page attributes - BHS*



Attribute	Meaning
Refer Aiming page attributes – SM for attribute details.	

> **Note**
>
> The Alignment Tone cable for a 450i Series uses an RJ-45 to headset cable whereas the 450 Series alignment tone cable uses an RJ-12 to headset cable.

Alignment Tone

For coarse alignment of the SM/BHS, use the Alignment Tool located at Tools ->Alignment Tool. Optionally, connect a headset alignment tone kit to the AUX/SYNC port of the SM/BHS and listen to the alignment tone, which indicates greater SM/BHS receive signal power by pitch. By adjusting the SM's/BHS's position until the highest frequency pitch is obtained operators and installers can be confident that the SM/BHS is properly positioned. For information on device GUI tools available for alignment, see sections Aiming page and Diagnostic LED – SM/BHS, Using the Link Capacity Test tooland Using AP Evaluation tool.

Figure 89: *PMP/PTP 450i Series link alignment tone*

Alignment Tool Headset and alignment tone adapters can be ordered from Cambium and Best-Tronics (http://btpa.com/Cambium-Products/) respectively using the following part numbers:

Table 101: Alignment Tool Headsets and Alignment tone adapter third party product details

Reference	Product description
ACATHS-01A	Alignment tool headset for the PMP/PTP 450 and 450i Series products
BT-1277	Headset alignment cable (RJ-45) for the PMP/PTP 450i Series products
BT-0674	Headset alignment cable (RJ-12) for the PMP/PTP 450 Series products.

Using the Link Capacity Test tool

The Link Capacity Test tab allows you to measure the throughput and efficiency of the RF link between two modules. Many factors, including packet length, affect throughput.

The Link Capacity Test tool has following modes:

- Link Test with Multiple VCs: Tests radio-to-radio communication across selected or all registered VCs, but does not bridge traffic (PMP 450m Series AP only).
- Link Test without Bridging: Tests radio-to-radio communication, but does not bridge traffic.
- Link Test with Bridging: Bridges traffic to “simulated” Ethernet ports, providing a status of the bridged link.
- Link Test with Bridging and MIR: Bridges the traffic during test and also adheres to any MIR (Maximum Information Rate) settings for the link.
- Extrapolated Link Test: Estimates the link capacity by sending few packets and measuring link quality.

The Link Capacity Test tab contains the settable parameter Packet Length with a range of 64 to 1714 bytes. This allows you to compare throughput levels that result from various packet sizes.

The Current Results Status also displayed date and time of last performed Link Capacity Test. If there is any change in time zone, the date and time will be adjusted accordingly.

Note

The Extrapolated Link Test can be run by Read-Only login also.

Performing Link Test

The link test is a tool that allows the user to test the performance of the RF link. Packets are added to one or more queues in the AP in order to fill the frame. Throughput and efficiency are then calculated during the test. The 450 and 450i APs offer link test options to one SM at a time. The 450m AP offers the option of a link test to multiple VCs at the same time. This allows the user to test throughput in MU-MIMO mode, in which multiple SMs are served at the same time.

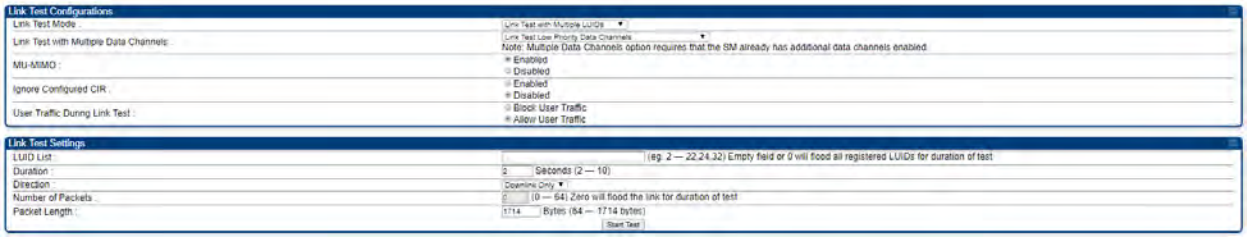
This new link test can be found under **Tools > Link Capacity Test.**

Link Test with Multiple LUIDs

Note

The “Link Test with Multiple LUIDs” Link Capacity Test is supported for PMP 450m Series AP only.

Figure 90: *Link Capacity Test – PMP 450m Series AP*



Procedure 24 Performing a Link Capacity Test - Link Test with Multiple LUIDs

Link Test Configurations parameters	
1	Access the Link Capacity Test tab in the Tools web page of the module.
2	Set Link Test Mode attribute to Link Test with Multiple LUIDs.
3	Set Link with Multiple Data Channels attribute to Link Test Low Priority Data Channels, Link Test Low and Medium Priority Data Channels, Link Test Low, Medium and High Priority Data Channels, or Link Test All Data Channels.
4	Set the MU-MIMO attribute to Enabled or Disabled. Note: The MU-MIMO feature is enabled on the Low Priority Data Channel only
5	Set the Ignore Configured CIR attribute to Enabled or Disabled.
6	Set the User Traffic During Link Test attribute to Block User Traffic or Allow User Traffic.
Link Test Settings parameters	
7	Enter LUID List (applicable for PMP 450m AP only) The Current Subscriber Module and LUID List are valid only when selecting Link Test with Multiple LUIDs. • Current Subscriber Module: select the LUID to perform the link test with • LUID list: select a list or range of LUIDs to include in the link test with multiple LUIDs If left blank, all LUIDs will be included in the link test
8	Type into the Duration field how long (in seconds) the RF link must be tested.
9	Select the Direction attribute to Bi-directional, Uplink Only, or Downlink Only.
10	Type into the Number of Packets field a value of 0 to flood the link for the duration of the test.
11	Type into the Packet Length field a value of 1714 to send 1714-byte packets during the test.
12	Click the Start Test button.

Figure 91: *Link Test with Multiple LUIDs*

Current Results Status

Test Duration: 10 Pkt Length: 1714 Test Direction Bi-Directional

Link Test with Multiple LUIDs

Flood Test Summary

Throughput			Average Group Size	
Downlink	Uplink	Aggregate	Downlink	Uplink
179.86 Mbps	206.49 Mbps	386.35 Mbps	7.0	6.9

Detailed Flood Test Statistics

Subscriber Module	LUID	Data Channel Priority	Tested	Throughput		Efficiency		Average Rate		Grouping Ratio	
				Downlink	Uplink	Downlink	Uplink				
				179.86 Mbps	206.49 Mbps	99%	96%	Transmit	Receive	Downlink	Uplink
SM01 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-1 - 10.120.247.120 - [0a-00-3e-b4-25-49]	019	Low	Yes	8.48 Mbps	9.78 Mbps	99%	96%	5.5X	5.8X	100%	99%
SM02 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-1 - 10.120.247.103 - [0a-00-3e-b4-26-df]	017	Low	Yes	8.42 Mbps	9.59 Mbps	99%	94%	5.4X	5.7X	100%	100%
SM03 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-2 - 10.120.247.104 - [0a-00-3e-b4-26-ba]	004	Low	Yes	8.45 Mbps	9.77 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM04 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-2 - 10.120.247.105 - [0a-00-3e-b4-25-59]	003	Low	Yes	8.45 Mbps	9.82 Mbps	100%	96%	5.5X	5.8X	100%	99%
SM05 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-3 - 10.120.247.112 - [0a-00-3e-b4-25-05]	012	Low	Yes	8.47 Mbps	9.74 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM06 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-3 - 10.120.247.107 - [0a-00-3e-b4-25-3a]	014	Low	Yes	8.46 Mbps	9.80 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM07 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-4 - 10.120.247.106 - [0a-00-3e-b4-23-bb]	005	Low	Yes	8.56 Mbps	9.77 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM08 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-4 - 10.120.247.113 - [0a-00-3e-b4-25-5a]	021	Low	Yes	8.49 Mbps	9.73 Mbps	99%	95%	5.5X	5.8X	100%	100%
SM09 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-5 - 10.120.247.111 - [0a-00-3e-b4-25-a9]	010	Low	Yes	8.57 Mbps	9.74 Mbps	99%	96%	5.5X	5.8X	99%	100%
SM10 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-5 - 10.120.247.118 - [0a-00-3e-b4-26-23]	022	Low	Yes	8.48 Mbps	9.80 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM11 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-6 - 10.120.247.119 - [0a-00-3e-b4-26-d1]	018	Low	Yes	8.51 Mbps	9.88 Mbps	99%	97%	5.5X	5.9X	100%	100%
SM12 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-6 - 10.120.247.117 - [0a-00-3e-b4-26-ce]	020	Low	Yes	8.48 Mbps	9.84 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM13 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-7 - 10.120.247.121 - [0a-00-3e-b4-25-17]	008	Low	Yes	10.21 Mbps	9.83 Mbps	93%	96%	6.6X	5.8X	99%	100%
SM14 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-7 - 10.120.247.122 - [0a-00-3e-b4-26-a2]	002	Low	Yes	8.47 Mbps	10.12 Mbps	100%	96%	5.5X	5.8X	100%	94%
SM15 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-8 - 10.120.247.108 - [0a-00-3e-b4-26-22]	013	Low	Yes	8.46 Mbps	9.78 Mbps	99%	96%	5.5X	5.8X	100%	100%
SM16 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-8 - 10.120.247.116 - [0a-00-3e-b4-25-fe]	016	Low	Yes	8.47 Mbps	9.88 Mbps	100%	96%	5.5X	5.8X	100%	100%
SM17 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-9 - 10.120.247.114 - [0a-00-3e-b4-25-b0]	009	Low	Yes	8.46 Mbps	9.89 Mbps	100%	97%	5.5X	5.9X	100%	100%
SM18 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-9 - 10.120.247.110 - [0a-00-3e-b4-24-21]	011	Low	Yes	8.47 Mbps	10.02 Mbps	99%	97%	5.5X	5.9X	100%	100%
SM19 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-10 - 10.120.247.102 - [0a-00-3e-b4-25-c7]	015	Low	Yes	8.47 Mbps	9.95 Mbps	99%	97%	5.5X	5.9X	100%	100%
SM20 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 2-10 - 10.120.247.115 - [0a-00-3e-b4-26-01]	006	Low	Yes	8.44 Mbps	8.09 Mbps	99%	97%	5.5X	5.8X	100%	100%
SM21 - PMP 450 - 5.4/5.7GHz MIMO OFDM - Row 1-11 - 10.120.247.109 - [0a-00-3e-b4-26-63]	007	Low	Yes	8.48 Mbps	11.57 Mbps	99%	96%	5.5X	5.8X	100%	100%

Slot Grouping

Group Size	% Downlink Distribution	% Uplink Distribution
1 (ungrouped)	0.0	1.8
2	0.0	0.0
3	0.0	0.0
4	0.0	0.0
5	0.0	0.0
6	1.6	0.0
7	98.4	98.2

Link Test ran on 13:07:33 05/09/2019 CDT

Link Test without Bridging, Link Test with Bridging or Link Test with Bridging and MIR

Figure 92: *Link Test without Bridging*

Link Test Configurations

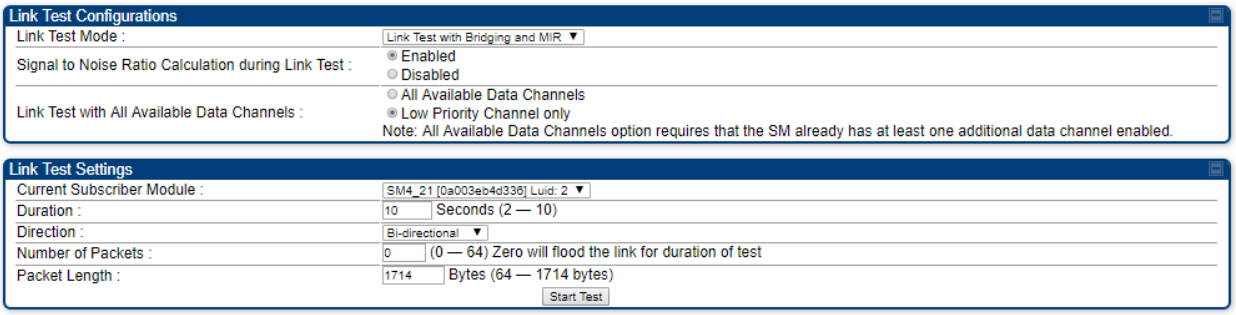
Link Test Mode :	Link Test without Bridging
Signal to Noise Ratio Calculation during Link Test :	(•) Enabled ( ) Disabled
Link Test with All Available Data Channels :	( ) All Available Data Channels (•) Low Priority Channel only Note: All Available Data Channels option requires that the SM already has at least one additional data channel enabled

Link Test Settings

Current Subscriber Module :	SM4_21 [0a003eb4d336] Luid: 2
Duration :	10 Seconds (2 — 10)
Direction :	Bi-directional
Number of Packets :	0 (0 — 64) Zero will flood the link for duration of test
Packet Length :	1714 Bytes (64 — 1714 bytes)

Start Test

Figure 93: *Link Test with Bridging and MIR*



Refer Link Test with Multiple LUIDs for Link Test procedure.

Figure 94: *Link Test without Bridging (1518-byte packet length)*

Current Results Status

Stats for LUID: 4 Test Duration: 5 Pkt Length: 1518 Test Direction Bi-Directional

Link Test without Bridging

Data Channel Priority	Downlink	Uplink	Aggregate	Packet Transmit	Packet Receive
				Actual	Actual
Low	22.70 Mbps	24.51 Mbps	47.21 Mbps, 3841 pps	9232 (1846 pps)	9977 (1995 pps)

Efficiency

Downlink				Uplink			
Efficiency	Fragments count		Signal to Noise Ratio	Efficiency	Fragments count		Signal to Noise Ratio
	Actual	Missed			Actual	Missed	
99%	221728	42	39 dB V 36 dB H	99%	239552	127	35 dB V 39 dB H

Link Quality
Downlink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors
V	QPSK	27701	25%	0.378
V	16-QAM	27702	25%	0.613
V	64-QAM	27701	25%	0.941
V	256-QAM	27700	25%	0.519
H	QPSK	27697	25%	1.719
H	16-QAM	27694	25%	2.487
H	64-QAM	27675	25%	3.287
H	256-QAM	27698	25%	1.595

Uplink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors
V	256-QAM	118324	100%	3.569
H	256-QAM	119788	100%	0.753

Link Test ran on 08:31:56 07/12/2018 UTC

Currently transmitting at:
8X/8X MIMO-B

Performing Extrapolated Link Test

The Extrapolated Link Test estimates the link capacity by sending few packets and measuring link quality. Once the test is initiated, the radio starts session at the lower modulation, 1X, as traffic is passed successfully across the link, the radio decides to try the next modulation, 2X. This process repeats until it finds best throughput to estimate capacity of link.

The procedure for performing Extrapolated Link Test is as follows:

Procedure 25 Performing an Extrapolated Link Test

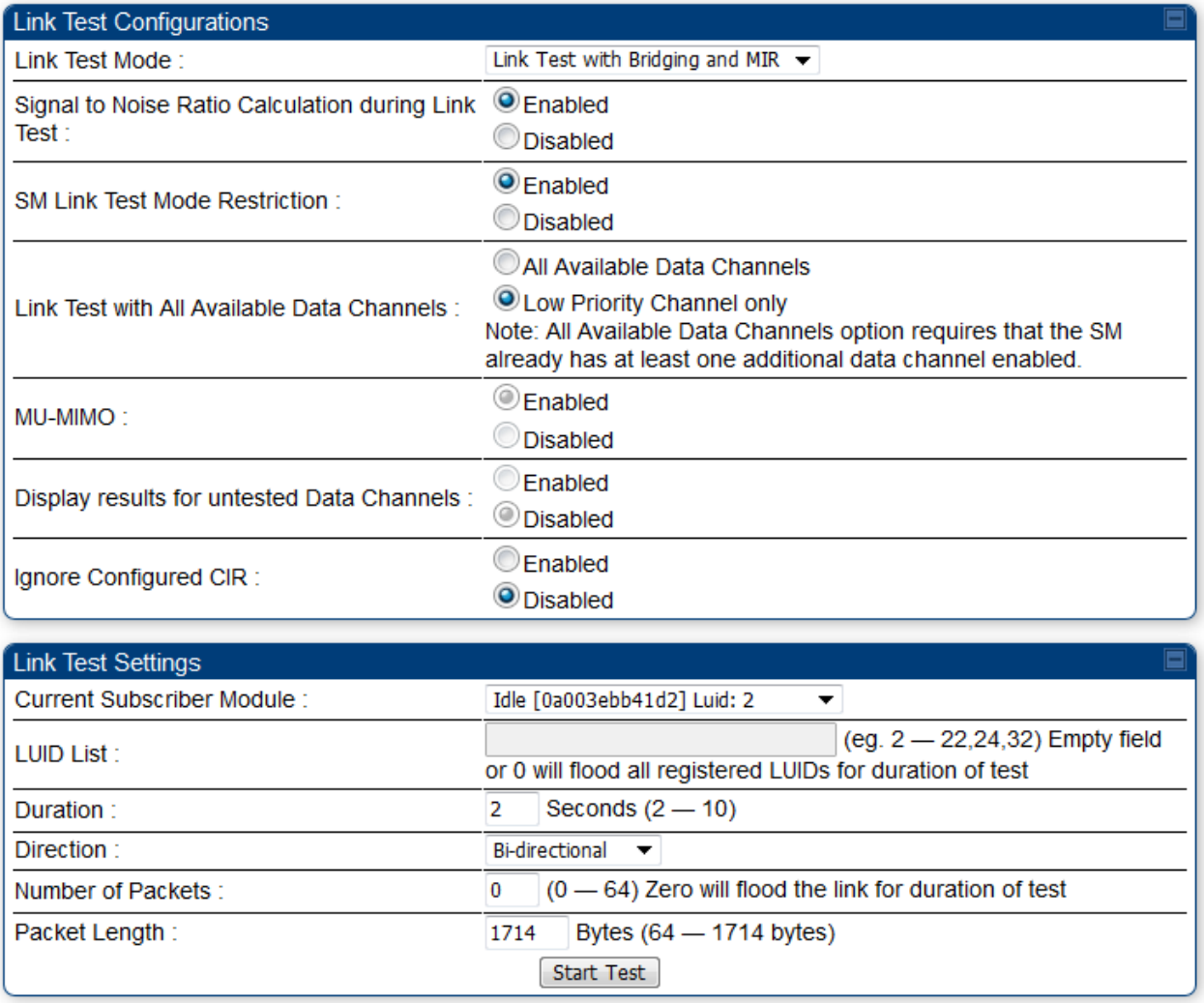
1	Access the Link Capacity Test tab in the Tools web page of the module.
2	Select Link Test Mode Extrapolated Link Test
3	Click the Start Test button.
4	In the Current Results Status block of this tab, view the results of the test.

Figure 95: *Extrapolated Link Test results*

Link Capacity Test page of AP

The Link Capacity Test page of AP is explained in below table.

Table 102: Link Capacity Test page attributes – 450m AP



Attribute	Meaning
Link Test Mode	Select Link Test Mode from drop-down menu: • Link Test with Multiple LUIDs (PMP 450m Series AP only) • Link Test without Bridging • Link Test with Bridging • Link Test with Bridging and MIR • Extrapolated Link Test

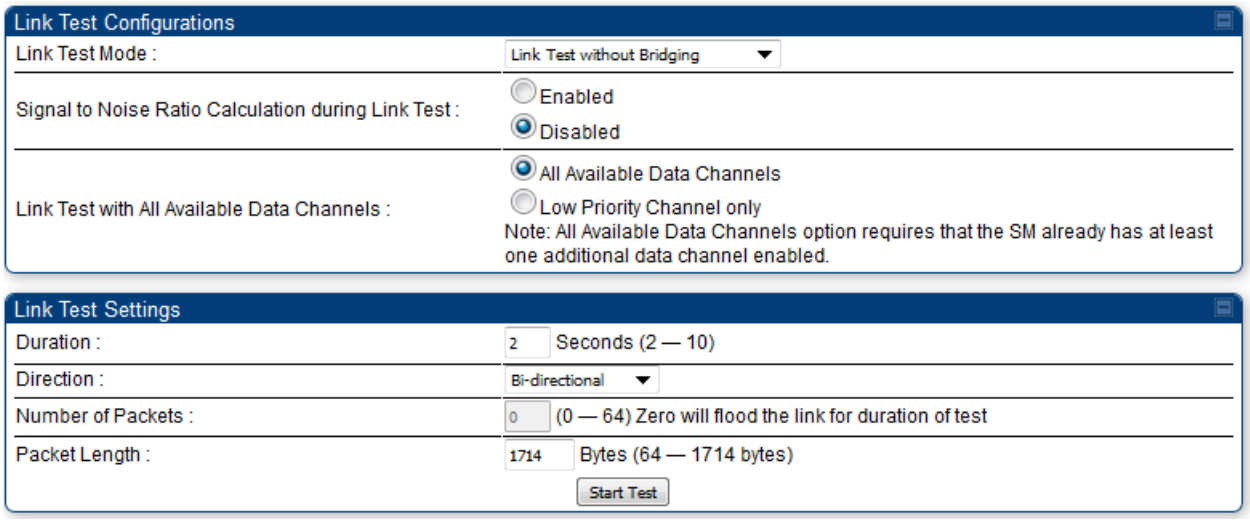
Attribute	Meaning
Signal to Noise Ratio Calculation during Link Test	Enable this attribute to display Signal-to-Noise information for the downlink and uplink when running the link test.
SM Link Test Mode Restriction	Enable this parameter to restrict SM link test mode.
Link Test with All Available Data Channels	This parameter is used to enable or disable usage of either all available data channels or low priority data channel only during the link test.
MU-MIMO	This parameter determines whether the DL flood test packets use MU-MIMO grouping or not. Note: This field is applicable only when the “Link Test Mode” field is set to “Link Test with Multiple LUIDs” option. Note: This field is applicable for PMP 450m APs only.
Display results for untested Data Channels	If “Link test with multiple VC’s” is run and a subset of registered VC’s enters into the VC List field, then enabling this field produces a table that displays results for VC’s with traffic which are in session; but not tested as part of the link test. Note: This field is applicable for PMP 450m flood tests only.
Ignore Configured CIR	Enable this parameter to schedule flood data regardless of the CIR configuration for each SM. For system release 16.1 and beyond, the exact impact of this setting depends on which scheduler "mode" has been configured by the operator on the AP's QoS page. Enabled: ‘Run Link Test with Multiple LUID's using Legacy scheduler, ignoring configured CIR's. Legacy scheduler is used here regardless of which scheduling mode has been configured. Disabled: If Legacy scheduler is enabled, test with legacy scheduler, using configured CIR's. If Proportional scheduler is enabled, test with proportional scheduler.
Current Subscriber Module	The SM with which the Link Capacity Test is run. This field is only applicable for AP (not SM page).
LUID List	This field is displayed for PMP 450m Series AP. It is only applicable for “Link Test with Multiple LUIDs” Test mode. Enter LUID List (e.g. 18 or above for low priority LUIDs and 255 or above for high priority LUIDs or 0 for all registered LUIDs) which needs to be used for link test traffic.
Duration	This field allows operators to configure a specified time for which the spectrum is scanned. If the entire spectrum is scanned prior to the end of the configured duration, the analyzer will restart at the beginning of the spectrum.

Attribute	Meaning
Direction	Configure the direction of the link test. Specify Downlink or Uplink to run the test only in the corresponding direction only. Specific Bi-Directional to run the test in both directions.
Number of Packets	The total number of packets to be sent during the Link Capacity Test. When Link Test Mode is set to Link Test Without Bridging this field is not configurable.
Packet Length	The size of the packets in Bytes to send during the Link Capacity Test

Link Capacity Test page of BHM/BHS/SM

The Link Capacity Test page of BHM/BHS is explained in below table.

Figure 96: *Link Capacity Test page attributes – BHM/BHS*



Attribute	Meaning
Link Test Mode	See Link Capacity Test page attributes – 450m AP
Signal to Noise Ratio Calculation during Link Test	
Link Test with All Available Data Channels	
Duration	
Direction	
Number of Packets	
Packet Length	

Using AP Evaluation tool

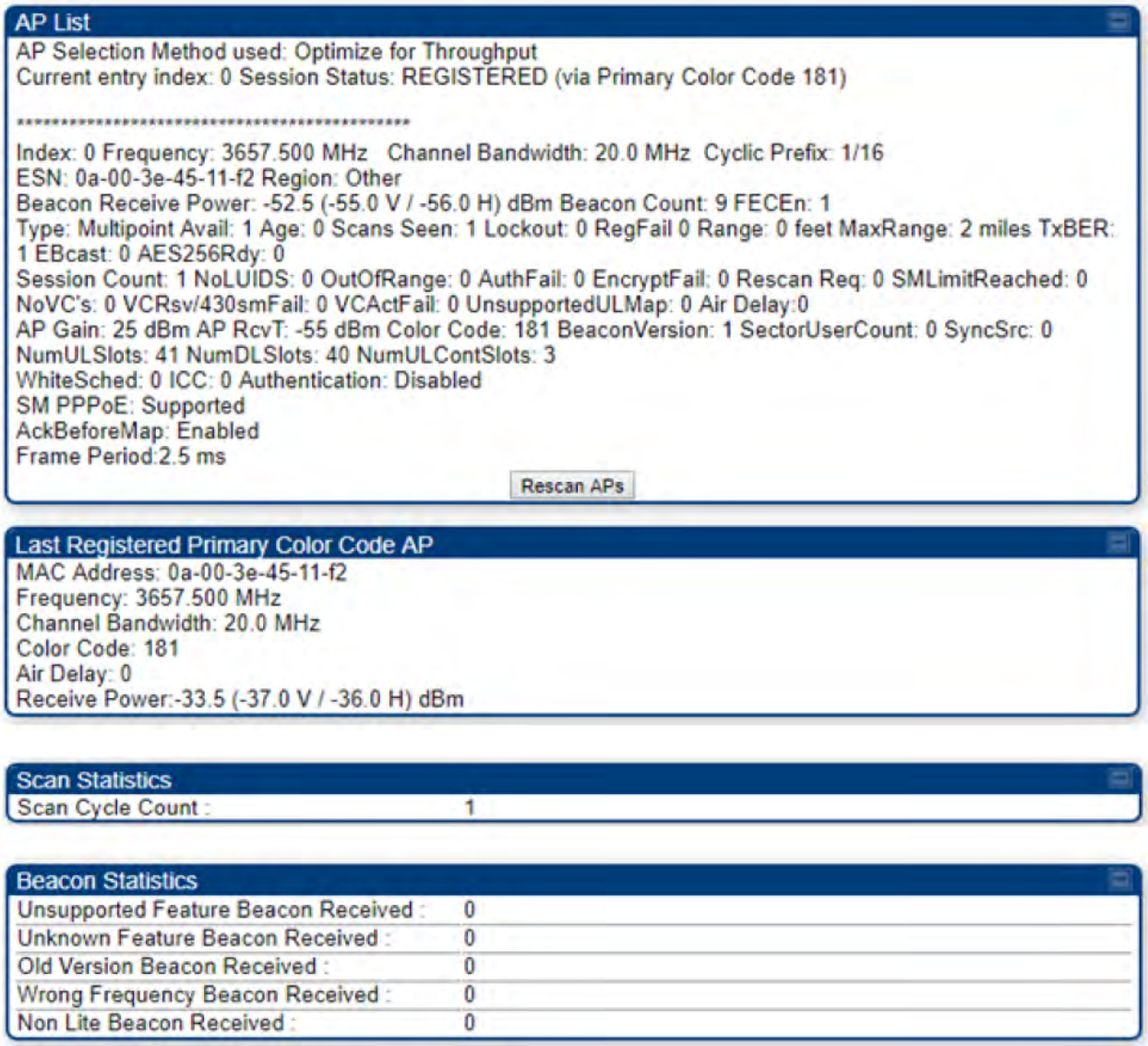
The AP Evaluation tab on Tools web page of the SM provides information about the AP that the SM sees.

> **Note**
>
> The data for this page may be suppressed by the SM Display of AP Evaluation Data setting in the Configuration > Security tab of the AP.
>
> The AP Eval results can be accessed via SNMP and config file.

AP Evaluation page

The AP Evaluation page of AP is explained in below table.

Table 103: AP Evaluation tab attributes



Attribute	Meaning
Index	This field displays the index value that the system assigns (for only this page) to the AP where this SM is registered.

Attribute	Meaning
Frequency	This field displays the frequency that the AP transmits.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the AP and the SM.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefixes mean that for every 16 bits of throughput data transmitted, an additional bit is used. The Cyclic Prefix 1/16 only can be selected at this time.
ESN	This field displays the MAC address (electronic serial number) of the AP. For operator convenience during SM aiming, this tab retains each detected ESN for up to 15 minutes. If the broadcast frequency of a detected AP changes during a 15-minute interval in the aiming operation, then a multiple instance of the same ESN is possible in the list. Eventually, the earlier instance expires and disappears and the later instance remains to the end of its interval, but you can ignore the early instance(s) whenever two or more are present.
Region	This field displays the AP's configured Country Code setting.
Power Level	This field displays the SM's combined received power level from the AP's transmission.
Beacon Count	A count of the beacons seen in a given time period.
FECEn	This field contains the SNMP value from the AP that indicates whether the Forward Error Correction feature is enabled. 0: FEC is disabled 1: FEC is enabled
Type	Multipoint indicates that the listing is for an AP.
Age	This is a counter for the number of minutes that the AP has been inactive. At 15 minutes of inactivity for the AP, this field is removed from the AP Evaluation tab in the SM.
Lockout	This field displays how many times the SM has been temporarily locked out of making registration attempts.
RegFail	This field displays how many registration attempts by this SM failed.
Range	This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.
MaxRange	This field indicates the configured value for the AP's Max Range parameter.
TxBER	A 1 in this field indicates the AP is sending Radio BER.
Ebcast	A 1 in this field indicates the AP or BHM is encrypting broadcast packets. A 0 indicates it is not.

Attribute	Meaning
Session Count	This field displays how many sessions the SM (or BHS) has had with the AP (or BHM). Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum. In the case of a multipoint link, if the number of sessions is significantly greater than the number for other SMs, then this may indicate a link problem or an interference problem.
NoLUIDs	This field indicates how many times the AP has needed to reject a registration request from a SM because its capacity to make LUID assignments is full. This then locks the SM out of making any valid attempt for the next 15 minutes. It is extremely unlikely that a non-zero number would be displayed here.
OutOfRange	This field indicates how many times the AP has rejected a registration request from a SM because the SM is a further distance away than the range that is currently configured in the AP. This then locks the SM out of making any valid attempt for the next 15 minutes.
AuthFail	This field displays how many times authentication attempts from this SM have failed in the AP.
EncryptFail	This field displays how many times an encryption mismatch has occurred between the SM and the AP.
Rescan Req	This field displays how many times a re-range request has occurred for the BHM that is being evaluated in the AP Eval page of a BHS.
SMLimitReached	This field displays 0 if additional SMs may be registered to the AP. If a 1 is displayed, the AP will not accept additional SM registrations.
NoVC's	This counter is incremented when the SM is registering to an AP which determines that no VC resources are available for allocation. This could be a primary data channel (a low priority data channel) or one of the other possible data channel priorities (a Medium priority data channel, or High priority data channel, or Ultra High priority data channel)
VCRsvFail	This counter is incremented when the SM is registering to an AP which has a VC resource available for allocation but cannot reserve the resource for allocation.
VCActFail	This counter is incremented when the SM is registering to an AP which has a VC resource available for allocation and has reserved the VC, but cannot activate the resource for allocation.
AP Gain	This field displays the total external gain (antenna) used by the AP.
RcvT	This field displays the AP's configured receive target for receiving SM transmissions (this field affects automatic SM power adjust).
Sector ID	This field displays the value of the Sector ID field that is provisioned for the AP.
Color Code	This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.

Attribute	Meaning
	Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes).
BeaconVersion	This field indicates that the beacon is OFDM (value of 1).
Sector User Count	This field displays how many SMs are registered on the AP.
NumULHalfSlots	This is the number of uplink slots in the frame for this AP.
NumDLHalfSlots	This is the number of downlink slots in the frame for this.
NumULContSlots	This field displays how many Contention Slots are being used in the uplink portion of the frame.
WhiteSched	Flag to display if schedule whitening is supported via FPGA
ICC	This field lists the SMs that have registered to the AP with their Installation Color Code (ICC), Primary CC, Secondary CC or Tertiary CC.
SM PPPoE	This filed provides information to the user whether the SM is supporting PPPoE or not.
Frame Period	This field displays the configured Frame Period of the radio.
Last Registered Primary Color Code AP	
MAC Address	This field displays the last registered AP's MAC address.
Frequency	This field displays the last registered AP's frequency.
Channel Bandwidth	This field displays the last registered AP's channel bandwidth.
Color Code	This field displays the last registered AP's color code.
Air Delay	This field displays the last registered AP's air delay.
Receive Power	This field displays the last registered AP's receive power.
Scan Statitistics	
Scan Cycle Count	The file displays the number of scan cycles. This increments after the SM completes scanning every configured frequency and channel bandwidth.
Beacon Statistics	
Unsupported Feature Beacon Received	Count of beacons that the SM has received that is from a beacon that it does not support, which will prevent registration. If encounter this, upgrade your SM to the latest supported software version.
Unknown Feature Beacon Received	Count of beacons that the SM has received that is from a beacon that is running a feature that is unknown, which will prevent registration. If this stat is encountered, upgrade your SM to the latest supported software version.
Old Version Beacon Received	Count of the beacons where the version in the beacon mismatched and prevented registration.

Attribute	Meaning
Wrong Frequency Beacon Received	Count of beacons that was reported on a different frequency than was received.

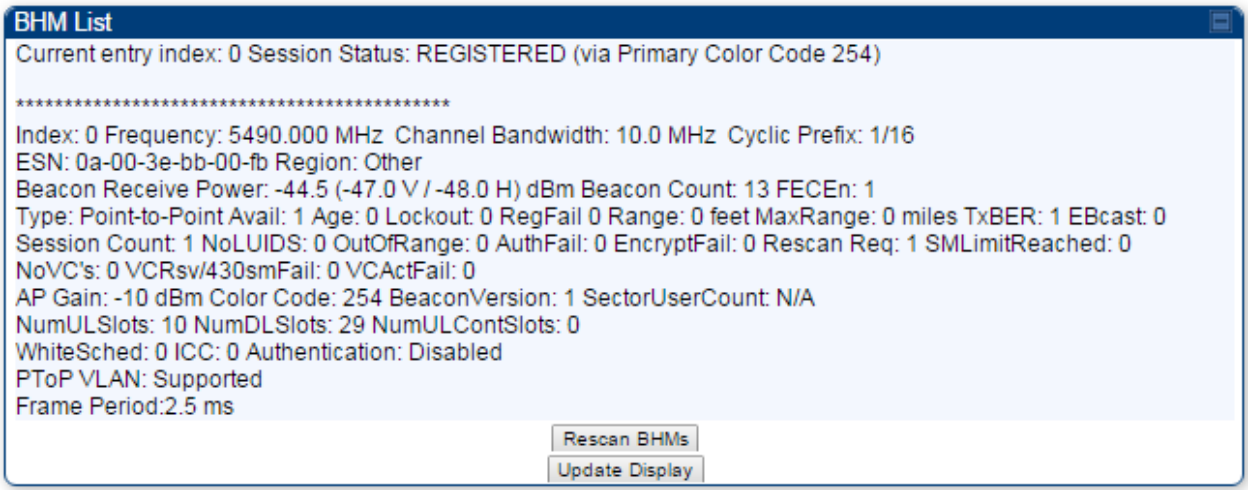
Using BHM Evaluation tool

The BHM Evaluation tab on Tools web page of the BHS provides information about the BHM that the BHS sees.

BHM Evaluation page of BHS

The BHM Evaluation page of BHS is explained in below figure.

Figure 97: *BHM Evaluation tab attributes - BHS*



Attribute	Meaning
Index	This field displays the index value that the system assigns (for only this page) to the BHM where this BHS is registered.
Frequency	This field displays the frequency that the BHM transmits.
Channel Bandwidth	The channel size used by the radio for RF transmission. The setting for the channel bandwidth must match between the BHM and the BHS.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefixes mean that for every 16 bits of throughput data transmitted, an additional bit is used.

Attribute	Meaning
ESN	This field displays the MAC address (electronic serial number) of the BHM. For operator convenience during BHS aiming, this tab retains each detected ESN for up to 15 minutes. If the broadcast frequency of a detected BHM changes during a 15-minute interval in the aiming operation, then a multiple instance of the same ESN is possible in the list. Eventually, the earlier instance expires and disappears and the later instance remains to the end of its interval, but you can ignore the early instance(s) whenever two or more are present.
Region	This field displays the BHM's configured Country Code setting.
Power Level	This field displays the BHS's combined received power level from the BHM's transmission.
Beacon Count	A count of the beacons seen in a given time period.
FECEn	This field contains the SNMP value from the BHM that indicates whether the Forward Error Correction feature is enabled. 0: FEC is disabled 1: FEC is enabled
Type	Multipoint indicates that the listing is for a BHM.
Age	This is a counter for the number of minutes that the BHM has been inactive. At 15 minutes of inactivity for the BHS, this field is removed from the BHM Evaluation tab in the BHS.
Lockout	This field displays how many times the BHS has been temporarily locked out of making registration attempts.
RegFail	This field displays how many registration attempts by this BHS failed.
Range	This field displays the distance in feet for this link. To derive the distance in meters, multiply the value of this parameter by 0.3048.
MaxRange	This field indicates the configured value for the AP's Max Range parameter.
TxBER	A 1 in this field indicates the BHM is sending Radio BER.
Ebcast	A 1 in this field indicates the BHM is encrypting broadcast packets. A 0 indicates it is not.
Session Count	This field displays how many sessions the BHS has had with the BHM. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum. In the case of a multipoint link, if the number of sessions is significantly greater than the number for other BHS's, then this may indicate a link problem or an interference problem.
NoLUIDs	This field indicates how many times the BHM has needed to reject a registration request from a BHS because its capacity to make LUID assignments is full. This then locks the BHS out of making any valid attempt for the next 15 minutes. It is extremely unlikely that a non-zero number would be displayed here.

Attribute	Meaning
OutOfRange	This field indicates how many times the BHM has rejected a registration request from a BHS because the BHS is a further distance away than the range that is currently configured in the BHM. This then locks the BHS out of making any valid attempt for the next 15 minutes.
AuthFail	This field displays how many times authentication attempts from this SM have failed in the BHM.
EncryptFail	This field displays how many times an encryption mismatch has occurred between the BHS and the BHM.
Rescan Req	This field displays how many times a re-range request has occurred for the BHM that is being evaluated in the BHM Eval page of a BHM.
SMLimitReached	This field displays 0 if additional BHSs may be registered to the BHM. If a 1 is displayed, the BHM will not accept additional BHS registrations.
NoVC's	This counter is incremented when the BHS is registering to a BHM which determines that no data channel resources are available for allocation. This could be a primary data channel (a low priority data channel) or one of the other possible data channel priorities (a Medium priority data channel, or High priority data channel, or Ultra High priority data channel)
VCRsvFail	This counter is incremented when the BHS is registering to a BHM which has a VC resource available for allocation but cannot reserve the resource for allocation.
VCActFail	This counter is incremented when the BHS is registering to a BHM which has a VC resource available for allocation and has reserved the VC, but cannot activate the resource for allocation.
AP Gain	This field displays the total external gain (antenna) used by the BHM.
RcvT	This field displays the AP's configured receive target for receiving BHS transmissions (this field affects automatic BHS power adjust).
Sector ID	This field displays the value of the Sector ID field that is provisioned for the BHM.
Color Code	This field displays a value from 0 to 254 indicating the BHM's configured color code. For registration to occur, the color code of the BHS and the BHM must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a BHS to register to only a specific BHM, even where the BHS can communicate with multiple BHMs. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes).
BeaconVersion	This field indicates that the beacon is OFDM (value of 1).
Sector User Count	This field displays how many BHS's are registered on the BHM.
NumULHalfSlots	This is the number of uplink slots in the frame for this BHM.
NumDLHalfSlots	This is the number of downlink slots in the frame for this.

Attribute	Meaning
NumULContSlots	This field displays how many Contention Slots are being used in the uplink portion of the frame.
WhiteSched	Flag to display if schedule whitening is supported via FPGA
ICC	This field lists the BHSs that have registered to the BHM with their Installation Color Code (ICC), Primary CC, Secondary CC or Tertiary CC.
SM PPPoE	This filed provides information to the user whether the BHS is supporting PPPoE or not.
Frame Period	This field displays the configured Frame Period of the radio.

Using the OFDM Frame Calculator tool

The first step to avoid interference in wireless systems is to set all APs/BHMs to receive timing from a synchronization source (Cluster Management Module, or Universal Global Positioning System). This ensures that the modules are in sync and start transmitting at the same time each frame.

The second step to avoid interference is to configure parameters on all APs/BHMs of the same frequency band in proximity such that they have compatible transmit/receive ratios (all stop transmitting each frame before any start receiving). This avoids the problem of one AP/BHM attempting to receive the signal from a distant SM/BHS while a nearby AP transmits, which could overpower that signal.

The following parameters on the AP determine the transmit/receive ratio:

- Max Range
- Frame Period
- Downlink Data percentage
- (reserved) Contention Slots

If OFDM (PMP 430, PMP 450, PTP 230) and FSK (PMP 1x0) APs/BHMs of the same frequency band are in proximity, or if APs/BHMs set to different parameters (differing in their Max Range values, for example), then operator must use the Frame Calculator to identify compatible settings.

The frame calculator is available on the Frame Calculator tab of the Tools web page. To use the Frame Calculator, type various configurable parameter values into the calculator for each proximal AP and then record the resulting AP/BHM Receive Start value. Next vary the Downlink Data percentage in each calculation and iterate until the calculated AP/BHM Receive Start for all collocated AP/BHMs where the transmit end does not come before the receive start.

The calculator does not use values in the module or populate its parameters. It is merely a convenience application that runs on a module. For this reason, you can use any FSK module (AP, SM, BHM, BHS) to perform FSK frame calculations for setting the parameters on an FSK AP and any OFDM module (AP, SM, BHM, BHS) to perform OFDM frame calculations for setting the parameters on an OFDM AP/BHM.

For more information on PMP/PTP 450 Platform co-location, see

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

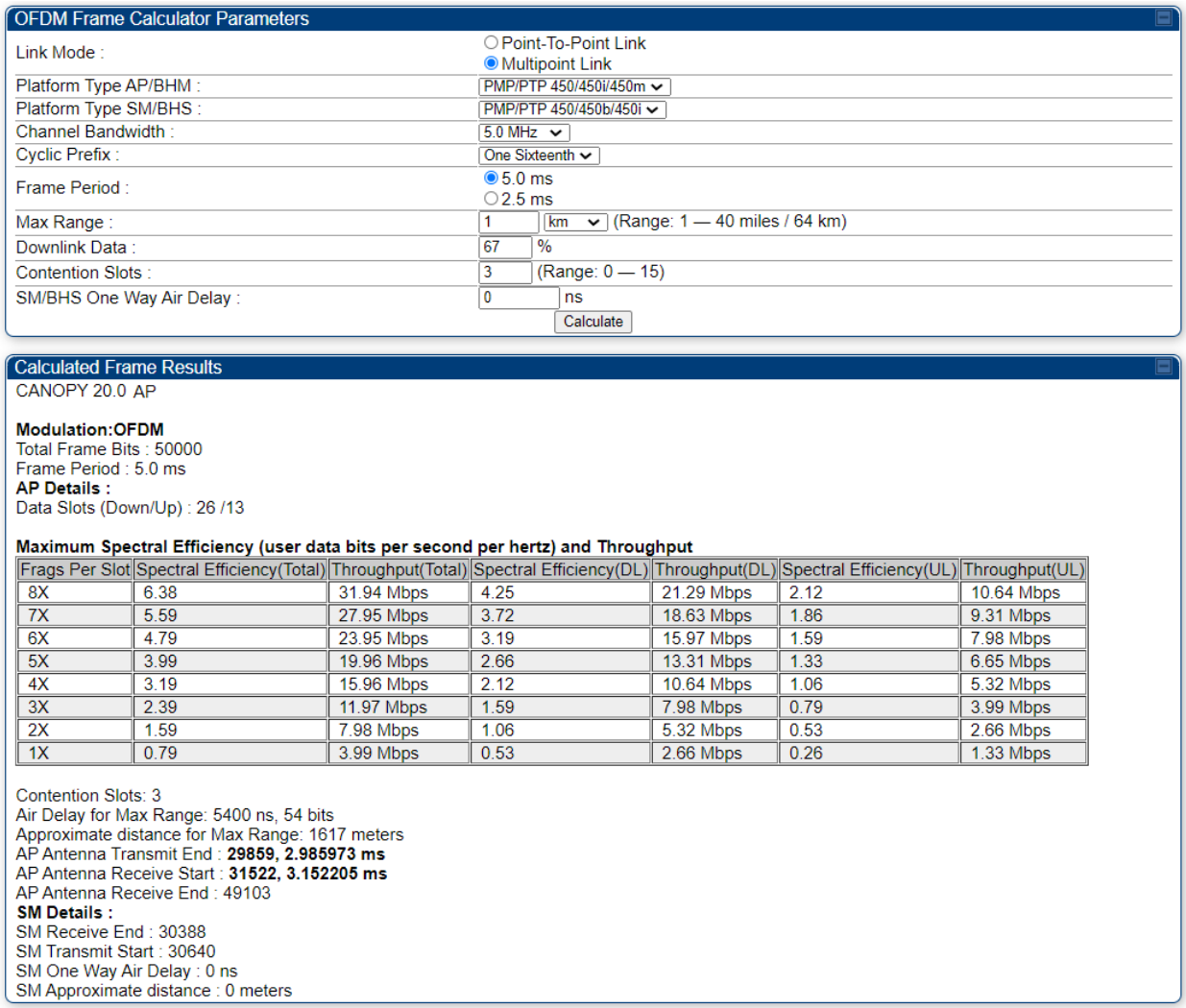
The co-location is also supported for 900 MHz PMP 450i APs (OFDM) and PMP 100 APs (FSK). Please refer Co-location of PMP 450 and PMP 100 systems in the 900 MHz band and migration recommendations document for details.

Caution

APs/BHMs that have slightly mismatched transmit-to-receive ratios and low levels of data traffic may see little effect on throughput. A system that was not tuned for co-location may work fine at low traffic levels, but encounter problems at higher traffic levels. The conservative practice is to tune for co-location before traffic ultimately increases. This prevents problems that occur as sectors are built.

The OFDM Frame Calculator page is explained in below table.

Table 104: OFDM Frame Calculator page attributes



Attribute	Meaning
Link Mode	For AP to SM frame calculations, select Multipoint Link For BHM to BHS frame calculations, select Point-To-Point Link
Platform Type AP/BHM	Use the drop-down list to select the hardware series (board type) of the AP/BHM.
Platform Type SM/BHS	Use the drop-down list to select the hardware series (board type) of the SM/BHS.
Channel Bandwidth	Set this to the channel bandwidth used in the AP/BHM.

Attribute	Meaning
Cyclic Prefix	Set this to the cyclic prefix used in the AP/BHM.
Max Range	Set to the same value as the Max Range parameter is set in the AP(s) or BHM(s).
Frame Period	Set to the same value as the Frame Period parameter is set in the AP(s) or BHM(s).
Downlink Data	Initially set this parameter to the same value that the AP/BHM has for its Downlink Data parameter (percentage). Then, use the Frame Calculator tool procedure as described inProcedure 26 Using the Frame Calculator , you will vary the value in this parameter to find the proper value to write into the Downlink Data parameter of all APs or BHMs in the cluster. PMP 450 Platform Family APs or BHMs offer a range of 15% to 85% and default to 75%. The value that you set in this parameter has the following interaction with the value of the Max Range parameter (above): The default Max Range value is 5 miles and, at that distance, the maximum Downlink Data value (85% in PMP 450 Platform) is functional.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. Set this parameter to the value of the Contention Slot parameter is set in the APs or BHMs.
SM/BHS One Way Air Delay	This field displays the time in ns (nano seconds), that a SM/BHS is away from the AP/BHM.

The Calculated Frame Results display several items of interest:

Table 105: OFDM Calculated Frame Results attributes

Attribute	Meaning
Modulation	The type of radio modulation used in the calculation (OFDM for 450 Platform Family)
Total Frame Bits	The total number of bits used in the calculated frames
Data Slots (Down/Up)	This field is based on the Downlink Data setting. For example, a result within the typical range for a Downlink Data setting of 75% is 61/21, meaning 61 data slots down and 21 data slots up.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator.
Air Delay for Max Range	This is the roundtrip air delay in bit times for the Max Range value set in the calculator
Approximate distance for Max Range	The Max Range value used for frame calculation
AP Transmit End	In bit times, this is the frame position at which the AP/BHM ceases transmission.
AP Receive Start	In bit times, this is the frame position at which the AP/BHM is ready to receive transmission from the SM/BHS.
AP Receive End	In bit times, this is the frame position at which the AP/BHM will cease receiving transmission from the SM/BHS.
SM Receive End	In bit times, this is the frame position at which the SM/BHS will cease receiving transmission from the AP/BHM.
SM Transmit Start	In bit times, this is the frame position at which the SM/BHS starts the transmission.
SM One Way Air Delay	This filed displays the time in ns, that SM/BHS is away from the AP/BHM.
SM Approximate distance	This field displays an approximate distance in miles (feet) that the SM/BHS is away from the AP/BHM.

To use the Frame Calculator to ensure that all APs or BHMs are configured to transmit and receive at the same time, follow the procedure below:

Procedure 26 Using the Frame Calculator

1	Populate the OFDM Frame Calculator parameters with appropriate values as described above.
2	Click the Calculate button.
3	Scroll down the tab to the Calculated Frame Results section
4	Record the value of the AP Receive Start field

5	Enter a parameter set from another AP in the system – for example, an AP in the same cluster that has a higher Max Range value configured.
6	Click the Calculate button.
7	Scroll down the tab to the Calculated Frame Results section
8	If the recorded values of the AP Receive Start fields are within 150 bit times of each other, skip to step 10.
9	If the recorded values of the AP Receive Start fields are not within 150 bit times of each other, modify the Downlink Data parameter until the calculated results for AP Receive Start are within 300 bit time of each other, if possible, 150 bit time.
10	Access the Radio tab in the Configuration web page of each AP in the cluster and change its Downlink Data parameter (percentage) to the last value that was used in the Frame Calculator.

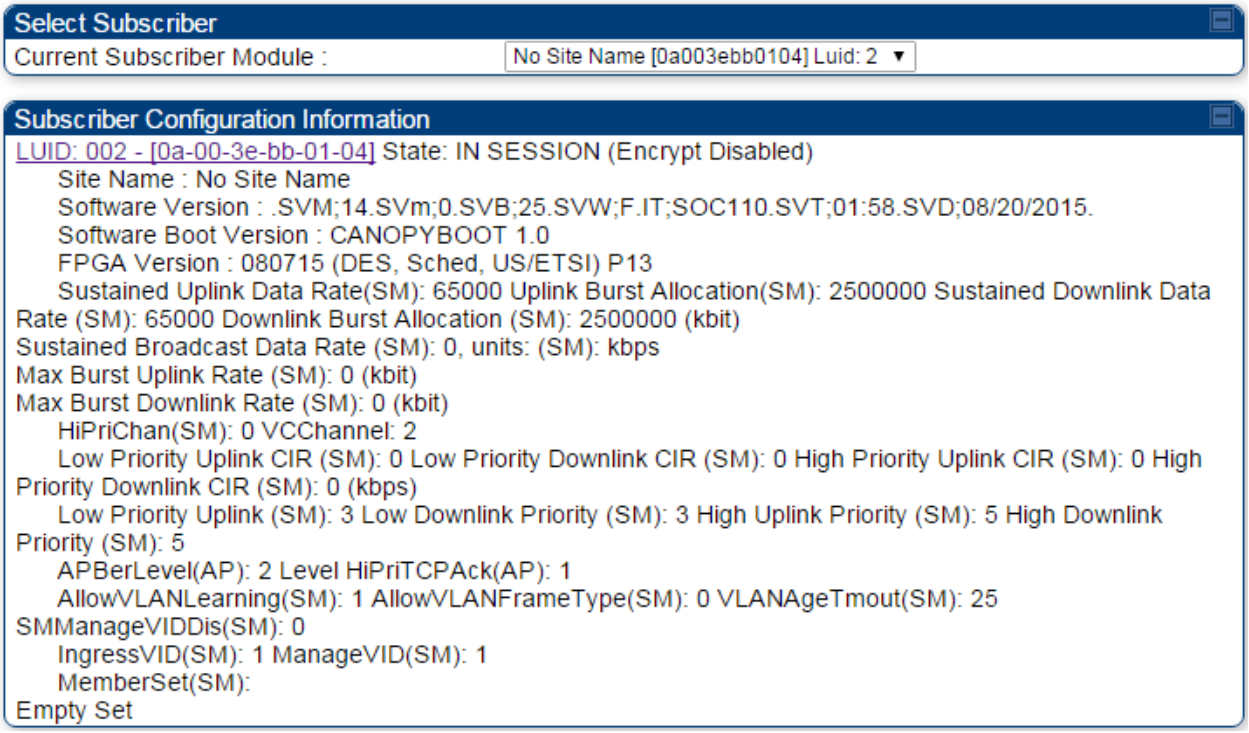
Using the Subscriber Configuration tool

The Subscriber Configuration page in the Tools page of the AP displays:

- The current values whose control may be subject to the setting in the Configuration Source parameter.
- An indicator of the source for each value.

This page may be referenced for information on how the link is behaving based on where the SM is retrieving certain QoS and VLAN parameters.

Figure 98: *SM Configuration page of AP*



The AP displays one of the following for the configuration source:

- (SM) – QoS/VLAN parameters are derived from the SM's settings
- (APCAP) – QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps)
- (D) – QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server.
- (AAA) – QoS/VLAN parameters are retrieved from the RADIUS server
- (BAM) – QoS/VLAN parameters are retrieved from a WM BAM server

Using the Link Status tool

The Link Status Tool displays information about the most-recent Link Test initiated on the SM or BHS. Link Tests initiated from the AP or BHM are not included in the Link Status table. This table is useful for monitoring link test results for all SMs or BHS in the system.

The Link Status table is color coded to display health of link between AP/BHM and SM/BHS. The current Modulation Level Uplink/Downlink is chosen to determine link health and color coded accordingly.

Uplink/Downlink Rate Column will be color coded using current Rate as per the table below:

Table 106: Color code versus uplink/downlink rate column

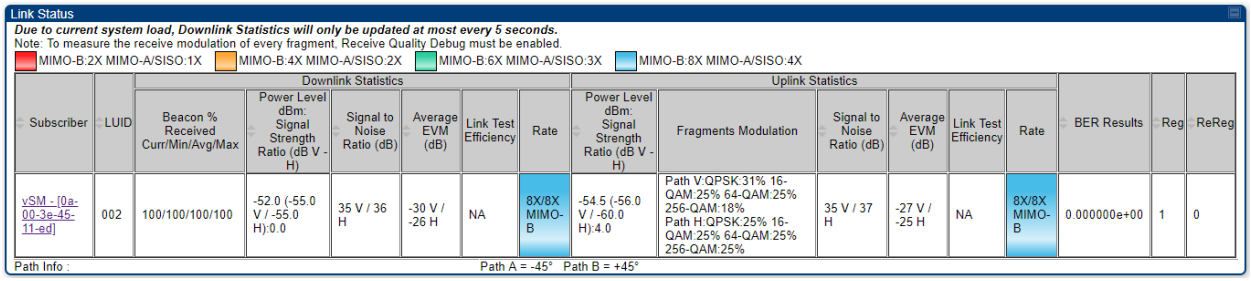
Actual Rate	1x	2x	3x	4x	5x	6x	7x	8x
MIMO-A	Red	Orange	Green	Blue	NA	NA	NA	NA
MIMO B	Red	Red	Orange	Orange	Green	Green	Blue	Blue

Link Status – AP/BHM

The current Uplink Rate for each SM or BHS in Session in now available on AP or BHM Link Status Page. From system release 15.2, a single Rate is used and shown for all data channels of an SM.

The Link Status tool results include values for the following fields for AP/BHM.

Table 107: Link Status page attributes – AP/BHM


Link Status

Due to current system load, Downlink Statistics will only be updated at most every 5 seconds.

Note: To measure the receive modulation of every fragment, Receive Quality Debug must be enabled.

MIMO-B:2X MIMO-A/SISO:1X MIMO-B:4X MIMO-A/SISO:2X MIMO-B:6X MIMO-A/SISO:3X MIMO-B:8X MIMO-A/SISO:4X

Subscriber	LUID	Downlink Statistics						Uplink Statistics						BER Results	Reg	ReReg
		Beacon % Received Curr/Min/Avg/Max	Power Level dBm: Signal Strength Ratio (dB V - H)	Signal to Noise Ratio (dB)	Average EVM (dB)	Link Test Efficiency	Rate	Power Level dBm: Signal Strength Ratio (dB V - H)	Fragments Modulation	Signal to Noise Ratio (dB)	Average EVM (dB)	Link Test Efficiency	Rate			
vSM - [0a-00-3e-45-11-ed]	002	100/100/100/100	-52.0 (-55.0 V / -55.0 H):0.0	35 V / 36 H	-30 V / -26 H	NA	8X/8X MIMO-B	-54.5 (-56.0 V / -60.0 H):4.0	Path V:QPSK:31% 16-QAM:25% 64-QAM:25% 256-QAM:18% Path H:QPSK:25% 16-QAM:25% 64-QAM:25% 256-QAM:25%	35 V / 37 H	-27 V / -25 H	NA	8X/8X MIMO-B	0.000000e+00	1	0

Path Info : Path A = -45° Path B = +45°

Attribute	Meaning
Subscriber	This field displays the MAC address and Site Name of the SM.

Attribute	Meaning
	Note The MAC is hot link to open the interface to the SM. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view. Site Name indicates the name of the SM. You can assign or change this name on the Configuration web page of the SM. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.
LUID	This field displays the LUID (logical unit ID) of the SM/BHS. As each SM or BHS registers to the AP/BHM, the system assigns an LUID of 2 or a higher unique number to the SM/BHS. If a SM/BHS loses registration with the AP/BHS and then regains registration, the SM/BHS will retain the same LUID. **Note** Both the LUID and the MAC are hot links to open the interface to the SM/BHS. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
Downlink Statistics - Beacon/Maps % Received Curr/Min/Max/Avg	This field displays a count of beacons and maps received by the SM in percentage. SMs operating on System Release 20.2.1 or later will send the the lower of the map and beacon percentages and that will be displayed in this field. SMs operating on System Release 20.2 or earlier will always send only the beacon percentage. This stat is recommended to be between 99-100%. If it is lower than 99%, it indicates a problematic link as beacons and maps are sent in the lowest modulation 1X MIMO-A. This statistic is updated every 15 seconds.
Downlink Statistics – Power Level: Signal Strength Ratio	This field represents the received power level at the SM/BHS as well as the ratio of horizontal path signal strength to vertical path signal strength at the SM/BHS.
Downlink Statistics – Signal to Noise Ratio	This field represents the signal to noise ratio for the downlink (displayed when parameter Signal to Noise Ratio Calculation during Link Test is enabled) expressed for both the horizontal and vertical channels.
Downlink Statistics – Average EVM (dB)	This field displays the average EVM statistics that measures RF signal quality.
Downlink Statistics – Link Test Efficiency	This field displays the efficiency of the radio link, expressed as a percentage, for the radio downlink.
Downlink Statistics – SU-MIMO Rate	The SU-MIMO rate applies to all AP platforms. For 450m, this field indicates the rate being used for symbols where this particular VC is not being MU-MIMO grouped with other SMs. For 450 and 450i platforms, there is no grouping and this field indicates the modulation rate for all symbols.

Attribute	Meaning
Downlink Statistics – MU-MIMO Rate	This field indicates the modulation rate used for symbols where the low or medium priority data channels are MU-MIMO scheduled by grouping it in the same slot with other low or Medium priority data channels from other SM's.
Uplink Statistics - Power Level: Signal Strength Ratio	This field represents the combined received power level at the AP/BHM as well as the ratio of horizontal path signal strength to vertical path signal strength.
Uplink Statistics – Fragments Modulation	The fragments modulation is an approximation at which modulation rate a packet was received. This stat is only for engineering debugging and is not available via SNMP and is not recommended to be used by customers. Different packets sizes can affect the reading to only show lower modulation rates. Also, unless "Receive Quality Debug" is enabled, it will just be a sampling of packets and not all the packets.
Uplink Statistics – Signal to Noise Ratio	This field represents the signal to noise ratio for the uplink (displayed when parameter Signal to Noise Ratio Calculation during Link Test is enabled) expressed for both the horizontal and vertical channels.
Uplink Statistics – Link Test Efficiency	This field displays the efficiency of the radio link, expressed as a percentage, for the radio uplink.
Uplink Statistics – SU-MIMO Rate	The SU-MIMO rate applies to all AP platforms. For 450m, this field indicates the rate being used for symbols where a VC is not being MU-MIMO grouped with other SMs. For 450 and 450i platforms, there is no grouping and this field indicates the modulation rate for all symbols.
Uplink Statistics – MU-MIMO Rate	This field indicates the modulation rate used for symbols where the low or medium priority data channels are MU-MIMO scheduled by grouping it in the same slot with other high or ultra high priority data channels from other SM's.
BER Results	This field displays the over-the-air Bit Error Rates for each downlink. (The ARQ [Automatic Resend Request] ensures that the transport BER [the BER seen end-to-end through a network] is essentially zero.) The level of acceptable over-the-air BER varies, based on operating requirements, but a reasonable value for a good link is a BER of 1e-4 (1×10^{-4}) or better, approximately a packet resend rate of 5%. BER is generated using unused bits in the downlink. During periods of peak load, BER data is not updated as often, because the system puts priority on transport rather than on BER calculation.
Reg Requests	A Reg Requests count is the number of times the SM/BHS registered after the AP/BHM determined that the link had been down. If the number of sessions is significantly greater than the number for other SMs/BHS, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).
ReReg Requests	A ReReg Requests count is the number of times the AP/BHM received a SM/BHS registration request while the AP/BHM considered the link to be still up (and therefore did not expect registration requests).

Attribute	Meaning
	If the number of sessions is significantly greater than the number for other SMs/BHS, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).

Link Status – SM/BHS

The Link Status tool of SM/BHS displays Downlink Status and Uplink Status information.

Table 108: Link Status page attributes – SM/BHS

Downlink Status	
Receive Power	-54.4 (-57.0 B / -57.9 A) dBm
Path Info	Path A = -45° Path B = +45°
Signal Strength Ratio	0.9dB B - A
Signal to Noise Ratio	34 B / 33 A dB
EVM	1 min: Worst: -27 B / -25 A, Avg: -27.2 (-28 B / -27 A), Best: -29 B / -28 A dB 5 min: Worst: -26 B / -25 A, Avg: -27.3 (-28 B / -27 A), Best: -29 B / -28 A dB 15 min: Worst: -26 B / -25 A, Avg: -27.2 (-28 B / -27 A), Best: -29 B / -29 A dB
Beacons / Maps	15 sec: 100% 1 min: 100% (min/avg/max) 15 min: 99/99/100% (min/avg/max)
Receive Fragments Modulation	Path B:QPSK:15% 16-QAM:43% 64-QAM:26% 256-QAM:16% Path A:QPSK:18% 16-QAM:37% 64-QAM:28% 256-QAM:17%
Latest Remote Link Test Efficiency Percentage	NA %
BER Total Avg Results	0.000000e+00

Uplink Status	
Transmit Power	2 dBm
Max Transmit Power	25 dBm
Power Level	-44.0 (-47.0 B / -47.0 A) dBm
Signal Strength Ratio	0.0dB B - A
Signal to Noise Ratio	35 dB B / 40 dB A
EVM	1 min: Worst: -25 B / -33 A, Avg: -33.0 (-32 B / -35 A), Best: -40 B / -38 A dB 5 min: Worst: -25 B / -33 A, Avg: -33.1 (-32 B / -35 A), Best: -40 B / -40 A dB 15 min: Worst: -23 B / -33 A, Avg: -33.2 (-32 B / -36 A), Best: -40 B / -40 A dB
Latest Remote Link Test Efficiency Percentage	NA %

Local Status	
Session Status	REGISTERED 8X/8X MIMO-B
Spatial Frequency	513

Link Quality Indicator	
LQI	100%
Downlink LQI	100%
Beacon / Map Quality Index	100%
Uplink LQI	100%
Reregistration Quality Index	100%
Reregistration Count	0

Reference LQI	
Reference Downlink Quality Index	None
Reference Uplink Quality Index	None
Access Point MAC Address	None

Latest Local Link Test Results

No test results available

Run Link Test

Attribute	Meaning
Downlink Status	
Receive Power	This field lists the current combined receive power level, in dBm.
Path Info	
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power for downlink.
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor for downlink.
EVM	This field displays the average EVM statistics that measures RF signal quality.

Attribute	Meaning
Beacons/Maps	Displays a count of beacons received by the SM in percentage. This value must be typically between 99-100%. If lower than 99%, it indicates a problematic link. This statistic is updated every 16 seconds.
Received Fragments Modulation	This field represents the percentage of fragments received at each modulation state, per path (polarization)
Latest Remote Link Test Efficiency Percentage	This field is not applicable.
BER Total Avg Results	This field displays the over-the-air average Bit Error Rates (BER) for downlink.
Beacons Received Last 15 minutes	The beacon count on the SM can be used to estimate the interference in the channel. The min/avg/max beacon percentage displayed based on this value for the last 15 mins.
Uplink Status	
Transmit Power	This field displays the current combined transmit power level, in dBm.
Max Transmit Power	This field displays the maximum transmit power of SM.
Power Level	This field indicates the combined power level at which the SM is set to transmit, based on the Country Code and Antenna Gain settings.
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power for uplink.
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor for uplink.
Average EVM	This field displays the average EVM statistics that measures RF signal quality.
Latest Remote Link Test Efficiency Percentage	This field is not applicable.
Local Stats	
Session Status	This field displays the current state, Virtual channel, channel rate adaptation and MIMO-A/MIMO-B/SISO status of SM.
Spatial Frequency	This filed displays the spatial frequency value of the VC or SM.
Run Link Test	Run Link Test See Exploratory Test section of Performing Extrapolated Link Test
Link Quality Indicator	

Attribute	Meaning
LQI	This field displays the quality of the link used for data communication between AP and SM. This value is derived by calculating: Downlink LQI value * Uplink LQI value * Re-Registration Quality Index value
Downlink LQI	This field displays the downlink quality of the link. It is the ratio of Actual Average Modulation Rate of the data packets and the expected modulation rate.
Downlink Actual Average Modulation Rate	This field displays the average value of the actual Downlink modulation rate.
Downlink Expected Modulation Rate	This field displays the expected Downlink modulation rate.
Beacon Quality Index	This field displays the Beacon Quality Index. It is calculated based on the receive beacon percentage.
Uplink LQI	This field displays the uplink quality of the link. It is the ratio of Actual Average Modulation Rate of the data packets and the expected modulation rate.
Uplink Actual Average Modulation Rate	This field displays the average value of the actual uplink modulation rate.
Uplink Expected Modulation Rate	This field displays the expected Uplink modulation rate.
Re-Registration Quality Index	This field displays the number of re-registrations of the SM. When there are no re-registrations, this quality index will be 100%.
Re-Registration Count	This field displays the re-registration count of the SM.
Reference Downlink Quality Index	Downlink reference EVM used for LQI calculations.
Reference Uplink Quality Index	Uplink reference EVM used for LQI calculations.
Access Point MAC Address	This field displays the MAC address of the AP to which this SM is registered.

Using BER Results tool

Radio BER data represents bit errors at the RF link level. Due to CRC checks on fragments and packets and ARQ (Automatic Repeat Request), the BER of customer data is essentially zero. Radio BER gives one indication of link quality. Other important indications to consider includes the received power level, signal to noise ratio and link tests.

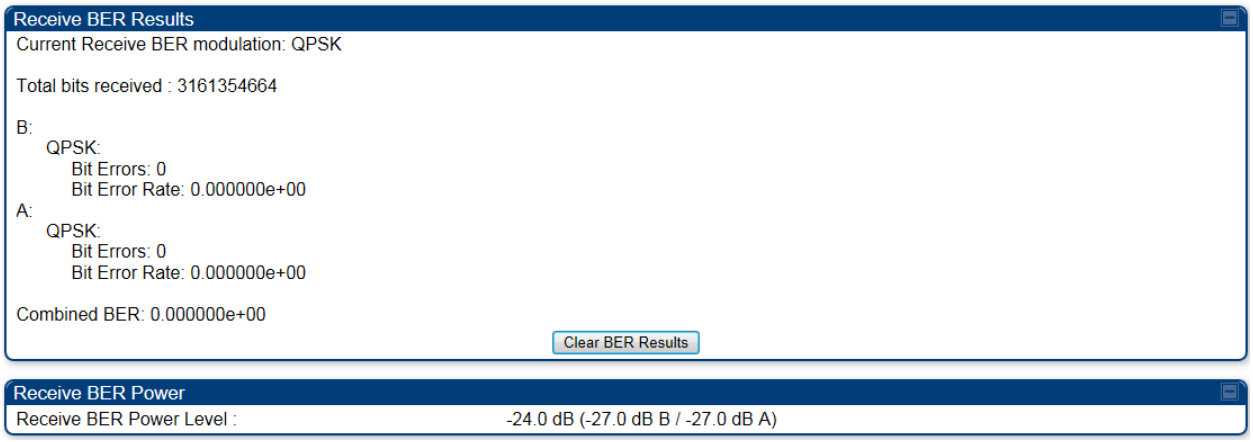
BER is only instrumented on the downlink and is displayed on the BER Results tab of the Tools page in any SM. Each time the tab is clicked, the current results are read and counters are reset to zero.

The BER Results tab can be helpful in troubleshooting poor link performance.

The link is acceptable if the value of this field is less than 10^{-4}. If the BER is greater than 10^{-4}, re-evaluate the installation of both modules in the link.

The BER test signal is broadcast by the AP/BHM (and compared to the expected test signal by the SM/BHS) only when capacity in the sector allows it. This signal is the lowest priority for AP/BHM transmissions.

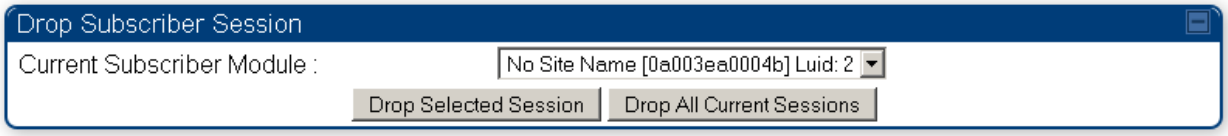
Figure 99: *BER Results tab of the SM*



Using the Sessions tool

The PMP 450 Platform Family AP has a tab Sessions under the Tools category which allows operators to drop one or all selected SM sessions and force a SM re-registration. This operation is useful to force QoS changes for SMs without losing AP logs or statistics. This operation may take 5 minutes to regain all SM registrations.

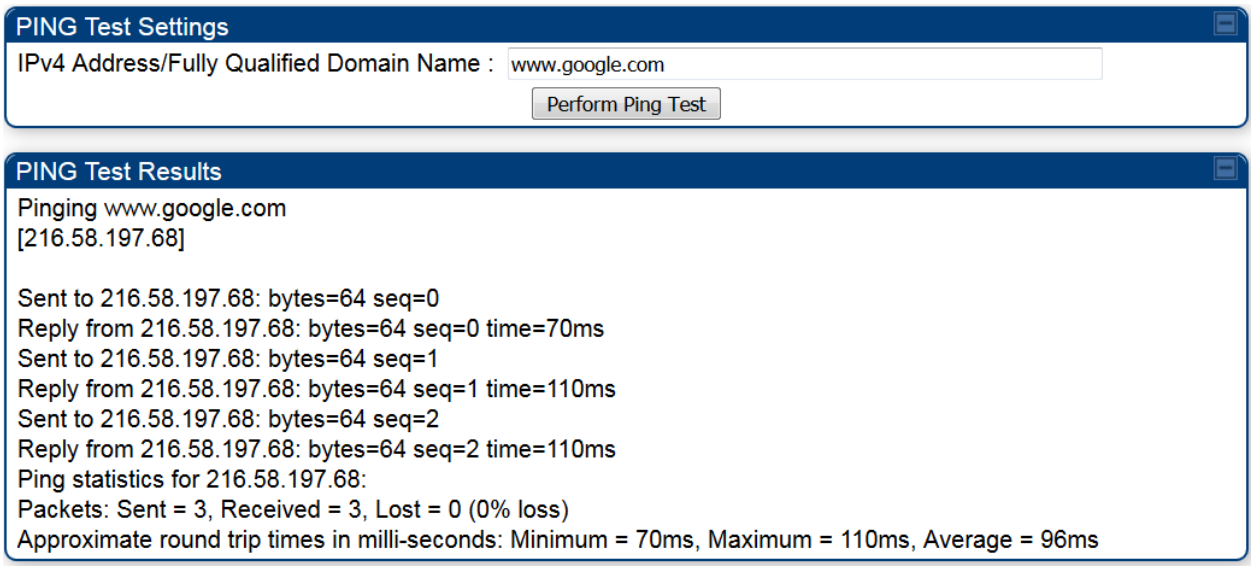
Figure 100: *Sessions tab of the AP*



Using the Ping Test tool

The PMP 450 Platform Family AP has a tab Ping Test under the Tools category which allows users to check the accessibility of the given IP V4 address or a valid domain name

Figure 101: *Ping Test tab of the AP*



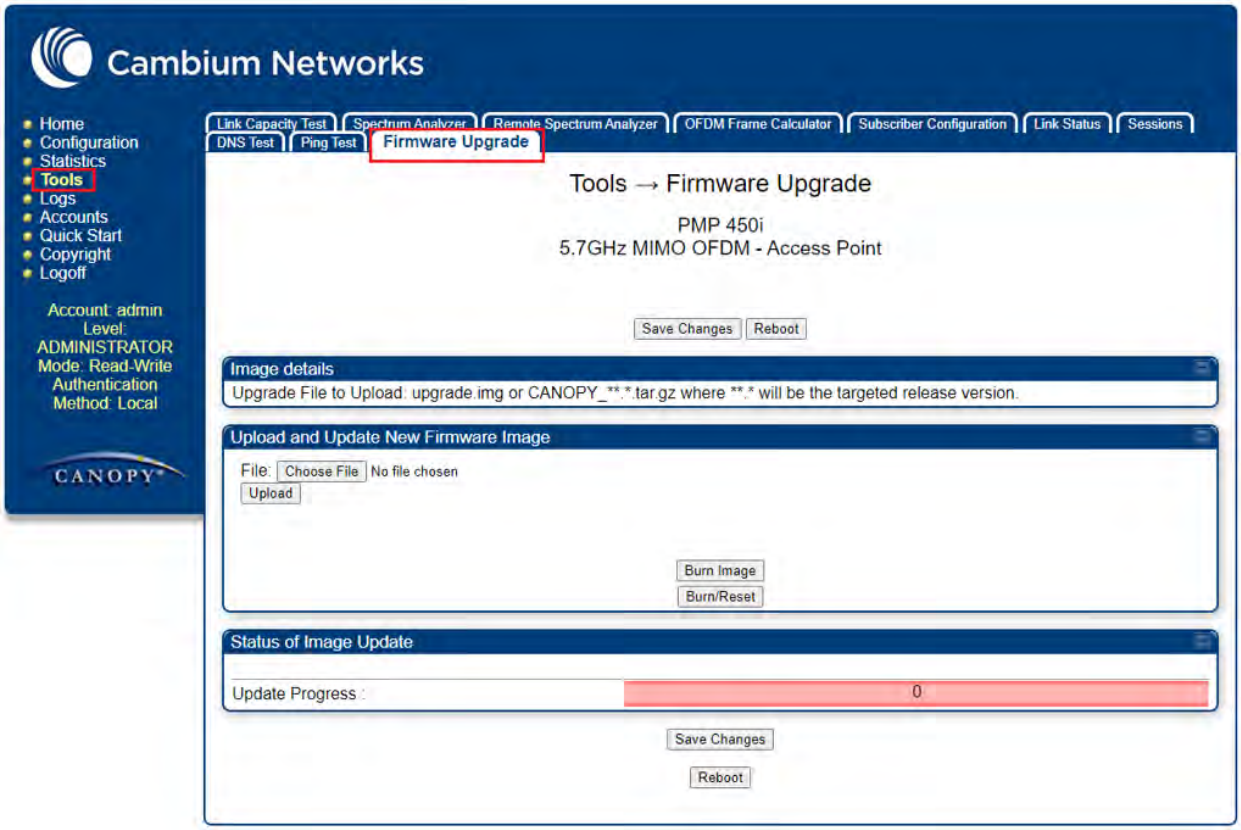
Note

When a domain name (for example, www.google.com) is used for ping test, make sure that Preferred DNS Server and Alternate DNS Server parameters are configured in the Configuration > IP tab of the AP.

Firmware Upgrade

Prior to System Release 22.0, the PMP 450 family of Radios can only be upgraded either from cnMaestro or CNUT. This feature allows the operator to upgrade software from the Radios Graphical User Interface (GUI). The software can be upgraded from the **Tools** -> **Firmware Upgrade** page, under the **Upload and Update New Firmware Image** section, by uploading the cnMaestro Software Package.

Figure 102: *Firmware upgrade*



Note

PMP 450 AP, PMP 450 SM, and PTP 450 Radios do not have enough resources to support uploading the cnMaestro software package.

The operator can upgrade PMP 450 AP, PMP 450 SM, and PTP 450 Radios from Web GUI by uploading a radio-specific image file. The image that can be uploaded to a Radio is listed under the Image details section, on the **Tools** -> **Firmware Upgrade** page and is shown in Figure 103 (for AP) and Figure 104 (for SM).

Figure 103: *Firmware upgrade page for PMP 450 AP*

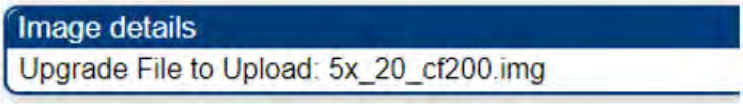
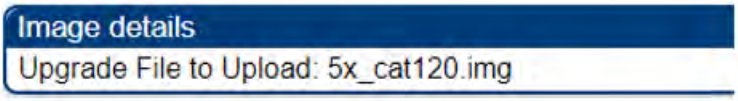


Figure 104: *Firmware upgrade page for PMP 450 SM*



Radio-specific image files can be extracted from the cnMaestro Software Package, using file extractor tools like WinZip, 7-Zip, etc.

Table 109 lists the image files specific to the Radios and their location in the cnMaestro software package.

Table 109: Image file location for Radio types

Radio Type	Image File	Location
PMP 450 AP	5x_20_cf200.img	\NIOS2\IMAGES\450\AP\SIGNED\
PMP 450 SM	5x_cat120.img	\NIOS2\IMAGES\450\SM_BH\SIGNED\
PTP 450	ptp450_c120.img	\NIOS2\IMAGES\450\SM_BH\SIGNED\

Chapter 3: Operation

This chapter provides instructions for operators of the 450 Platform Family wireless Ethernet Bridge. The following topics are described in this chapter:

- System information
  - Viewing General Status
  - Viewing Session Status
  - Viewing Remote Subscribers
  - Interpreting messages in the Event Log
  - Viewing the Network Interface
  - Viewing the Layer 2 Neighbors
- System statistics
  - Viewing the Scheduler Statistics
  - Viewing list of Registration Failures statistics
  - Interpreting Bridging Table statistics
  - Interpreting Translation Table statistics
  - Interpreting Ethernet statistics
  - Interpreting RF Control Block statistics
  - Interpreting VLAN statistics
  - Interpreting Data Channels statistics
  - Interpreting Proportional Scheduler

- Interpreting MIR/Burst statistics
    - Interpreting Overload statistics
    - Interpreting DHCP Relay statistics
    - Interpreting Filter statistics
    - Viewing ARP statistics
    - Viewing NAT statistics
    - Viewing NAT DHCP Statistics
    - Interpreting Sync Status statistics
    - Interpreting PPPoE Statistics for Customer Activities
    - Interpreting Bridge Control Block statistics
    - Interpreting SNMPv3 Statistics
    - Interpreting syslog statistics
    - Interpreting Frame Utilization statistics
- Radio Recovery

System information

This section describes how to use the summary and status pages to monitor the status of the Ethernet ports and wireless link.

- Viewing General Status
- Viewing Session Status
- Viewing Remote Subscribers
- Interpreting messages in the Event Log
- Viewing the Network Interface
- Viewing the Layer 2 Neighbors

Viewing General Status

The General Status tab provides information on the operation of this AP/BHM and SM/BHS. This is the page that opens by default when you access the GUI of the radio.

General Status page of AP

The General Status page of PMP 450m AP is explained in General Status page attributes – PMP 450m AP

The General Status page of PMP 450 AP is explained in General Status page attributes – PMP 450 AP

The General Status page of PMP 450i AP is explained in General Status page attributes – PMP 450i AP.

The General Status page of 450v AP is explained in General Status page attributes – 450v AP.

Table 110: General Status page attributes – PMP 450m AP

Device Information	
Device Type :	5.7GHz MU-MIMO OFDM - Access Point - 0a-00-3e-60-34-c8
Board Type :	P14
Product Type :	PMP 450m
Software Version :	CANOPY 15.2 AP
Bootloader Version :	BOOTLOADER 15.1.1/161 2017-06-21 06:50:26 -0500
CPU Usage :	0%
Board MSN :	M9SM0024C4GC
Board Model :	C050045A101A
FPGA Version :	031c76
Uptime :	3d, 03:55:00
System Time :	09:45:10 05/25/2018 UTC
Main Ethernet Interface :	100Base-TX Full Duplex
Region Code :	Other
Regulatory :	Passed
Channel Frequency :	5800.0 MHz
Channel Bandwidth :	10.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Encryption :	Capable of AES-256 but configured to None
Color Code :	245
Max Range :	25 km
EIRP :	33 dBm
Temperature :	47 °C / 116 °F

Access Point Stats	
Registered SM Count :	1 (1 Data Channels)
Sync Pulse Status :	Receiving Sync (100.0% Sync pulses received)
Sync Pulse Source :	Power Port (Canopy Sync)
Maximum Count of Registered SMs :	1

Frame Configuration Information	
Data Slots Down :	15
Data Slots Up :	16
Contention Slots :	4

cnMaestro Connection Stats	
Connection Status :	Device Approval Pending (qa.cloud.cambiumnetworks.com)
AccountID :	

Site Information	
Site Name :	450m
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
MU-MIMO Mode :	MU-MIMO
AES-256 Encryption Keyed :	False
Time Updated and Location Code :	08/10/2017 09:12:40 - sdfs

Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the device, its module type and its MAC address.
Board Type	This field indicates the series of hardware.
Product Type	The field indicates model number of 450m device. The 450m Series has two model variants. • PMP 450m: This model works in SU-MIMO mode which is default “limited” mode. The MU-MIMO license can be purchased from Cambium Networks and applied. MU-MIMO: This model works in MU-MIMO mode.
Software Version	This field indicates the system release, the time and date of the release and whether communications involving the module are secured by AES encryption. If you request technical support, provide the information from this field.
Bootloader Version	This field indicates the version of Uboot running on the 450m AP platform.
CPU Usage	This field indicates the current CPU utilization of the device.

Attribute	Meaning
Board MSN	This field indicates the Manufacturer's Serial number. A unique serial number assigned to each radio at the factory for inventory and quality control.
Board Model	This field indicates the Manufacturer's Model number. A unique serial number assigned to each for inventory and quality control.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. If the AP is connected to a CMM4, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.
Main Ethernet Interface	This field indicates the speed and duplex state of the Ethernet interface to the AP.
Region Code	A parameter that offers multiple fixed selections, each of which automatically implements frequency band range for the selected region. Units shipped to regions other than restrictions the United States must be configured with the corresponding Region Code to comply with local regulatory requirements.
Regulatory	This field indicates whether the configured Country Code and radio frequency are compliant with respect to their compatibility. 450 Platform Family products shipped to the United States is locked to a Country Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Country Code to comply with local regulatory requirements.
DFS (Dynamic Frequency Selection)	This field dynamically selects frequency based on detection of radar pulses.
Channel Frequency	This field indicates the current operating center frequency, in MHz.
Channel Bandwidth	This field indicates the current size of the channel band used for radio transmission.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Frame Period	This field indicates the current Frame Period setting of the radio in ms.
Encryption	This field indicates the capability and the encryption configuration of the device.
Color Code	This field displays a value from 0 to 254 indicating the AP's configured color code. For registration to occur, the color code of the SM and the AP must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.

Attribute	Meaning
	Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes).
Max Range	This field indicates the setting of the Max Range parameter, which contributes to the way the radio transmits. Verify that the Max Range parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.
EIRP	This field indicates the combined power level at which the AP will transmit, based on the Country Code.
Temperature	This field indicates the current operating temperature of the device board.
CBSD Grant State	This field indicates the CBRS Registration and Grant state as described in Winnforum document WINNF-TS-0016. For more information on CBRS procedures and states see the Cambium's **CBRS Consolidated Procedurs** Guide.
Registered SM Count	This field indicates how many SMs are registered to the AP.
Sync Pulse Status	This field indicates the status of synchronization as follows: Generating Sync indicates that the module is set to generate the sync pulse. Receiving Sync indicates that the module is set to receive a sync pulse from an outside source and is receiving the pulse. No Sync Since Boot up / ERROR: No Sync Pulse indicates that the module is set to receive a sync pulse from an outside source and is not receiving the pulse. **Note** When this message is displayed, the AP transmitter is turned off to avoid self-interference within the system.
Sync Pulse Source	This field indicates the status of the synchronization source: Searching indicates that the unit is searching for a GPS fix Timing Port/UGPS indicates that the module is receiving sync via the timing AUX/SYNC timing port Power Port indicates that the module is receiving sync via the power port (Ethernet port). On-board GPS indicates that the module is receiving sync via the unit's internal GPS module
Maximum Count of Registered SMs	This field displays the largest number of SMs that have been simultaneously registered in the AP since it was last rebooted. This count can provide some insight into sector history and provide comparison between current and maximum SM counts at a glance.

Attribute	Meaning
Data Slots Down	This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the AP to the SM). The AP calculates the number of data slots based on the Max Range, Downlink Data and (reserved) Contention Slots configured by the operator.
Data Slots Up	This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data and (reserved) Contention Slots configured by the operator.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. See Contention slots.
Connection Status	This field indicates the device connectivity to cnMaestro (Cambium's cloud-based network management system).
Account ID	This field shows Account ID which is registered with Cambium Networks and it allows operator to manage devices using cnMaestro.
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.
Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.
MU-MIMO Mode	This field displays information about MU-MIMO mode. If AP is keyed as MU-MIMO, it will display "MU-MIMO" (Multi User - MIMO) otherwise it will display "SU-MIMO" (Single User - MIMO).
AES-256 Encryption Keyed	This displays the status of the entered AES-256 Encryption Key. Note To enable AES-256 Encryption, a feature key needs to be purchased.
Time Updated and Location Code	This field displays information about the keying of the radio.

Table 111: General Status page attributes – PMP 450 AP

Device Information	
Device Type :	5.7GHz MIMO OFDM - Access Point - 0a-00-3e-b1-2a-78
Board Type :	P12
Product Type :	PMP 450
Software Version :	CANOPY 15.2 AP
CPU Usage :	Curr/Max: 9%/95%
Board MSN :	6069QU0F0C
FPGA Version :	062618
PLD Version :	20
Uptime :	03:44:31
System Time :	09:11:33 07/12/2018 UTC
Main Ethernet Interface :	100Base-TX Full Duplex
Region Code :	Other
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	5850.0 MHz
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Encryption :	Capable of AES-128 but configured to None
Color Code :	171
Max Range :	3 Miles
Transmit Power :	0 dBm
Total Antenna Gain :	0 dBi
Temperature :	29 °C / 85 °F

Access Point Stats	
Registered SM Count :	1 (1 Data Channels)
Sync Pulse Status :	Generating Sync
Sync Pulse Source :	Self Generate
Maximum Count of Registered SMs :	1

Frame Configuration Information	
Data Slots Down :	40
Data Slots Up :	41
Contention Slots :	3

cnMaestro Connection Stats	
Connection Status :	Connected (cloud.cambiumnetworks.com)
AccountID :	GRE001

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
AES-256 Encryption Keyed :	False
Time Updated and Location Code :	05/09/2017 06:23:21 - INTL

Attribute	Meaning
Device Type	See General Status page attributes – PMP 450m AP for details
Board Type	
Product Type	This indicates model of the device.
Software Version	See General Status page attributes – PMP 450m AP for details
CPU Usage	This field indicates the current CPU utilization of the device.
Board MSN	This field indicates the Manufacturer's Serial number. A unique serial number assigned to each radio at the factory for inventory and quality control.
FPGA Version	See General Status page attributes – PMP 450m AP for details
PLD Version	This field indicates the firmware version on the Programmable Logic Device.
Uptime	See General Status page attributes – PMP 450m AP for details
System Time	
Main Ethernet Interface	
Region Code	See General Status page attributes – PMP 450m AP for details
Regulatory	
Antenna Type	
Channel Center Frequency	
Channel Bandwidth	
Cyclic Prefix	
Frame Period	
Color Code	
Max Range	
Transmit Power	This field indicates the combined power level at which the AP is set to transmit, based on the Country Code and Antenna Gain settings.
Temperature	See General Status page attributes – PMP 450m AP for details
Total Antenna Gain	This field indicates the total antenna gain.

Attribute	Meaning
Sync Pulse Status	See General Status page attributes – PMP 450m AP for details
Sync Pulse Source	
Maximum Count of Registered SMs	
Data Slots Down	
Data Slots Up	
Contention Slots	
Connection Status	
Account ID	
Site Name	
Site Contact	
Site Location	
Time Updated and Location Code	

Table 112: General Status page attributes – PMP 450i AP

Device Information	
Device Type :	5.4GHz MIMO OFDM - Access Point - 0a-00-3e-bb-01-77
Board Type :	P13
Product Type :	PMP 450i
Software Version :	CANOPY 15.1.5 AP-None
CPU Usage :	2%
Board MSN :	PMP450iMSN
Board Model :	C050045A010A
FPGA Version :	020118
Uptime :	2d, 07:56:57
System Time :	17:58:46 01/03/2016 UTC
Main Ethernet Interface :	100Base-TX Full Duplex
Aux Ethernet Interface :	Disabled (PoE Disabled)
Region Code :	Other
Regulatory :	Passed
DFS :	Idle
Antenna Type :	External
Channel Frequency :	5705.0 MHz
Channel Bandwidth :	40.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Color Code :	133
Max Range :	2 Miles
Transmit Power :	27 dBm
Total Antenna Gain :	40 dBi
Temperature :	36 °C / 97 °F

Access Point Stats	
Registered SM Count :	1 (1 Data Channels)
Sync Pulse Status :	Receiving Sync (100.0% Sync pulses received)
Sync Pulse Source :	Power Port (Canopy Sync)
Maximum Count of Registered SMs :	1

Access Point Stats	
Registered SM Count :	1 (1 Data VCs)
Sync Pulse Status :	Generating Sync
Sync Pulse Source :	Self Generate
Maximum Count of Registered SMs :	1

Frame Configuration Information	
Data Slots Down :	129
Data Slots Up :	43
Contention Slots :	3

cnMaestro Connection Stats	
Connection Status :	Cambium-ID Not Configured
AccountID :	

Site Information	
Site Name :	450i AP-133
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
Time Updated and Location Code :	11/01/2017 13:21:54 - INTL

Attribute	Meaning
Device Type	See General Status page attributes – PMP 450m AP for details
Board Type	
Product Type	This indicates model of the device.
Software Version	See General Status page attributes – PMP 450m AP for details
CPU Usage	This field indicates the current CPU utilization of the device.
Board MSN	This field indicates the Manufacturer's Serial number. A unique serial number assigned to each radio at the factory for inventory and quality control.
Board Model	This field indicates the Manufacturer's Model number.
FPGA Version	See General Status page attributes – PMP 450m AP for details
Uptime	
System Time	
Main Ethernet Interface	
Aux Ethernet Interface	See General Status page attributes – PMP 450m AP for details

Attribute	Meaning
Region Code	See General Status page attributes – PMP 450m AP for details
Regulatory	
Antenna Type	
Channel Center Frequency	
Channel Bandwidth	
Cyclic Prefix	
Frame Period	
Color Code	
Max Range	
Transmit Power	This field indicates the combined power level at which the AP is set to transmit, based on the Country Code and Antenna Gain settings.
Total Antenna Gain	This field indicates the total antenna gain.
Temperature	See General Status page attributes – PMP 450m AP for details
802.3at Type 2 PoE Status	The field displays whether PoE Classification functionality is enabled or disabled. It is only applicable for 450i Series devices.
Registered SM Count	See General Status page attributes – PMP 450m AP for details
Sync Pulse Status	
Sync Pulse Source	
Maximum Count of Registered SMs	
Data Slots Down	
Data Slots Up	
Contention Slots	See General Status page attributes – PMP 450m AP for details
Connection Status	
Account ID	
Site Name	
Site Contact	
Site Location	
Time Updated and Location Code	

Table 113: General Status page attributes – PMP 450v AP

Device Information	
Device Type :	6GHz U-NII-5 MIMO OFDM - Access Point - 02-04-56-00-00-68
Board Type :	P16
Product Type :	PMP 450v 4x4
Software Version :	CANOPY 23.0 (Build SIT-8) AP
CPU Usage :	Curr/Max: 2%/100%
Board MSN :	MZYE00000068
Board Model :	C060045A402A EngineeringKey
FPGA Version :	101123
Uptime :	22:24:20
System Time :	09:17:36 11/10/2023 UTC
Main Ethernet Interface :	1000Base-T Full Duplex
Aux Ethernet Interface :	Disabled (PoE Disabled)
Region Code :	United States
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	6400.0 MHz
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Encryption :	Capable of AES-128 but configured to None
Color Code :	50
Max Range :	2 Miles
EIRP :	16 dBm
Transmit Power :	16 dBm / -31 dBm
Total Antenna Gain :	0 dBi
Temperature :	34 °C / 94 °F

Access Point Stats	
Registered SM Count :	1 (1 Data Channels)
Sync Pulse Status :	Generating Sync
Sync Pulse Source :	Self Generate
Maximum Count of Registered SMs :	1

Frame Configuration Information	
Data Slots Down :	61
Data Slots Up :	20
Contention Slots :	3

cnMaestro Connection Stats	
Connection Status :	Connected (qa.cloud.cambiumnetworks.com)
AccountID :	5_0_0_X_CLOUD_REGRESSION

Site Information	
Site Name :	pmp canopy v
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
AES-256 Encryption Keyed :	False
FCC Access to 6 GHz (UNII-5, UNII-7) :	True (Engineering Key Override)
Time Updated and Location Code :	10/13/2023 19:48:17 - INTL

Attribute	
Device Type	See General Status page attributes – PMP 450i AP
Board Type	
Product Type	
Software Version	
CPU Usage	
Board MSN	
Board Model	
FPGA Version	
Uptime	
System Time	
Main Ethernet Interface	
Aux Ethernet Interface	
Region Code	See General Status page attributes – PMP 450i AP
Regulatory	
Antenna Type	
Channel Center Frequency	
Channel Bandwidth	
Cyclic Prefix	
Frame Period	
Color Code	
Max Range	
Transmit Power	
Total Antenna Gain	
Temperature	

Attribute	
Registered SM Count	
Sync Pulse Status	
Sync Pulse Source	
Maximum Count of Registered SMs	
Data Slots Down	
Data Slots Up	
Contention Slots	
Connection Status	
Account ID	
Site Name	
Site Contact	
Site Location	
Feature Key Information AES-256 Encryption Keyed	
FCC Access to 6 GHz (UNII-5, UNII-7)	
Time Updated and Location Code	

General status page - SM

The SM's General Status page is explained in below table.

Note

For accurate power level readings to be displayed, traffic must be present on the radio link.

Table 114: General Status page attributes - SM

Device Information	
Device Type :	4.9/5.9GHz MIMO OFDM - Subscriber Module - 0a-00-3e-78-15-10
Board Type :	P15
Product Type :	PMP 450b High Gain
Software Version :	CANOPY 15.2 SM
CPU Usage :	3%
Board MSN :	M9SM00Z7P2P2
Board Model :	C050045C012A
FPGA Version :	051918
Uptime :	3d, 03:53:38
System Time :	09:49:44 05/25/2018 UTC
Main Ethernet Interface :	No Link
Region Code :	Other
DFS :	Idle
Antenna Type :	Integrated
Frame Period :	2.5 ms
Encryption :	None
Temperature :	68 °C / 155 °F

Subscriber Module Stats	
Session Status :	REGISTERED 8X/8X MIMO-B
Session Uptime :	00:03:29
Registered AP :	0a-00-3e-45-11-ee 3.65-pmp450-Ap_209.124
Registered AP Software Version :	CANOPY 21.0 (Build DEV-186)
Color Code :	212 (Primary)
Sector ID :	0
Channel Frequency :	3630.000 MHz
Channel Bandwidth :	20.0 MHz
Cyclic Prefix :	1/16
Air Delay :	1700 ns, approximately 254 meters Min: 100 ns 14 meters Max:1750 ns 262 meters
Receive Power :	-51.0 dBm
Signal Strength Ratio :	0.3dB B - A
Signal to Noise Ratio :	43 B / 43 A dB
Path Info :	Path A = -45° Path B = +45°
Beacons / Maps :	100% (min/avg/max)
AP Frame Utilization :	Downlink:0% Uplink:0% (last minute)
EIRP :	17 dBm
Transmit Power :	4 dBm
Total Antenna Gain :	13 dBi
CBRS Status :	Enabled by AP

Frame Configuration Information	
Data Slots Down :	129
Data Slots Up :	43
Contention Slots :	3

Region Specific Information	
Region Code :	United Kingdom

cnMaestro Connection Stats	
Connection Status :	Resolving URL (cloud.cambiumnetworks.com - Default Cloud URL)
AccountID :	

Site Information	
Site Name :	450b LG
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
Maximum Throughput :	Unlimited
Time Updated and Location Code :	03/02/2018 09:16:11 - INTL

Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the SM, its module type and its MAC address.
Board Type	This field indicates the series of hardware.
Product Type	This indicates model of the device.
Software Version	This field indicates the system release, the time and date of the release. If you request technical support, provide the information from this field.
CPU Usage	This field indicates the current CPU utilization of the device.
Board MSN	This field indicates the Manufacturer's Serial number. A unique serial number assigned to each radio at the factory for inventory and quality control.
Board Model	This field indicates the Manufacturer's Model number.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).
Ethernet Interface	This field indicates the speed and duplex state of Ethernet interface to the SM.
Regional Code	A parameter that offers multiple fixed selections, each of which automatically implements frequency band range restrictions for the selected region. Units shipped to regions other than the United States must be configured with the corresponding Country Code to comply with local regulatory requirements.
DFS	This field indicates that DFS operation is enabled based on the configured region code, if applicable.
Antenna Type	The current antenna type that has been selected.

Attribute	Meaning
Frame Period	This field indicates the current Frame Period setting of the radio in ms.
Encryption	This field indicates the capability and the encryption configuration of the device.
Temperature	The current operating temperature of the board.
Session Status	This field displays the following information about the current session: Scanning indicates that this SM currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page. Syncing indicates that this SM currently attempts to receive sync. Registering indicates that this SM has sent a registration request message to the AP and has not yet received a response. Registered indicates that this SM is both: • registered to an AP. • ready to transmit and receive data packets.
Session Uptime	This field displays the duration of the current link. The syntax of the displayed time is hh:mm:ss.
Registered AP	Displays the MAC address and site name of the AP to which the SM is registered to. This parameter provides click-through proxy access to the AP's management interface.
Color Code	This field displays a value from 0 to 254 indicating the SM's configured color code. For registration to occur, the color code of the SM and the AP must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes).
Channel Frequency	This field lists the current operating frequency of the radio.
Channel Bandwidth	The size in MHz of the operating channel.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Air Delay	This field displays the current air delay in nanoseconds between this SM and the AP, and the distance that computes to. The distances reported as less than 200 feet (61 meters) are unreliable. If the Nomadic Mode feature is enabled, this field will also include minimum and maximum air delays measured for this SM since this air interface connection was established.

Attribute	Meaning
Receive Power	This field lists the current combined receive power level, in dBm.
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power.
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor.
Beacons	Displays a count of beacons received by the SM in percentage. This value must be typically between 99-100%. If lower than 99%, it indicates a problematic link. This statistic is updated every 16 seconds.
Transmit Power	This field lists the current combined transmit power level, in dBm. Note The red SM message “target power exceeded maximum” does not necessarily indicate a problem. 7 dBm (target power [24 dBm] exceeded maximum) In this case, the AP is requesting the SM to transmit at a higher power level, but the SM is restricted due to EIRP limits or hardware capabilities. This message can be an indication that the SM is deployed further from the AP than optimal, causing the AP to adjust the SM to maximum transmit power.
Data Slots Down	This field lists the number of slots used for downlink data transmission.
Data Slots Up	This field lists the number of slots used for uplink data transmission.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. See Contention slots .
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the SM Configuration page. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.
Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page.
Maximum Throughput	This field indicates the limit of aggregate throughput for the SM and is based on the default (factory) limit of the SM and any floating license that is currently assigned to it.
Time Updated and Location Code	This field displays information about the keying of the radio.

Note

For PMP 450 SM 900 MHz, there is additional parameter Path Info (under Subscriber Module Stats) which displays polarization path(A & B) information.

Device Information	
Device Type :	900MHz - Subscriber Module - 0a-00-3e-45-fc-36
Board Type :	P11 C120
Software Version :	CANOPY 14.2 (Build 12) SM-DES
Board MSN :	6069RU0TYJ
Board Model :	C009045C001A
FPGA Version :	040716
Uptime :	00:30:16
System Time :	02:36:06 02/13/2011 IST
Main Ethernet Interface :	No Link
Region Code :	Other
Antenna Type :	External
Frame Period :	5.0 ms
Temperature :	78 °C / 172 °F

Subscriber Module Stats	
Session Status :	REGISTERED VC 18 Rate 8X/6X MIMO-B
Session Uptime :	00:26:35
Registered AP :	0a-00-3e-45-86-f0 SIT-waterfall
Color Code :	86 (Primary)
Channel Frequency :	912.00 MHz
Channel Bandwidth :	10.0 MHz
Cyclic Prefix :	1/16
Air Delay :	175 ns, approximately 0.016 miles (86 feet)
Receive Power :	-71.9 dBm
Signal Strength Ratio :	3.0dB B - A
Signal to Noise Ratio :	28 B / 28 A dB
Path Info :	Path A = -45° Path B = +45°
Beacons :	100 %
Transmit Power :	25 dBm
Total Antenna Gain :	0 dBi (0 dBi external + 0 dBi internal)

General Status page of BHM

The BHM's General Status page is explained in below table.

Table 115: General Status page attributes - BHM

Device Information	
Device Type :	5.7GHz MIMO OFDM - Backhaul - Timing Master - 0a-00-3e-bb-b0-c1
Board Type :	P13
Product Type :	PTP 450i
Software Version :	CANOPY 15.1.5 BHUL450-None
CPU Usage :	2%
Board MSN :	M9TJ1G92GCJH
Board Model :	C050045B001A
FPGA Version :	020118
Uptime :	01:01:51
System Time :	23:19:08 01/02/2016 UTC
Main Ethernet Interface :	100Base-TX Full Duplex
Aux Ethernet Interface :	Disabled (PoE Disabled)
Region Code :	Other
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	5750.0 MHz
Channel Bandwidth :	40.0 MHz
Cyclic Prefix :	1/16
Frame Period :	5.0 ms
Color Code :	38
Transmit Power :	16 dBm
Total Antenna Gain :	0 dBi
Temperature :	31 °C / 88 °F
802.3at Type 2 PoE Status :	Not Present (Ignored)

Backhaul Stats	
Timing Slave Status :	Connected
Sync Pulse Status :	Generating Sync
Sync Pulse Source :	Self Generate

Frame Configuration Information	
Data Slots Down :	191
Data Slots Up :	192

cnMaestro Connection Stats	
Connection Status :	Remote management using cnMaestro is disabled
AccountID :	

Site Information	
Site Name :	
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
Time Updated and Location Code :	01/03/2018 05:59:03 - FXGD

Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the BHM, its module type and its MAC address.
Board Type	This field indicates the series of hardware.
Product Type	This indicates model of the device.
Software Version	This field indicates the system release, the time and date of the release. If you request technical support, provide the information from this field.

Attribute	Meaning
CPU Usage	This field indicates the current CPU utilization of the device.
Board MSN	This field indicates the Manufacture's Serial number. A unique serial number assigned to each radio at the factory for inventory and quality control.
Board Model	This field indicates the Manufacturer's Model number.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. Any BHS that registers to a BHM inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).
Ethernet Interface	This field indicates the speed and duplex state of Ethernet interface to the BHM.
Antenna Type	The current antenna type that has been selected.
Temperature	The current operating temperature of the board.
Session Status	This field displays the following information about the current session: Scanning indicates that this BHS currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page. Syncing indicates that this BHM currently attempts to receive sync. Registering indicates that this BHM has sent a registration request message to the BHM and has not yet received a response. Registered indicates that this BHM is both: • Registered to a BHM. • Ready to transmit and receive data packets.
Session Uptime	This field displays the duration of the current link. The syntax of the displayed time is hh:mm:ss.
Registered Backhaul	Displays the MAC address and site name of the BHM to which the BHS is registered to. This parameter provides click-through proxy access to the BHM's management interface.
Channel Frequency	This field lists the current operating frequency of the radio.
Receive Power	This field lists the current combined receive power level, in dBm.
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power.
Transmit Power	This field lists the current combined transmit power level, in dBm.

Attribute	Meaning
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor.
Beacons	Displays a count of beacons received by the BHM in percentage. This value must be typically between 99-100%. If lower than 99%, it indicates a problematic link. This statistic is updated every 16 seconds.
Air Delay	This field displays the distance in feet between this BHS and the BHM. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.
Data Slots Down	This field lists the number of slots used for downlink data transmission.
Data Slots Up	This field lists the number of slots used for uplink data transmission.
Regional Code	A parameter that offers multiple fixed selections, each of which automatically implements frequency band range restrictions for the selected region. Units shipped to regions other than the United States must be configured with the corresponding Country Code to comply with local regulatory requirements.
Site Name	This field indicates the name of the physical module. Assign or change this name in the Configuration > SNMP page. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.
Time Updated and Location Code	This field displays information about the keying of the radio.

General Status page of BHS

The BHS's General Status page is explained in below table.

Table 116: General Status page attributes - BHS

Device Information	
Device Type :	4.9/5.9GHz MIMO OFDM - Backhaul - Timing Slave - 0a-00-3e-bb-ae-1b
Board Type :	P13
Product Type :	PTP 450i
Software Version :	CANOPY 15.1.5 BHUL450-DES
CPU Usage :	2%
Board MSN :	M9TJ1DRLGM5L
Board Model :	C050045B001A
FPGA Version :	020118
Uptime :	01:00:23
System Time :	23:22:08 01/02/2016 UTC
Main Ethernet Interface :	No Link
Aux Ethernet Interface :	Disabled (PoE Disabled)
Region Code :	Other
DFS :	Idle
Antenna Type :	External
Frame Period :	5.0 ms
Temperature :	27 °C / 81 °F
802.3at Type 2 PoE Status :	Not Present (Ignored)

Timing Slave Stats	
Session Status :	REGISTERED VC 18 Rate 8X/1X MIMO-A VC 255 Rate 8X/8X MIMO-B
Session Uptime :	00:59:53
Registered Backhaul :	0a-00-3e-bb-b0-c1
Channel Frequency :	5750.0 MHz
Channel Bandwidth :	40.0 MHz
Cyclic Prefix :	1/16
Air Delay :	100 ns, approximately 0.009 miles (49 feet)
Receive Power :	-42.9 dBm
Signal Strength Ratio :	2.0dB V - H
Signal to Noise Ratio :	43 V / 43 H dB
Transmit Power :	16 dBm
Total Antenna Gain :	0 dBi
Beacons :	100 %

Frame Configuration Information	
Data Slots Down :	191
Data Slots Up :	192

Region Specific Information	
Region Code :	Other

cnMaestro Connection Stats	
Connection Status :	Device Not Claimed (cloud.cambiumnetworks.com - Default Cloud URL)
AccountID :	

Site Information	
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Feature Key Information	
Time Updated and Location Code :	01/03/2018 06:11:06 - HJDJ

Attribute	Meaning
Device Type	See General Status page of BHS
Board Type	
Software Version	
CPU Usage	
Board MSN	
Board Model	
FPGA Version	
Uptime	
System Time	
Ethernet Interface	
Antenna Type	
Temperature	
Session Status	
Session Uptime	
Registered Backhaul	
Channel Frequency	
Receive Power	
Signal Strength Ratio	
Transmit Power	
Signal to Noise Ratio	
Beacons	
Air Delay	
Data Slots Down	
Data Slots Up	
Regional Code	
Site Name	See General Status page of BHS
Site Contact	
Site Location	
Time Updated and Location Code	

Viewing Session Status

The Session Status page in the Home page provides information about each SM or BHS that has registered to the AP or BHM. This information is useful for managing and troubleshooting a system. This page also includes the current active values on each SM or BHS for MIR and VLAN, as well as the source of these values, representing the SM/BHS itself, Authentication Server, or the Authentication Server and SM/BHS.

> **Note**
>
> For accurate power level readings to be displayed, traffic must be present on the radio link.

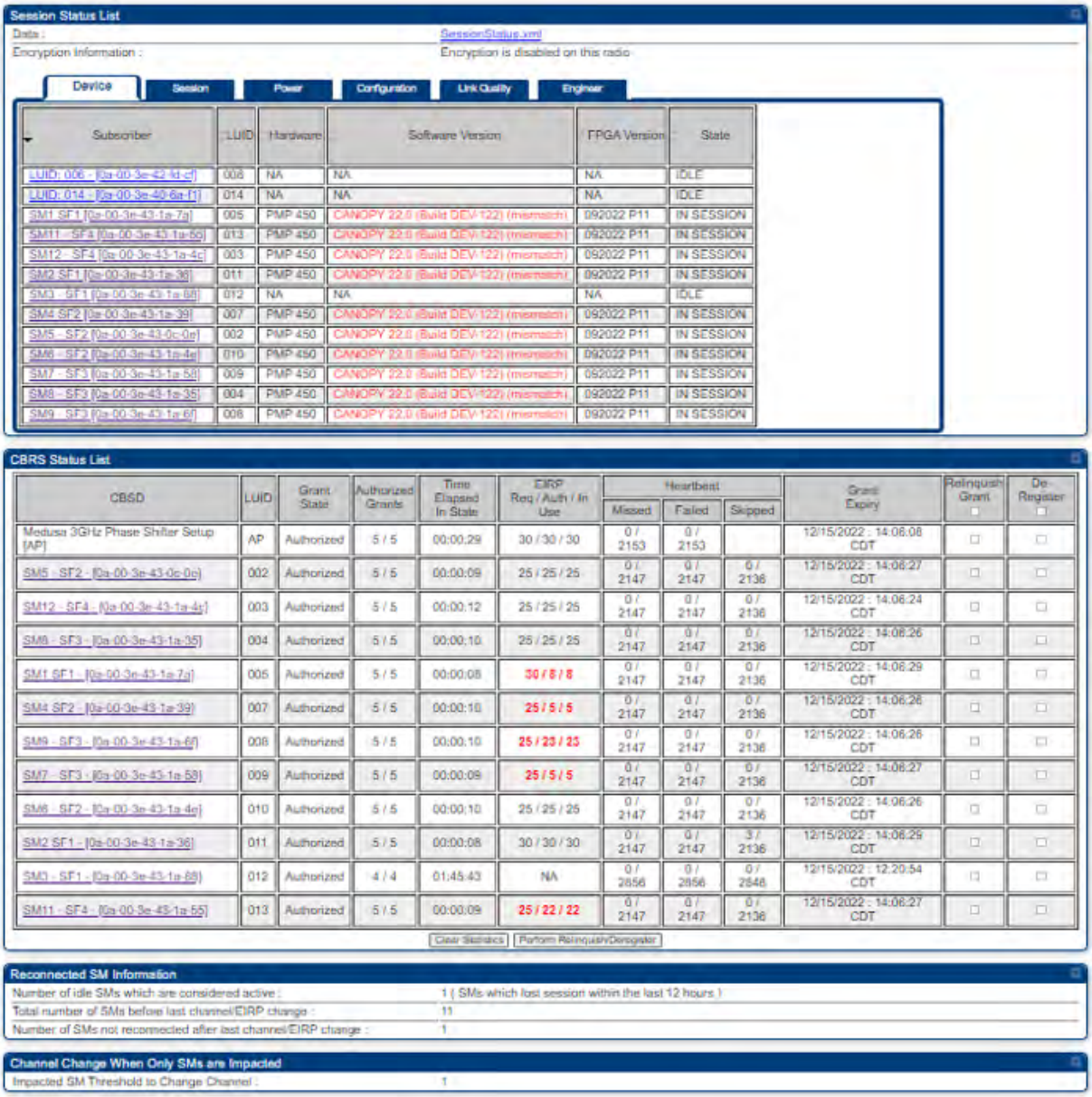
The Session Status List has four tabs: Device, Session, Power, Configuration, and Link Quality.

The Session Status .xml hyper link allows user to export session status page from web management interface of AP or BHM. The session status page will be exported in xml file.

Device tab

The Device tab provides information on the Subscriber's LUID and MAC, Hardware, Software, FPGA versions and the state of the SM/BHS (Registered and/or encrypted).

Table 117: Device tab attributes



Session Status List

Data : SessionStatus.xml

Encryption Information : Encryption is disabled on this radio

Device | Session | Power | Configuration | Link Quality | Engineer

Subscriber	LUID	Hardware	Software Version	FPGA Version	State
LUID: 006 - [0a-00-3e-42-fd-cf]	006	NA	NA	NA	IDLE
LUID: 014 - [0a-00-3e-40-6a-[1]	014	NA	NA	NA	IDLE
SM1 SF1 [0a-00-3e-43-1a-7g]	005	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM11 - SF4 [0a-00-3e-43-1a-55]	013	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM12 - SF4 [0a-00-3e-43-1a-4c]	003	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM2 SF1 [0a-00-3e-43-1a-36]	011	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM3 - SF1 [0a-00-3e-43-1a-68]	012	NA	NA	NA	IDLE
SM4 SF2 [0a-00-3e-43-1a-39]	007	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM5 - SF2 [0a-00-3e-43-0c-0e]	002	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM6 - SF2 [0a-00-3e-43-1a-4e]	010	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM7 - SF3 [0a-00-3e-43-1a-58]	009	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM8 - SF3 [0a-00-3e-43-1a-35]	004	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION
SM9 - SF3 [0a-00-3e-43-1a-6f]	008	PMP 450	CANOPY 22.0 (Build DEV-122) (mismatch)	092022 P11	IN SESSION

CBRS Status List

CBSD	LUID	Grant State	Authorized Grants	Time Elapsed In State	EIRP Req / Auth / In Use	Heartbeat Missed	Heartbeat Failed	Heartbeat Skipped	Grant Expiry	Relinquish Grant	De-Register
Medusa 3GHz Phase Shifter Setup [AP]	AP	Authorized	5 / 5	00:00:29	30 / 30 / 30	0 / 2153	0 / 2153		12/15/2022 : 14:06:08 CDT		
SM5 - SF2 - [0a-00-3e-43-0c-0e]	002	Authorized	5 / 5	00:00:09	25 / 25 / 25	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:27 CDT		
SM12 - SF4 - [0a-00-3e-43-1a-4c]	003	Authorized	5 / 5	00:00:12	25 / 25 / 25	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:24 CDT		
SM8 - SF3 - [0a-00-3e-43-1a-35]	004	Authorized	5 / 5	00:00:10	25 / 25 / 25	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:26 CDT		
SM1 SF1 - [0a-00-3e-43-1a-7g]	005	Authorized	5 / 5	00:00:08	30 / 8 / 8	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:29 CDT		
SM4 SF2 - [0a-00-3e-43-1a-39]	007	Authorized	5 / 5	00:00:10	25 / 5 / 5	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:26 CDT		
SM9 - SF3 - [0a-00-3e-43-1a-6f]	008	Authorized	5 / 5	00:00:10	25 / 23 / 23	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:26 CDT		
SM7 - SF3 - [0a-00-3e-43-1a-58]	009	Authorized	5 / 5	00:00:09	25 / 5 / 5	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:27 CDT		
SM6 - SF2 - [0a-00-3e-43-1a-4e]	010	Authorized	5 / 5	00:00:10	25 / 25 / 25	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:26 CDT		
SM2 SF1 - [0a-00-3e-43-1a-36]	011	Authorized	5 / 5	00:00:08	30 / 30 / 30	0 / 2147	0 / 2147	3 / 2136	12/15/2022 : 14:06:29 CDT		
SM3 - SF1 - [0a-00-3e-43-1a-68]	012	Authorized	4 / 4	01:45:43	NA	0 / 2856	0 / 2856	0 / 2548	12/15/2022 : 12:20:54 CDT		
SM11 - SF4 - [0a-00-3e-43-1a-55]	013	Authorized	5 / 5	00:00:09	25 / 22 / 22	0 / 2147	0 / 2147	0 / 2136	12/15/2022 : 14:06:27 CDT		

Clear Statistics | Perform Relinquish/Deregister

Reconnected SM Information

Number of idle SMs which are considered active : 1 (SMs which lost session within the last 12 hours)

Total number of SMs before last channel/EIRP change : 11

Number of SMs not reconnected after last channel/EIRP change : 1

Channel Change When Only SMs are Impacted

Impacted SM Threshold to Change Channel : 1

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name of the SM/BHS. **Note**: The MAC is a hot link to open the interface to the SM/BHS. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view. Site Name indicates the name of the SM/BHS. Change this name on the Configuration web page of the SM/BHS. This information is also set into the sysName SNMP MIB-II object and can be polled by an SNMP management server.

Attribute	Meaning
LUID	This field displays the LUID (logical unit ID) of the SM/BHS. As each SM or BHS registers to the AP/BHM, the system assigns an LUID of 2 or a higher unique number to the SM/BHS. If a SM/BHS loses registration with the AP/BHS and then regains registration, the SM/BHS will retain the same LUID. **Note**: Both the LUID and the MAC are hot links to open the interface to the SM/BHS. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
Hardware	This field displays the SMs or BHS hardware type.
Software Version	This field displays the software release that operates on the SM/BHS, the release date and time of the software.
FPGA Version	This field displays the version of FPGA that runs on the SM/BHS
State	This field displays the current status of the SM/BHS as either • IN SESSION to indicate that the SM/BHS is currently registered to the AP/BHM. • IDLE to indicate that the SM/BHS was registered to the AP/BHM at one time, but now is not. This field also indicates whether the encryption scheme in the module is enabled.
Airlink Security	Attribute is available if AP security setting is AES. Will be missing if security setting is NONE. Possible values are AES-128 and AES-256.
Grant State	This field displays the current Grant State such as Registered, Granted, Suspended, Authorized and Unregistered.
Authorized Grants	The field indicates the total number of AUTHORIZED grants for this device, followed by the total number of grants for this device. If the Multigrant feature is disabled, there will never be more than 1 grant per device.
Time Elapsed In State	Displays the time since the last state change.
EIRP Req/Auth/In Use	**Req:** EIRP requested in the Grant Request. **Auth:** EIRP allowed by the SAS in the grant response. CBRS operators using Federated Wireless SAS might also see a TMP flag in this field. This indicates that the Authorized grant value is a **same day** grant value - a temporary value while the SAS does more precise calculations on what a final value could be. This TMP flag would be cleared in less than 24 hours - at the next CBRS CPAs interval, at which time the final EIRP value, which can be more, less, or equal to the TMP value, would be granted.

Attribute	Meaning
	In Use: For SMs, this value is the smaller of the **granted EIRP** and the **Max EIRP** configured on the SM. It represents the largest EIRP value the SM can power control up to. A cnMaestro obtained grant value larger than the SMs configured Max EIRP is 1 scenario where this **In Use** value is lower than the Authorized value. A runtime edit of the SM's Max EIRP to a value lower than the authorized value is another example, although in this case the **In Use** value does not reflect the edit until the next SM or AP reboot.
Heartbeat	**Missed:** The heartbeat request was sent but no response was received. **Failed:** The heartbeat response was received with a failure code. **Skipped:** The AP did not include this SM in the HB exchange (For SM only).
Grant Expiry	Displays the Day/Time grant expires.
Relinguish Grant	Check and click **Perform Religuish/Deregister** button to relinquish this grant. Keep checked to prevent the device to request the same grant.
De-Register	Check and click the **Perform Religuish/Deregister** button to de-register this device (and relinquish associated grants). Keep checked to prevent the device from de-registering.
Number of idle SMs which are considered active	This is a count of the number of SMs that, after a channel/EIRP change, are currently in IDLE state and are being tracked and expected to reconnect to compute the percentage used in the SM Reconnection Percentage alarm feature. SMs that were IDLE just before a channel/EIRP change, but had a connected state at any time in the 12 hours before the channel/EIRP are counted. Additionally, if the AP rebooted 12 hours before the channel/EIRP change, all IDLE SMs are counted.
Total number of SMs before last channel/EIRP change	This is the total number of SMs that were connected before the most recent change and the number of SMs that were idle just before the channel/EIRP change but are being considered active per the definition described in the **Number of idle SMs which are considered active** above.
Number of SMs not reconnected after last channel/EIRP change	This is a count of the number of SMs that are expected to reconnect, but have not reconnected to the air interface since the last channel/EIRP change.
Channel Change When Only SMs are Impacted	This statistic is a computation of the number of active SMs that need to experience a termination or suspension before the **Channel Change When Only SMs are Impacted** feature is invoked, moving the sector's channel, based only on CBRS SM terminations or suspensions while the AP is authorized. Only currently active SMs factor into this statistic. For example, if four SMs are active and the **Threshold for Channel Change** configuration item is left at its default value of 10%, then this statistic has a value of 1. Changing the **Threshold for Channel Change** configuration value from 10% to 26% changes this statistic to a value of 2.

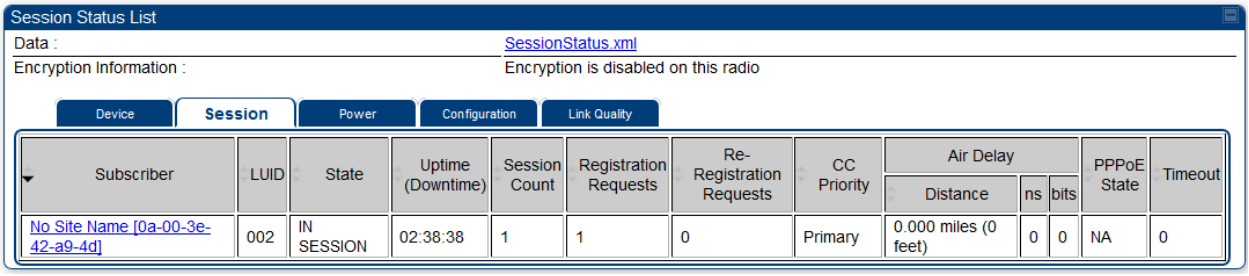
Note

Reconnected SM Information table of counters is not normally visible – it's not visible after an AP upgrade or reboot. The table will appear and begin updating when a channel/EIRP change has been made.

Session tab

The Session tab provides information on the SMs or BHS Session Count, Reg Count, Re-Reg Count, Uptime, Air delay, PPPoE State and Timeouts.

Table 118: Session tab attributes



Session Status List

Data : SessionStatus.xml

Encryption Information : Encryption is disabled on this radio

Device | Session | Power | Configuration | Link Quality

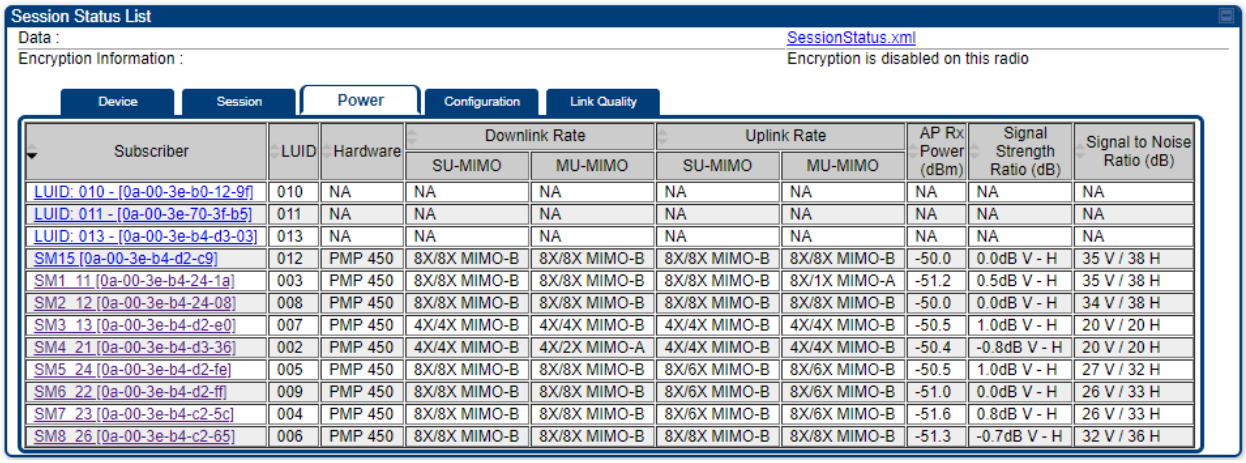
Subscriber	LUID	State	Uptime (Downtime)	Session Count	Registration Requests	Re-Registration Requests	CC Priority	Air Delay			PPPoE State	Timeout
								Distance	ns	bits		
No Site Name [0a-00-3e-42-a9-4d]	002	IN SESSION	02:38:38	1	1	0	Primary	0.000 miles (0 feet)	0	0	NA	0

Attribute	Meaning
Subscriber	See Device tab attributes
LUID	See Device tab attributes
State	This filed displays the status of the registered SM.
Uptime (Downtime)	Once a SM/BHS successfully registers to an AP/BHM, this timer is started. If a session drops or is interrupted, this timer is reactivated once re-registration is complete.
Session Count	This field displays how many sessions the SM/BHS has had with the AP/BHM. Typically, this is the sum of Registration Requests and Re-Registration Requests. However, the result of internal calculation may display here as a value that slightly differs from the sum. If the number of sessions is significantly greater than the number for other SMs or BHS, then this may indicate a link problem or an interference problem.
Registration Requests	When a SM/BHS makes a Registration Request, the AP/BHM checks its local session database to see whether it was registered earlier. If the AP/BHM concludes that the SM/BHS is not currently in session database and it is valid Registration Request, then the request increments the value of this field. In ideal situation, the Registration Requests indicates total number of connected SMs to an AP. **Note** The user can clear Registration Requests by dropping all current sessions of SM (or BHS) from Configuration > Tools > Sessions menu.
Re-Registration Requests	When a SM/BHS makes a Registration Request, the AP/BHM checks its local session database to see whether it was registered earlier. If the AP/BHM concludes that the SM/BHS is currently in session database, then the request increments the value of this field. Typically, a Re-Registration Requests is the case where both: • SM/BHS attempts to reregister for having lost communication with the AP/BHM.

Attribute	Meaning
	• AP/BHM has not yet observed the link to the SM/BHS as being down. It is possible for a small period of time if there is no downlink traffic and AP/BHM still assumes the session is up, but the SM/BHS, loses session and quickly re-connects before the AP/BHM knew the session had dropped. This is how a re-registration happens. If the number of sessions is significantly greater than the number for other SMs or BHS, then this may indicate a link problem (check mounting, alignment, receive power levels) or an interference problem (conduct a spectrum scan).
CC Priority	The field displays Color Code Priority (ICC, Primary, Secondary or Tertiary) of all connected SM.
AirDelay	This field displays the distance of the SM/BHS from the AP/BHM in meters, nanoseconds and bits. At close distances, the value in this field is unreliable.
PPPoE state	This field displays the current PPPoE state (whether configured) of the SM/BHS.
Timeout	This field displays the timeout in seconds for management sessions via HTTP, ftp access to the SM/BHS. 0 indicates that no limit is imposed.

Power tab

Table 119: Power tab attributes



Session Status List

Data : SessionStatus.xml

Encryption Information : Encryption is disabled on this radio

Device | Session | Power | Configuration | Link Quality

Subscriber	LUID	Hardware	Downlink Rate		Uplink Rate		AP Rx Power (dBm)	Signal Strength Ratio (dB)	Signal to Noise Ratio (dB)
			SU-MIMO	MU-MIMO	SU-MIMO	MU-MIMO			
LUID: 010 - [0a-00-3e-b0-12-9f]	010	NA	NA	NA	NA	NA	NA	NA	NA
LUID: 011 - [0a-00-3e-70-3f-b5]	011	NA	NA	NA	NA	NA	NA	NA	NA
LUID: 013 - [0a-00-3e-b4-d3-03]	013	NA	NA	NA	NA	NA	NA	NA	NA
SM15 [0a-00-3e-b4-d2-c9]	012	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	-50.0	0.0dB V - H	35 V / 38 H
SM1_11 [0a-00-3e-b4-24-1a]	003	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	8X/1X MIMO-A	-51.2	0.5dB V - H	35 V / 38 H
SM2_12 [0a-00-3e-b4-24-08]	008	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	-50.0	0.0dB V - H	34 V / 38 H
SM3_13 [0a-00-3e-b4-d2-e0]	007	PMP 450	4X/4X MIMO-B	4X/4X MIMO-B	4X/4X MIMO-B	4X/4X MIMO-B	-50.5	1.0dB V - H	20 V / 20 H
SM4_21 [0a-00-3e-b4-d3-36]	002	PMP 450	4X/4X MIMO-B	4X/2X MIMO-A	4X/4X MIMO-B	4X/4X MIMO-B	-50.4	-0.8dB V - H	20 V / 20 H
SM5_24 [0a-00-3e-b4-d2-fe]	005	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/6X MIMO-B	8X/6X MIMO-B	-50.5	1.0dB V - H	27 V / 32 H
SM6_22 [0a-00-3e-b4-d2-ff]	009	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/6X MIMO-B	8X/6X MIMO-B	-51.0	0.0dB V - H	26 V / 33 H
SM7_23 [0a-00-3e-b4-c2-5c]	004	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/6X MIMO-B	8X/6X MIMO-B	-51.6	0.8dB V - H	26 V / 33 H
SM8_26 [0a-00-3e-b4-c2-65]	006	PMP 450	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	8X/8X MIMO-B	-51.3	-0.7dB V - H	32 V / 36 H

Attribute	Meaning
Subscriber	See Device tab attributes
LUID	
Hardware	This field displays the SMs or BHS hardware type.
Downlink Rate SU-MIMO	This field displays whether the high-priority channel is enabled in the SM/BHS and the status of rate adapt. For example, if “8X/4X” is listed, the radio is capable of operating at 8X but is currently operating at 4X, due to RF conditions.

Attribute	Meaning
	This field also states whether it is MIMO-A or MIMO-B radio e.g. “8X/8X MIMO-B” indicates MIMO-B and “8X/4X MIMO-A” indicates MIMO-A. A data channel starts at its lowest modulation and slowly rate adapts up, as traffic is successfully transmitted over the data channel. From system release 15.2, all data channels in a single SM will have the same modulation rates. Note: The SU-MIMO rate applies to all AP platforms. For 450m, this field indicates the rate being used for symbols where this particular VC is not being MU-MIMO grouped with other SMs.
Downlink Rate MU-MIMO	This field indicates the modulation rate used for symbols where the low or medium priority data channels are MU-MIMO scheduled by grouping it in the same slot with other low or Medium priority data channels from other SM's.
Uplink Rate SU-MIMO	This field the status of rate adapt. For example, if “8X/4X” is listed, the radio is capable of operating at 8X but is currently operating at 4X, due to RF conditions. This field also states whether it is MIMO-A or MIMO-B radio e.g. “8X/8X MIMO-B” indicates MIMO-B and “8X/4X MIMO-A” indicates MIMO-A. A data channel starts at its lowest modulation and slowly rate adapts up, as traffic is successfully transmitted over the data channel. From system release 15.2, all data channels in a single SM will have the same modulation rates. Note: The SU-MIMO rate applies to all AP platforms. For 450m, this field indicates the rate being used for symbols where this particular VC is not being MU-MIMO grouped with other SMs.
Uplink Rate MU-MIMO	This field indicates the modulation rate used for symbols where the MUMIMO groupable data channels are MU-MIMO scheduled by grouping it in the same slot with other MU-MIMO groupable data channels from other SM's.
AP Rx Power (dBm)	This field indicates the AP’s or BHM’s combined receive power level for the listed SM/BHS.
Signal Strength Ratio (dB)	This field displays the ratio of the Vertical path received signal power to the Horizontal path received signal power. This ratio can be useful for determining multipathing conditions (high vertical to horizontal ratio) for Uplink.
Signal to Noise Ratio (dB)	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor. In other words, it indicates signal to noise ratio for Uplink.

Configuration tab

The Configuration tab provides information on the SMs or BHS Uplink or Downlink (UL/DL) Sustained Data Rate, UL/DL Burst Allocation, UL/DL Burst Rate, UL/DL Low Priority CIR, UL/DL Medium Priority CIR UL/DL High Priority CIR, UL/DL Ultra High Priority CIR, the UL/DL Broadcast or Multicast Allocation, SM Prioritization Group, RADIUS Authentication Reply, and RADIUS Authentication Server. This data is refreshed based on the Web Page Auto Update setting on the AP’s or BHS’s General Configuration page.

Table 120: Configuration tab attributes

Session Status List

Data : SessionStatus.xml

Encryption Information : Encryption is disabled on this radio

Device | Session | Power | Configuration | Link Quality

Subscriber	LUID		Sustained Data Rate Cap (kbps)	Sustained Data Rate (kbps)	Burst Allocation (kbit)	Max Burst Rate (kbit)	Low Priority CIR (kbps)	Medium Priority CIR (kbps)	High Priority CIR (kbps)	Ultra High Priority CIR (kbps)	Broadcast/Multicast Allocation	SM Prioritization Group (Disabled)	RADIUS Authentication Reply	RADIUS Authentication Server
No Site Name [0a-00-3e-42-a9-4d]	002	Uplink	4000	4000(AAA)	2900(AAA)	5000(AAA)	0(D)	NA	0(D)	NA	50000(D)	Low(D)	SM on 10.110.207.101	10.110.207.101
		Downlink		4000(AAA)	2900(AAA)	5000(AAA)	0(D)	NA	0(D)	NA				

Attribute	Meaning
Subscriber	See Device tab attributes
LUID	
Sustained Data Rate Cap (kbps)	This field specifies the maximum sustained data rate between SM/BHS and AP/BHM. If this field displays “Uncapped”, then there is no limit set for data rate. If this field displays 4000, then the maximum sustained data rate between SM/BHS and AP/BHM is limited to 4000 kbps.
Sustained Data Rate (kbps) - Uplink	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified rate at which each SM/BHS registered to this AP/BHM is replenished with credits for transmission. The configuration source of the value is indicated in parentheses. See Maximum Information Rate (MIR) Parameters on page 1.
Sustained Data Rate (kbps) - Downlink	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified the rate at which the AP/BHM should be replenished with credits (tokens) for transmission to each of the SMs/BHS’s in its sector. The configuration source of the value is indicated in parentheses. See Maximum Information Rate (MIR) Parameters.
Burst Allocation (kbit) - Uplink	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified maximum amount of data that each SM/BHS is allowed to transmit before being recharged at the Sustained Uplink Data Rate with credits to transmit more. The configuration source of the value is indicated in parentheses. See Interaction of Burst Allocation and Sustained Data Rate Settings.
Burst Allocation (kbit) - Downlink	This field displays the value that is currently in effect for the SM/BHS, with the source of that value in parentheses. This is the specified the rate at which the AP/BHM should be replenished with credits (tokens) for transmission to each of the SMs/BHS’s in its sector. The configuration source of the value is indicated in parentheses. See Interaction of Burst Allocation and Sustained Data Rate Settings.
Max Burst Rate (kbit) - Uplink	The data rate at which an SM/BHS is allowed to burst (until burst allocation limit is reached) before being recharged at the Sustained Uplink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited.

Attribute	Meaning
	See Interaction of Burst Allocation and Sustained Data Rate Settings.
Max Burst Rate (kbit) - Downlink	The data rate at which an SM/BHS is allowed to burst (until burst allocation limit is reached) before being recharged at the Sustained Downlink Data Rate with credits to transit more. When set to 0 (default), the burst rate is unlimited. See Interaction of Burst Allocation and Sustained Data Rate Settings.
Low Priority CIR	This field indicates the minimum rate at which low priority traffic is sent over the uplink and downlink (unless CIR is oversubscribed or RF link quality is degraded).
Medium Priority CIR	This field indicates the minimum rate at which medium priority traffic is sent over the uplink and downlink (unless CIR is oversubscribed or RF link quality is degraded).
High Priority CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink and downlink (unless CIR is oversubscribed or RF link quality is degraded).
Ultra High Priority CIR	This field indicates the minimum rate at which ultra high priority traffic is sent over the uplink and downlink (unless CIR is oversubscribed or RF link quality is degraded).
Broadcast/Multicast Allocation	This field displays the data rate at which Broadcast and Multicast traffic is sent via the radio link.
SM Prioritization Group	This field displays the priority level configured on the SM under SM Prioritization Group.
RADIUS Authentication Reply	This field displays whether RADIUS server is reachable or not.
RADIUS Authentication Server	This field displays the associated RADIUS Authentication Server for each SM where it was authenticated. This information is useful when there are multiple RADIUS servers (maximum three servers supported by Cambium). If one server is not reachable, other configured servers are tried in sequential order as a fall-back. In this scenario, the Session Status is useful to identify associate RADIUS Authentication Server for all connected SMs.

Table 121: Session Status > Configuration CIR configuration denotations

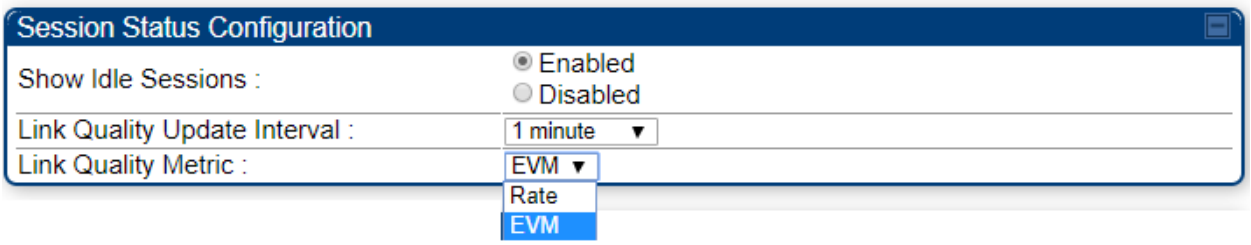
Attribute	Meaning
(SM)	QoS/VLAN parameters are derived from the SM's/BHS's settings
(APCAP)	QoS/VLAN parameters are derived from the AP's settings, including any keyed capping (for radios capped at 4 Mbps, 10 Mbps, or 20 Mbps)
(D)	QoS/VLAN parameters are retrieved from the device, due to failed retrieval from the AAA or WM server.
(AAA)	QoS/VLAN parameters are retrieved from the RADIUS server
(BAM)	QoS/VLAN parameters are retrieved from a WM BAM server

Link Quality tab

The Link Quality tab provides information on the Subscriber's UID, Link quality, Downlink, Uplink, Beacon, ReReg, and the Uptime.

This data is refreshed based on the Link Quality Update Interval parameter configuration under the Sessions Status page.

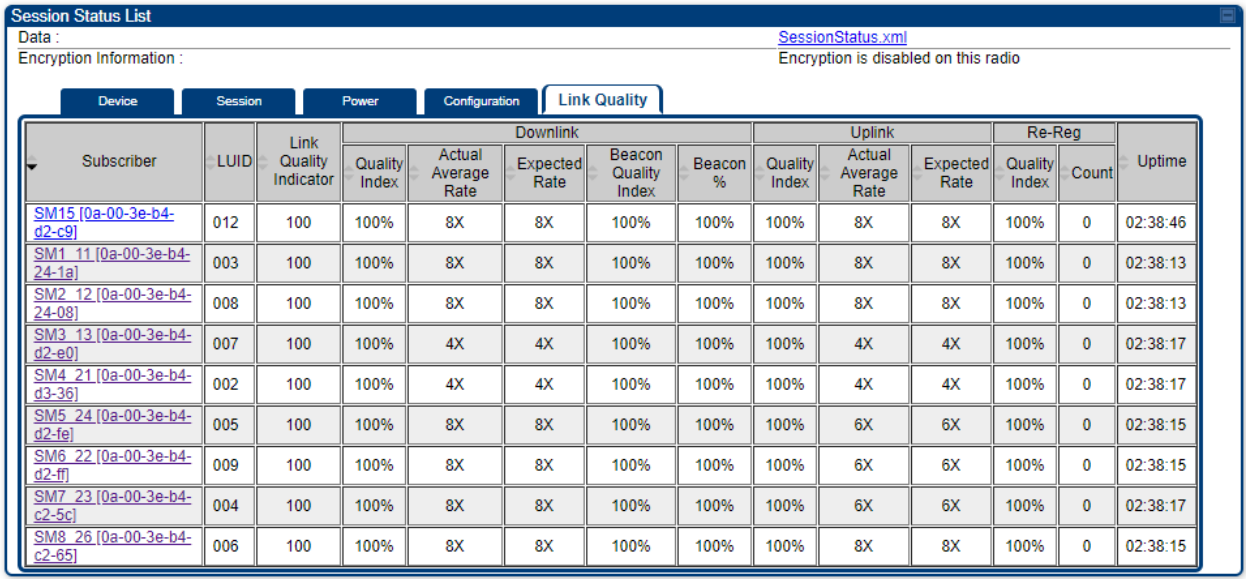
Link Quality Metric parameter offers an option to choose either EVM or Rate based LQI calculation.



The Link Quality tab displays the calculated Link Quality Indicator (LQI) for the configured interval (Link Quality Update Interval parameter).

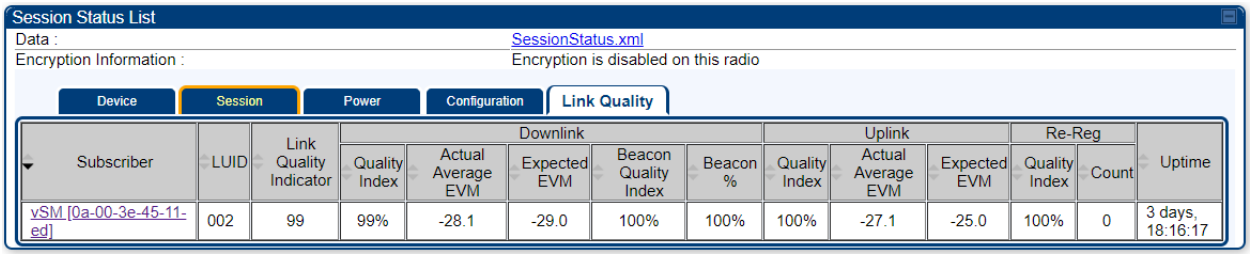
Table 122: Link Quality tab attributes

Link Quality Metric: Rate



Subscriber	LUID	Link Quality Indicator	Downlink					Uplink			Re-Reg		Uptime
			Quality Index	Actual Average Rate	Expected Rate	Beacon Quality Index	Beacon %	Quality Index	Actual Average Rate	Expected Rate	Quality Index	Count	
SM15 [0a-00-3e-b4-d2-c9]	012	100	100%	8X	8X	100%	100%	100%	8X	8X	100%	0	02:38:46
SM1_11 [0a-00-3e-b4-24-1a]	003	100	100%	8X	8X	100%	100%	100%	8X	8X	100%	0	02:38:13
SM2_12 [0a-00-3e-b4-24-08]	008	100	100%	8X	8X	100%	100%	100%	8X	8X	100%	0	02:38:13
SM3_13 [0a-00-3e-b4-d2-e0]	007	100	100%	4X	4X	100%	100%	100%	4X	4X	100%	0	02:38:17
SM4_21 [0a-00-3e-b4-d3-36]	002	100	100%	4X	4X	100%	100%	100%	4X	4X	100%	0	02:38:17
SM5_24 [0a-00-3e-b4-d2-fe]	005	100	100%	8X	8X	100%	100%	100%	6X	6X	100%	0	02:38:15
SM6_22 [0a-00-3e-b4-d2-ff]	009	100	100%	8X	8X	100%	100%	100%	6X	6X	100%	0	02:38:15
SM7_23 [0a-00-3e-b4-c2-5c]	004	100	100%	8X	8X	100%	100%	100%	6X	6X	100%	0	02:38:17
SM8_26 [0a-00-3e-b4-c2-65]	006	100	100%	8X	8X	100%	100%	100%	8X	8X	100%	0	02:38:15

Link Quality Metric: EVM



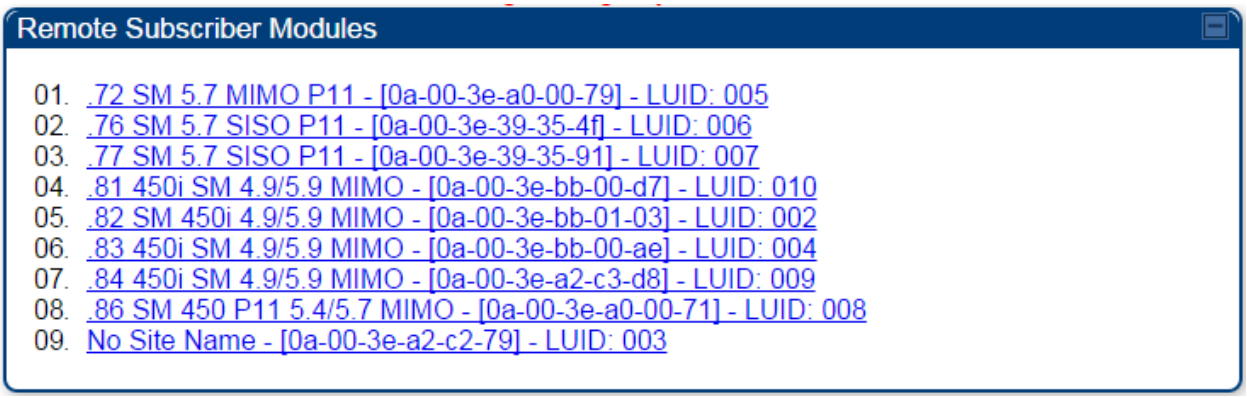
Subscriber	LUID	Link Quality Indicator	Downlink					Uplink			Re-Reg		Uptime
			Quality Index	Actual Average EVM	Expected EVM	Beacon Quality Index	Beacon %	Quality Index	Actual Average EVM	Expected EVM	Quality Index	Count	
vSM [0a-00-3e-45-11-ed]	002	99	99%	-28.1	-29.0	100%	100%	100%	-27.1	-25.0	100%	0	3 days, 18:16:17

Attribute	Meaning
Subscriber	See Device tab attributes
LUID	
Link Quality Indicator	This field displays quality of the link. It is calculated based on receive power, modulation rate, re-registrations and beacon percentage.
Downlink - Quality Index	This field displays the downlink quality in percentage. It is calculated based on Downlink receiver power, modulation rate, and beacon percentage.
Downlink - Actual Average Rate	This field displays the average Downlink modulation rate. For 450m, this field specifies the SU-MIMO Modulation Rate. When Rate based LQI is selected, only actual rate and expected rate will be displayed.
Downlink - Actual Average EVM	This field displays the average Downlink EVM rate.
Downlink - Expected Rate	This field displays the expected modulation rate based on receive power in Downlink. When EVM based LQI is selected, only actual EVM and expected EVM will be displayed.
Downlink - Beacon Quality Index	This field displays the beacon quality index. It is calculated based on beacon percentage.
Downlink - Beacon %	This field displays the received beacon percentage.
Uplink - Quality Index	This field displays the uplink quality in percentage. It is calculated based on Uplink receiver power and modulation rate.
Uplink -Actual Average Rate	This field displays the average Uplink modulation rate.
Uplink -Actual Average EVM	This field displays the average Uplink EVM rate.
Uplink - Expected Rate	This field displays the expected modulation rate based on receive power in Uplink.
Re-Reg - Quality Index	This field displays the re-registration quality. It is calculated based on the re-registration count.
Re-Reg Count	This field displays the number of re-registrations.
Uptime	This field displays the uptime of the device.

Viewing Remote Subscribers

This page allows to view the web pages of registered SMs or BHS over the RF link. To view the pages for a selected SM/BHS, click its link. The General Status page of the SM opens.

Figure 105: *Remote Subscribers page of AP*



Interpreting messages in the Event Log

Each line in the Event Log of a module Home page begins with a time and date stamp. However, some of these lines wrap as a combined result of window width, browser preferences and line length. You may find this tab easiest to use if you expand the window till all lines are shown beginning with time and date stamp.

Time and Date Stamp

The time and date stamp reflect one of the following:

- GPS time and date directly or indirectly received from the CMM4.
- NTP time and date from a NTP server (CMM4 may serve as an NTP server)
- The running time and date that you have set in the Time & Date web page.

> **Note**
>
> In the Time & Date web page, if you have left any time field or date field unset and clicked the Set Time and Date button, then the time and date default to 00:00:00 UT: 01/01/00.
>
> A reboot causes the preset time to pause or, in some cases, to run in reverse. Additionally, a power cycle resets the running time and date to the default 00:00:00 UT: 01/01/00. Thus, whenever either a reboot or a power cycle has occurred, must reset the time and date in the Time & Date web page of any module that is not set to receive sync.

Event Log Data Collection

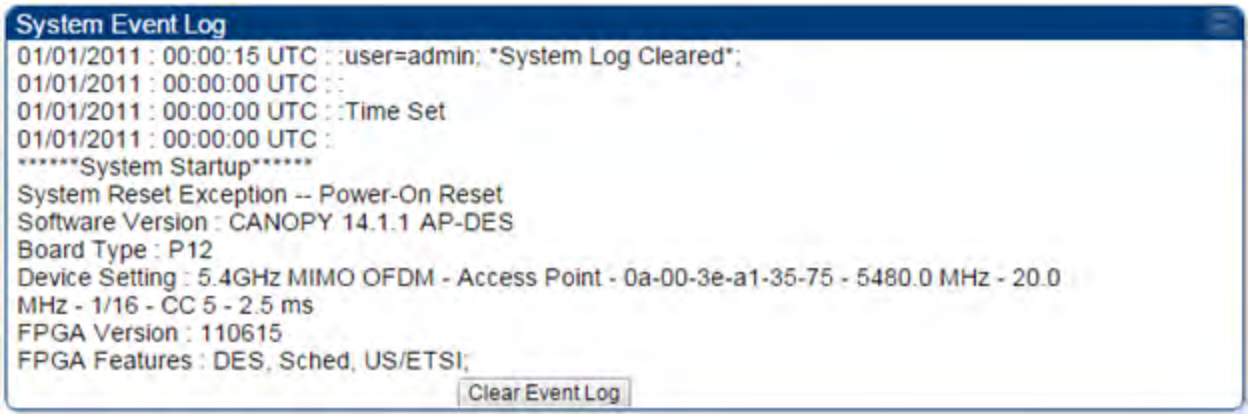
The collection of event data continues through reboots and power cycles. When the buffer allowance for event log data is reached, the system adds new data into the log and discards an identical amount of the oldest data.

Each line that contains the expression WatchDog flags an event that was both:

- considered by the system software to have been an exception
- recorded in the preceding line.

Conversely, a Fatal Error () message flags an event that is recorded in the next line. Some exceptions and fatal errors may be significant and require either operator action or technical support.

Figure 106: *Event log data*



Messages that Flag Abnormal Events

The messages listed below flag abnormal events and, case by case, may signal the need for corrective action or technical support.

Table 123: Event Log messages for abnormal events

Event Message	Meaning
FatalError ()	The event recorded on the line immediately beneath this message triggered the Fatal Error ().
Loss of GPS Sync Pulse	Module has lost GPS sync signal.
Machine Check Exception	This is a symptom of a possible hardware failure. If this is a recurring message, begin the RMA process for the module.
System Reset Exception External Hard Reset	The unit lost power or was power cycled.
System Reset Exception External Hard Reset WatchDog	The event recorded on the preceding line triggered this WatchDog message.

Messages that Flag Normal Events

The messages listed below record normal events and typically do not signal a need for any corrective action or technical support.

Table 124: Event Log messages for normal events

Event Message	Meaning
Acquired GPS Sync Pulse.	Module has acquired GPS sync signal.
FPGA Features	Type of encryption.
FPGA Version	FPGA (JBC) version in the module.

Event Message	Meaning
GPS Date/Time Set	Module is now on GPS time.
Reboot from Webpage	Module was rebooted from management interface.
Software Boot Version	Boot version in the module.
Software Version	The software release and authentication method for the unit.
System Log Cleared	Event log was manually cleared.

Viewing the Network Interface

In any module, the LAN1 Network Interface section of this tab displays the defined Internet Protocol scheme for the Ethernet interface to the module. In SM/BHS devices, this page also provides an RF Public Network Interface section, which displays the Internet Protocol scheme defined for network access through the master device (AP/BHM).

Figure 107: *Network Interface tab of the AP*

LAN1 Network Interface	
Ethernet Interface :	1000Base-TX Full Duplex
IP address :	10.120.226.64
Subnet Mask :	255.255.254.0
Gateway IP address :	10.120.226.254
Preferred DNS Server :	10.120.12.31
Alternate DNS Server :	10.120.12.30
DHCP status :	DHCP not enabled

Figure 108: *Network Interface tab of the SM*

LAN1 Network Interface	
Ethernet Interface :	1000Base-TX Full Duplex
IP address :	10.120.216.220
Subnet Mask :	255.255.255.0
Gateway IP address :	10.120.216.254
Preferred DNS Server :	0.0.0.0
Alternate DNS Server :	0.0.0.0
DHCP status :	DHCP not enabled

Viewing the Layer 2 Neighbors

In the Layer 2 Neighbors tab, a module reports any device from which it has received a message in Link Layer Discovery Protocol within the previous two minutes. Given the frequency of LLDP messaging, this means that the connected device will appear in this tab 30 seconds after it is booted and remain until two minutes after its shutdown.

Figure 109: *Layer 2 Neighbors page*

System statistics

This section describes how to use the system statistics pages to manage the performance of the PMP/PTP 450 Platform Family link.

Viewing the Scheduler Statistics

The **Statistics -> Scheduler** page is applicable for all modules (AP/SM/BHM/BHS) and the parameters are displayed as shown below:

Table 125: Radio Statistics attributes for (AP/SM/BHM/BHS)

Radio Statistics	
Transmit Unicast Data Count :	6715
Transmit Broadcast Data Count :	904747
Transmit Multicast Data Count :	0
Receive Unicast Data Count :	1328470
Receive Broadcast Data Count :	57683
Receive Multicast Data Count :	0
Transmit Control Count :	98
Receive Control Count :	177
In Sync Count :	0
Out of Sync Count :	0
Overrun Count :	0
Underrun Count :	0
Receive Corrupt Data Count :	0
Receive Corrupt Control Data Count :	0
Receive Bad Broadcast Control Count :	0
Rcv LT Start :	3
Rcv LT Start HS :	5
Rcv LT Result :	5
Xmt LT Result :	0
Frame Too Big :	0
Bad RCV Fragment :	0
Bad RCV Fragment Length :	0
VC Clear Error Count :	0
Rx No Buffer Count :	0
Scheduler Error :	90
Transmit Ring Error :	0
TDD Slips :	0

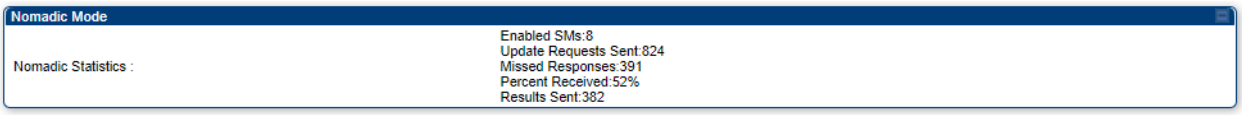
Attribute	Meaning
Transmit Unicast Data Count	Total amount of unicast packets transmitted from the radio
Transmit Broadcast Data Count	Total amount of broadcast packets transmitted from the radio
Transmit Multicast Data Count	Total amount of multicast packets transmitted by the radio
Receive Unicast Data Count	Total amount of unicast packets received by the radio
Receive Broadcast Data Count	Total amount of broadcast packets received by the radio

Attribute	Meaning
Receive Multicast Data Count	Total amount of multicast packets received by the radio
Transmit Control Count	Amount of radio control type messages transmitted (registration requests and grants, etc.)
Receive Control Count	Amount of radio control type messages received (registration requests and grants, etc.)
In Sync Count	Number of times the radio has acquired sync. When GPS synchronization is used it is number of times GPS sync acquired. For the SM, it is the number of times the SM successfully obtained sync with an AP.
Out of Sync Count	Number of times the radio lost same sync lock
Overrun Count	Number of times FPGA frame has overrun its TX Frame
Underrun Count	Number of times FPGAs TX Frame aborted prematurely
Receive Corrupt Data Count	Number of times a corrupt packet has been received at the FPGA.
Receive Corrupt Control Data Count	Number of times a corrupt control data packet has been received at the FPGA.
Receive Bad Broadcast Control Count	Number of times the radio has received an invalid control message via broadcast (SM only).
Rcv LT Start	Number of Link Test Start messages received. A remote radio has requested that this radio start a link test to it.
Rcv LT Start HS	Number of Link Test Start Handshake messages received. This radio requested that a remote radio start a link test and the remote radio has sent a handshake back acknowledging the start.
Rcv LT Result	This radio received Link Test results from the remote radio under test. When this radio initiates a link test, the remote radio will send its results to this radio for display.
Xmt LT Result	This radio transmitted its link test results to the remote radio under test. When the remote radio initiates a link test, this radio must send its results to the remote radio for display there.
Frame Too Big	This statistic indicates the number of packets received and processed by the radios which were greater than max packet size 1700 bytes.
Bad Acknowledgment	This statistic indicates the number of packets received as bad acknowledgment. It is for engineering use only.
Bad Fragment	This statistic indicates number of fragments tagged internally as bad. It is for engineering use only.
VC Clear Error Count	This statistic indicates number of times VC clear failed.

Attribute	Meaning
Rx No Buffer Count	Currently unused
Scheduler Error	This error is incremented when the scheduler cannot send or get scheduled to send a packet. It is also called as “VC Error”.
Transmit Ring Error	This is a state that records when Canopy’s MAC Transmit Ring Error. One or more of these will cause the session to drop and be re-established. That static should be zero. If you are seeing this statistic increment, please contact Cambium support.
TDD Slips	TDD Slips indicate that the 450m AP processer is heavily loaded and could lead to buffer discards.

The **Nomadic Mode** table is applicable for all modules (AP/SM) and the parameters are displayed as shown below:

Table 126: Nomadic mode for AP



Attribute	Meaning
Enabled SMs	The number of registered SMs in this sector that have the Nomadic Mode feature enabled.
Update Requests Sent	Nomadic mode ranging updates are a 3 step exchange. The first step is an update request sent to the SM from the AP. This statistic counts the total number of these update requests sent to all the nomadic mode enabled SMs in the sector since the stats were last cleared.
Missed Responses	The second step in the 3 step ranging update exchange is an update response sent from the SM to the AP. Because these responses use the sector's contention space, missed responses will be common.
Percent Received	This is simply the percentage of responses that were not missed.
Results sent	The third step in the 3 steps ranging from update exchange is a Nomadic Mode result sent to the SM. Note that not received update responses will be valid, so it's common that the Results Sent/Update Requests Sent rate may be less than the Percent Received.

Note

The Nomadic Mode feature is not supported on PMP 450m and in PTP modes.

Table 127: Nomadic mode for SM

Attribute	Meaning
Update Responses Sent	The number of Nomadic Mode update responses sent to the AP.

Viewing list of Registration Failures statistics

SM Registration Failures page of AP

The SM Registration Failures tab identifies SMs that have recently attempted and failed to register to this AP. With its time stamps, these instances may suggest that a new or transient source of interference exists.

Table 128: SM Registration Failures page attributes - AP

Attribute	Meaning
Status 17 Flag 0	No response was received from the AAA server and hence SM is trying to send a session request again.

BHS Registration Failures page of BHM

Table 129: BHS Registration Failures page attributes - BHM

Attribute	Meaning
Status 17 Flag 0	No response was received from the AAA server and hence BHS is trying to send a session request again.

There is a list of flags from 0 to 20 as shown in Flags status and the “Flags” can be ignored.

Table 130: Flags status

Flag	Meaning	Flag	Meaning
0	Normal	11	AP Lite Limit Reached
1	Out of Range	12	Only Ver 9.5+ Allowed
2	No Luids	13	Temporary Data VC for AAA
3	BH ReRange	14	AAA Authentication Failure

Flag	Meaning	Flag	Meaning
4	Auth Fail	15	Registration Grant Reject
5	Encrypt Fail	16	Blank
6	Power Adjust	17	AAA Session Retry
7	No VCs	18	AAA Reauth Failure
8	Reserve VC Fail	19	RegReq at zero power
9	Activate VC Fail	20	RegReq no time ref
10	Hi VC Setup Fail	-	-

Interpreting Bridging Table statistics

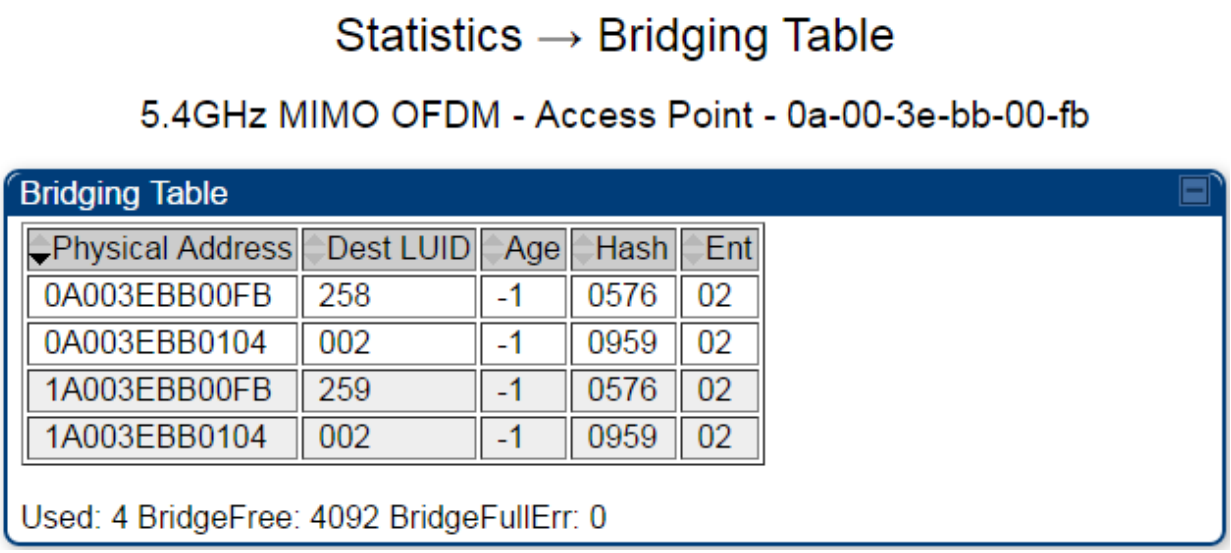
If NAT (network address translation) is not active on the SM/BHS, then the Bridging Table page provides the MAC address of all devices that are attached to registered SMs/BHS (identified by LUIDs).

The SM/BHS management MAC addresses are also added in bridge table upon SMs/BHS registration. These entries will be remove automically from the table once SMs/BHS is de-registered. This alleviates the arp cache > bridge cache timeout problems.

The bridging table allows data to be sent to the correct module as follows:

- For the AP/BHM, the uplink is from RF to Ethernet. Thus, when a packet arrives in the RF interface to the AP/BHM, the AP/BHM reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the RF interface.
- For the SM/BHS, the uplink is from Ethernet to RF. Thus, when a packet arrives in the Ethernet interface to one of these modules, the module reads the MAC address from the inbound packet and creates a bridging table entry of the source MAC address on the other end of the Ethernet interface.

Figure 110: *Bridging Table page*



The Bridging Table supports up to 4096 entries.

Interpreting Translation Table statistics

When Translation Bridging is enabled in the AP, each SM keeps a table mapping MAC addresses of devices attached to the AP to IP addresses, as otherwise the mapping of end-user MAC addresses to IP addresses is lost. (When Translation Bridging is enabled, an AP modifies all uplink traffic originating from registered SMs such that the source MAC address of every packet is changed to that of the SM which bridged the packet in the uplink direction.)

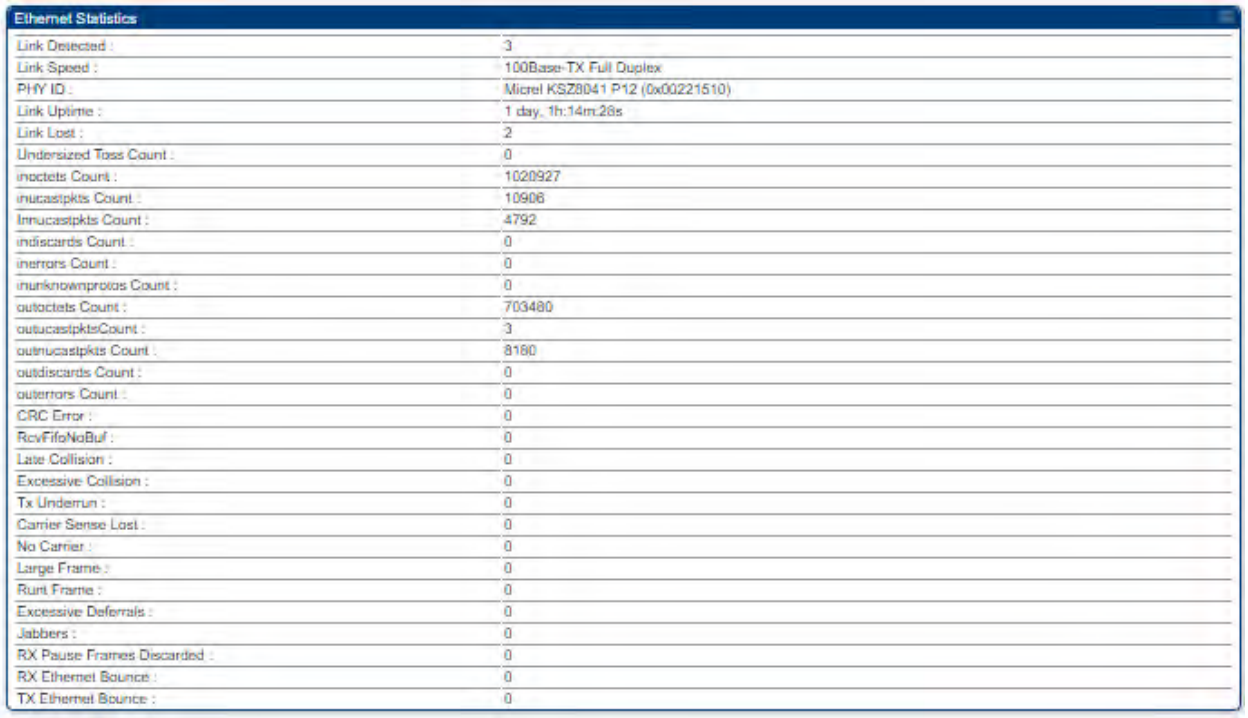
Figure 111: *Translation Table page of SM*

Interpreting Ethernet statistics

The Statistics > Ethernet page reports TCP throughput and error information for the Ethernet connection of the module. This page is applicable for all modules (AP/SM/BHM/BHS).

The Ethernet page displays the following fields.

Table 131: Ethernet tab attributes



Ethernet Statistics	
Link Detected :	3
Link Speed :	100Base-TX Full Duplex
PHY ID :	Micrel KSZ8041 P12 (0x00221510)
Link Uptime :	1 day, 1h:14m:28s
Link Lost :	2
Undersized Toss Count :	0
inoctets Count :	1020927
inucastpkts Count :	10906
Innucastpkts Count :	4792
indiscards Count :	0
inerrors Count :	0
inunknownprotos Count :	0
outoctets Count :	703480
outucastpktsCount :	3
outnucastpkts Count :	8180
outdiscards Count :	0
outerrors Count :	0
CRC Error :	0
RcvFifoNoBuf :	0
Late Collision :	0
Excessive Collision :	0
Tx Underrun :	0
Carrier Sense Lost :	0
No Carrier :	0
Large Frame :	0
Runt Frame :	0
Excessive Deferrals :	0
Jabbers :	0
RX Pause Frames Discarded :	0
RX Ethernet Bounce :	0
TX Ethernet Bounce :	0

Attribute	Meaning
Link Detected	3 indicates that an Ethernet link is established to the radio, 0 indicates that no Ethernet link is established.
Link Speed	This field indicates the speed of the link set of negotiated.
PHY ID	This field indicates the identifier of the Ethernet PHY chip on the PCB.
Link Uptime	This field indicates how long the Ethernet link has been up.
Link Lost	This field indicates a count of how many times the Ethernet link was lost.
Undersized Toss Count	This field indicates the number of packets that were too small to process and hence discarded.
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
indiscards Count	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. (Some of these packets may have been discarded to increase buffer space.)
inerrors Count	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
inunknownprotos Count	This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.
outoctets Count	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
outnucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outdiscards Count	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrrors Count	This field displays how many outbound packets contained errors that prevented their transmission.
RxBabErr	This field displays how many receiver babble errors occurred.
RcvFifoNoBuf	This field displays the number of times no FIFO buffer space was able to be allocated.

Attribute	Meaning
	Note: PMP 450 AP running in Gigabit Ethernet Mode displays error “RcfFifoNoBuf” which indicates packet loss. For 450 AP platforms, if ethernet auto-negotation is set to Gigabit, then it is a known limitation that “RcfFifoNoBuf” error will be seen. This issue is not seen if autonegotation is set to 100Mbps or lower, and the issue is not seen on 450i or 450m AP's.
RxOverrun	This field displays how many receiver overrun errors occurred on the Ethernet controller.
Late Collision	This field displays how many late collisions occurred on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. A collision that occurs after the first 512 bits is considered a late collision. **Caution** A late collision is a serious network problem because the frame being transmitted is discarded. A late collision is most commonly caused by a mismatch between duplex configurations at the ends of a link segment.
Excessive Collisions	This field displays the number of packets whose retransmission limit expired.
TxUnderrun	This field displays how many transmission-underrun errors occurred on the Ethernet controller.
Carrier Sense Lost	This field displays how many carrier sense lost errors occurred on the Ethernet controller.
No Carrier	This field displays how many no carrier errors occurred on the Ethernet controller.
Large Frame	An ethernet packet that has been recieved that is greater than the board MTU, or a segmented frame.
Excessive Deferrals	The number of frames that are not sent after the time exceeds the maximum-packet time.
Jabbers	A count of the number of attempts to send a packet > 2048 bytes.
RX Pause Frames Discarded	A count of the number of Ethernet pause frames discarded.
RX Ethernet Bounce	Number of times ethernet link has been bounced due to not receiving any ethernet packets over the configured ethernet bounce timeout interval.
TX Ethernet Bounce	Number of times ethernet link has been bounced due to not transmitting any ethernet packets over the configured ethernet bounce timeout interval.

Interpreting RF Control Block statistics

The Statistics > Radio page is applicable for all module (AP/SM/BHM/BHS). The Radio page of the Statistics page displays the following fields.

Table 132: Radio (Statistics) page attributes – RF Control Block

RF Control Block Statistics	
inoctets Count :	653532396
inucastpkts Count :	423096
Innucastpkts Count :	35848043
indiscards Count :	0
inerrors Count :	0
inunknownprotos Count :	0
outoctets Count :	138721214
outucastpktsCount :	401826
outnucastpkts Count :	13855
outdiscards Count :	120
outerrors Count :	0

Attribute	Meaning
inoctets Count	This field displays how many octets were received on the interface, including those that deliver framing information.
inucastpkts Count	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Innucastpkts Count	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
indiscards Count	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. This stat is pegged whenever corrupt data is received by software or whenever the RF Software Bridge queue is full. Corrupt data is a very unusual event because all packets are CRC checked by hardware before being passed into software. The likely case for indiscards is if the RF bridge queue is full. If this is the case the radio is most likely PPS limited due to excessive small packet traffic or a problem at the Ethernet interface. If there is a problem at the Ethernet interface there is likely to be discards at the Ethernet as well.
inerrors Count	This field displays how many inbound packets contained errors that prevented their delivery to a higher-layer protocol.
inunknownprotos Count	This field displays how many inbound packets were discarded because of an unknown or unsupported protocol.
outoctets Count	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
outucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.

Attribute	Meaning
outnucastpkts Count	This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.
outdiscards Count	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. (Some of these packets may have been discarded to increase buffer space.)
outerrrors Count	This field displays how many outbound packets contained errors that prevented their transmission.

Interpreting Sounding statistics for AP

In the 450m AP GUI, sounding statistics can be found under Statistics > Sounding Statistics.

Table 133: Sounding Statistics - 450m AP page attributes

Sounding Statistics

Subscriber	LUID	Spatial Frequency	Azimuth (Degrees)	Downlink		Uplink	
				Sounding State	MU-MIMO Rate	Sounding State	MU-MIMO Rate
SM4_21 [0a-00-3e-b4-d3-36]	002	879	-59.7, -9.1, 41.6	TRACKING	4X/2X MIMO-A	TRACKING	4X/4X MIMO-B
SM1_11 [0a-00-3e-b4-24-1a]	003	2	-50.6, 0.1, 50.7	TRACKING	8X/8X MIMO-B	TRACKING	8X/1X MIMO-A
SM7_23 [0a-00-3e-b4-c2-5c]	004	879	-59.7, -9.1, 41.6	TRACKING	8X/8X MIMO-B	TRACKING	8X/6X MIMO-B
SM5_24 [0a-00-3e-b4-d2-fe]	005	879	-59.7, -9.1, 41.6	TRACKING	8X/8X MIMO-B	TRACKING	8X/6X MIMO-B
SM8_26 [0a-00-3e-b4-c2-65]	006	879	-59.7, -9.1, 41.6	TRACKING	8X/8X MIMO-B	TRACKING	8X/8X MIMO-B
SM3_13 [0a-00-3e-b4-d2-e0]	007	2	-50.6, 0.1, 50.7	TRACKING	4X/4X MIMO-B	TRACKING	4X/4X MIMO-B
SM2_12 [0a-00-3e-b4-24-08]	008	2	-50.6, 0.1, 50.7	TRACKING	8X/8X MIMO-B	TRACKING	8X/8X MIMO-B
SM6_22 [0a-00-3e-b4-d2-ff]	009	879	-59.7, -9.1, 41.6	TRACKING	8X/8X MIMO-B	TRACKING	8X/6X MIMO-B
SM15 [0a-00-3e-b4-d2-c9]	012	2	-50.6, 0.1, 50.7	TRACKING	8X/8X MIMO-B	TRACKING	8X/8X MIMO-B

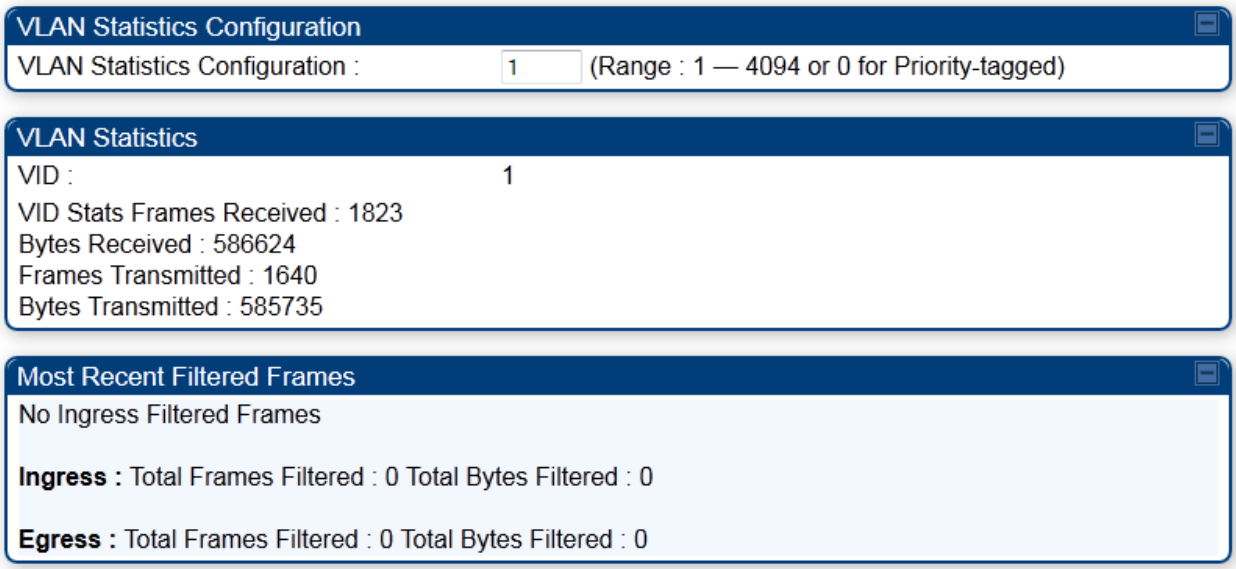
Attribute	Meaning
Subscriber	This field displays the MAC address and Site Name of the SM/BHS. As each SM or BHS registers to the AP/BHM.
LUID	This field displays the LUID (logical unit ID) of the SM/BHS. As each SM or BHS registers to the AP/BHM, the system assigns an LUID of 2 or a higher unique number to the SM/BHS. If a SM/BHS loses registration with the AP/BHS and then regains registration, the SM/BHS will retain the same LUID.
Spatial Frequency	This field displays the spatial frequency value of the LUID or SM. Values 0 to 1023 are valid and value 2048 is considered as invalid.
Azimuth	This field displays the Azimuth range in degrees corresponding to the spatial frequencies of the bin. The zero-degree azimuth is boresight. **Note** Some SF ranges correspond to multiple azimuth ranges. This is because for some spatial frequencies the AP generates beams in multiple azimuth directions. The SM can be physically located in any of the azimuth ranges.
Downlink - Sounding State	Different types of Sounding states are:

Attribute	Meaning
	• UNKNOWN: SM has recently registered to the AP but not registered with the channel manager yet. • NEW: SM has been registered with the channel manager and will soon transition to ASSESSING. • ASSESSING: AP will instruct SM to take the channel measurements. Channel estimates and spatial frequencies will be calculated. • TRACKING: Valid measurements resulted in good channel estimates and spatial frequency. This SM can now be used for MU-MIMO. • INVALID: Inconsistent measurements resulting in no channel estimate or spatial frequency. This SM cannot be used for MU-MIMO and it will ultimately be re-assessed. • NOT ELIGIBLE: Due to poor RF link conditions, the RF link as rate adapted down to SU-MIMO transmissions.
Downlink - MU-MIMO Rate	This field indicates the modulation rate used for symbols where this particular LUID is MU-MIMO scheduled by grouping it in the same slot with other LUIDs.
Uplink - Sounding State	This field indicates the status of uplink sounding.
Uplink - MU-MIMO Rate	This field indicates the modulation rate used for symbols where the MU-MIMO groupable data channels are MU-MIMO scheduled by grouping it in the same slot with other MU-MIMO groupable data channels from other SM's.

Interpreting VLAN statistics

The Statistics > VLAN page provides a list of the most recent packets that were filtered because of VLAN membership violations. It is applicable for all modules (AP/SM/BHM/BHS).

Table 134: VLAN page attributes



Attribute	Meaning
Unknown	This must not occur. Contact Technical Support.
Only Tagged	The packet was filtered because the configuration is set to accept only packets that have an 802.1Q header and this packet did not.
Ingress	When the packet entered through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
Local Ingress	When the packet was received from the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership. This must not occur. Contact Technical Support.
Egress	When the packet attempted to leave through the wired Ethernet interface, the packet was filtered because it indicated an incorrect VLAN membership.
Local Egress	When the packet attempted to reach the local TCP/IP stack, the packet was filtered because it indicated an incorrect VLAN membership.

Interpreting Data Channels statistics

The Statistics > Data Channels page displays information about data channels used in data communications. This page is applicable for all modules (AP/SM/BHM/BHS).

The Data VC tab displays the fields as explained in Data Channel page attributes.

Table 135: Data Channel page attributes

Data Channel Statistics

Subscriber	LUID	Channel Priority	Inbound Statistics					Outbound Statistics					Queue Overflow	High Priority Queue
			octets	ucast pkts	nucast pkts	discards	errors	octets	ucast pkts	nucast pkts	discards	errors		
SM4_21	002	Low	88471406	8	51742	0	0	78002604	681	45566	0	0	0	160
SM4_21	002	Medium	107730	0	63	0	0	107730	0	63	0	0	0	0
SM4_21	002	High	107730	0	63	0	0	107730	0	63	0	0	0	0
SM4_21	002	Ultra High	1038574	6678	100	0	0	152829	158	311	0	0	0	406
SM1_11	003	Low	1959	4	2	0	0	99422	777	0	0	0	0	241
SM1_11	003	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM1_11	003	High	0	0	0	0	0	0	0	0	0	0	0	0
SM1_11	003	Ultra High	648533	3960	36	0	0	41899	158	198	0	0	0	356
SM7_23	004	Low	10898303	5	6375	0	0	98431	811	1	0	0	0	292
SM7_23	004	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM7_23	004	High	0	0	0	0	0	0	0	0	0	0	0	0
SM7_23	004	Ultra High	636897	4008	37	0	0	45099	158	248	0	0	0	406
SM5_24	005	Low	10893173	5	6372	0	0	98204	764	1	0	0	0	234
SM5_24	005	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM5_24	005	High	0	0	0	0	0	0	0	0	0	0	0	0
SM5_24	005	Ultra High	671486	4291	37	0	0	45099	158	248	0	0	0	406
SM8_26	006	Low	14487593	5	8474	0	0	95888	742	1	0	0	0	224
SM8_26	006	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM8_26	006	High	0	0	0	0	0	0	0	0	0	0	0	0
SM8_26	006	Ultra High	751670	4625	36	0	0	45057	157	248	0	0	0	405
SM3_13	007	Low	12993053	5	7600	0	0	89789	670	1	0	0	0	154
SM3_13	007	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM3_13	007	High	0	0	0	0	0	0	0	0	0	0	0	0
SM3_13	007	Ultra High	636026	3966	36	0	0	45099	158	248	0	0	0	406
SM2_12	008	Low	21802973	5	12752	0	0	94194	739	1	0	0	0	220
SM2_12	008	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM2_12	008	High	0	0	0	0	0	0	0	0	0	0	0	0
SM2_12	008	Ultra High	637607	3981	36	0	0	45099	158	248	0	0	0	406
SM6_22	009	Low	10908563	5	6381	0	0	100175	801	1	0	0	0	275
SM6_22	009	Medium	0	0	0	0	0	0	0	0	0	0	0	0
SM6_22	009	High	0	0	0	0	0	0	0	0	0	0	0	0
SM6_22	009	Ultra High	696681	4521	36	0	0	45099	158	248	0	0	0	406
SM15	012	Low	22323135	3924	12741	0	0	142215	946	250	0	0	0	675
Multicast	252	NA	NA	NA	NA	NA	NA	86504	0	415	0	0	NA	NA
Broadcast	255	NA	NA	NA	NA	NA	NA	1006314	18	15912	0	0	NA	NA

Data Channel Statistics

Subscriber	LUID	SM Pri	Channel Priority	Inbound Statistics					Outbound Statistics				
				octets	ucast pkts	nucast pkts	discards	errors	octets	ucast pkts	nucast pkts	discards	errors
Broadcast	255	NA	NA	NA	NA	NA	NA	NA	5527765	399	25160	0	0
Multicast	252	NA	NA	NA	NA	NA	NA	NA	0	0	0	0	0
No Site Name	002	Low	Low	1948	4	1	0	0	2618	7	0	0	0
No Site Name	002	Low	High	8112944	49563	396	0	0	6033604	46613	4010	0	0

Fragments Modulation

Note: To measure the receive modulation of every fragment, Receive Quality Debug must be enabled.

Subscriber	LUID	Receive Fragments Modulation				Retransmitted Fragments
		QPSK	16-QAM	64-QAM	256-QAM	
No Site Name	002	44171 256	43626 221	43594 173	231 99	0

Attribute	Meaning
Subscriber	This field displays the MAC address and Site Name of the SM/BHS.
LUID	This field displays the LUID (logical unit ID) of the SM/BHS. As each SM or BHS registers to the AP/BHM, the system assigns an LUID of 2 or a higher unique number to the SM/BHS. If a SM/BHS loses registration with the AP/BHS and then regains registration, the SM/BHS will retain the same LUID. **Note** Both the LUID and the MAC are hot links to open the interface to the SM/BHS. In some instances, depending on network activity and network design, this route to the interface yields a blank web page. If this occurs, refresh your browser view.
Channel Priority	This field displays the channel priority for the virtual channel. The values supported are Low, Medium, High, and Ultra High.
Inbound Statistics, octets	This field displays how many octets were received on the interface, including those that deliver framing information.
Inbound Statistics, ucastpkts	This field displays how many inbound subnetwork-unicast packets were delivered to a higher-layer protocol.
Inbound Statistics, nucastpkts	This field displays how many inbound non-unicast (subnetwork-broadcast or subnetwork-multicast) packets were delivered to a higher-layer protocol.
Inbound Statistics, discards	This field displays how many inbound packets were discarded without errors that would have prevented their delivery to a higher-layer protocol. Inbound discard statistics are incremented similar to the indiscards stat on the RF control block stats page. The sum of all data VC indiscards must be close to the RF control block in discards. If indiscards are evenly distributed across SMs, then the radio is PPS limited due to either excessive small packet transmissions, or a problem at the Ethernet link. If indiscards are contained to one or a few SMs, then there is likely a problem at or underneath the SM which is incrementing the count.
Outbound Statistics, octets	This field displays how many octets were transmitted out of the interface, including those that deliver framing information.
Outbound Statistics, ucastpkts	This field displays how many packets for which the higher-level protocols requested transmission to a subnetwork-unicast address. The number includes those that were discarded or not sent.
Outbound Statistics, nucastpkts	This field displays how many packets for which the higher-level protocols requested transmission to a non-unicast (subnetwork-broadcast or subnetwork-multicast) address. The number includes those that were discarded or not sent.

Attribute	Meaning
Outbound Statistics, discards	This field displays how many outbound packets were discarded without errors that would have prevented their transmission. Outbound discard statistics are incremented if a VC is not active when a packet is ready to send. This is a rare condition.
Outbound Statistics, errors	This field displays how many outbound packets contained errors that prevented their transmission.
Queue Overflow	This is a count of packets that were discarded because the queue for the VC was already full. If Queue Overflows are being seen across most or all SMs, then there is either an interferer local to the AP or the APs RF link is at capacity. If Queue Overflows are being seen at one or only a few SMs, then it is likely that there is a problem with those specific links whether it is insufficient signal strength, interferer, or a problem with the actual SM hardware.
High Priority Queue	This is a count of packets that were received on high priority queue.
Fragments Modulation - Receive Fragments Modulation	
QPSK	This field displays how many inbound fragments were received via the QPSK modulation scheme.
16-QAM	This field displays how many inbound fragments were received via the 16-QAM modulation scheme.
64-QAM	This field displays how many inbound fragments were received via the 64-QAM modulation scheme.
256-QAM	This field displays how many inbound fragments were received via the 256-QAM modulation scheme.
Retransmitted Fragments	This field displays how many outbound fragments were retransmitted.

Interpreting Proportional Scheduler

The Statistics > Proportional Scheduler page displays information:

Table 136: MIR/Burst page attributes for AP

Trial active. Device is running in MU-MIMO mode. Please obtain a key to permanently enable MU-MIMO mode.

Proportional Scheduler Stats

Subscriber	LUID	Configuration			Downlink Statistics					Uplink Statistics				
		Lock Modulation	Modulation	Weight	Rate Plan (Kbps)	Current Modulation	Slots Percentage	Guaranteed Minimum Throughput(Kbps)	Sustained Data Rate (Kbps)	Rate Plan (Kbps)	Current Modulation	Slots Percentage	Guaranteed Minimum Throughput(Kbps)	Sustained Data Rate (Kbps)
Broadcast	255	Disable		1.0	1000	1X	11.9%	998	NA	NA	NA	NA	NA	NA
SM11 - SF4	002	Disable		1.0	10000	8X	4.4%	2949	155000	10000	8X	5.0%	3441	155000
SM3 - SF1	003	Enable Below Threshold	4X	1.0	10000	2X	8.8%	1475	155000	10000	2X	10.0%	1720	155000
SM10 - SF4	004	Disable		1.0	20000	8X	8.8%	5898	155000	20000	8X	10.0%	6881	155000
SM8 - SF3	005	Disable		1.0	10000	8X	4.4%	2949	155000	10000	8X	5.0%	3441	155000
SM9 - SF3	006	Disable		1.0	10000	8X	4.4%	2949	155000	10000	8X	5.0%	3441	155000
SM7 - SF3	007	Disable		1.0	20000	8X	8.8%	5898	155000	20000	8X	10.0%	6881	155000
SM12 - SF4	008	Disable		1.0	10000	8X	4.4%	2949	155000	10000	8X	5.0%	3441	155000
SM5 - SF2	009	Disable		1.0	10000	8X	4.4%	2949	155000	10000	8X	5.0%	3441	155000
SM2 SF1	010	Disable		1.0	10000	4X	8.8%	2949	155000	10000	4X	10.0%	3441	155000
SM4 SF2	011	Disable		1.0	20000	8X	8.8%	5898	155000	20000	8X	10.0%	6881	155000
SM6 - SF2	012	Disable		1.0	10000	8X	4.4%	2949	155000	10000	8X	5.0%	3441	155000
SM1 SF1	013	Disable		1.0	20000	4X	17.6%	5919	155000	20000	4X	20.0%	6881	155000
Total					161000		99.9%	46729	1860000	160000		100.0%	53331	1860000

Attribute	Meaning
Subscriber	See Device tab attributes
LUID	
Lock Modulation	This field displays the Lock Modulation mode of all registered SMs.
Modulation	The database configured Lock Modulation value if lock modulation is set to Enable below threshold or Enabled.
Weight	This field displays the weight of each registered SM. For more information about Weight, See QoS page attributes - AP.
Downlink Statistics	This field displays the Dowlink statistics of every registered SM.
Uplink Statistics	This field displays the Uplink statistics of every registered SM.
Rate Plan	This field displays the rate plan associated with each SM.
Current Modulation	The currently operating modulation of this SM.
Slots Percentage	This field displays the percentage of slot used by each SM.
Guaranteed minimum throughput	Guaranteed minimum throughput based on the SM's Rate Plan configuration, it's current modulation rate, and any Lock Modulation settings. For 450m AP's the maximum possible Throughput shown here assumes all SUMIMO scheduling. MUMIMO scheduling will result in higher TPUT.
Sustained Data Rate	This field displays the preset rate limit of data transfer for every SM.

Interpreting MIR/Burst statistics

The Statistics > MIR/Burst page displays information about MIR/Burst. This page is applicable for all modules (AP/SM).

The MIR/Burst tab displays the fields as explained in MIR/Burst page attributes for AP and MIR/Burst page attributes for SM.

Table 137: MIR/Burst page attributes for AP

MIR / Burst Statistics

Note: Uplink values are configuration values only. Live uplink values will be shown on the SM.

Subscriber	Current Downlink Bucket Size	Downlink MIR	Downlink MIR Per 500ms Interval	Downlink Max Bucket Size	Current Max Burst Bucket Size	Downlink Max Burst MIR	Downlink Max Burst MIR Per 500ms Interval	Uplink MIR	Uplink Max Bucket Size	Uplink Max Burst MIR
No Site Name - LUID: 002	2500000000	30000000	15000000	2500000000	0	0 (Not Limited)	0 (Not Limited)	30000000	2500000000	0 (Not Limited)

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name of the SM/BHS. As each SM or BHS registers to the AP/BHM, the system assigns an LUID of 2 or a higher unique number to the SM/BHS. As of release 15.2, if an SM/BHS loses registration with the AP/BHM and then regains registration, the SM/BHS retains the same LUID.
Current Downlink Bucket Size	This field displays the number of bits in the bucket to be potentially consumed at above-MIR rates, up to Max Burst MIR rate.
Downlink MIR	This field displays the active configured MIR rate per second. This is the rate that the bucket is filled with bits.
Downlink MIR Per 500ms Interval	This field displays the rate that the bucket is filled with bits at every 500 ms interval.
Downlink Max Bucket Size	This field displays the configured maximum bucket size, which is the maximum number of bits that can be in the bucket. The bucket fills at MIR rate and can hold this number of bits, which is a configuration value.
Current Max Burst Bucket Size	If Max Burst is enabled, there is a secondary “bucket” that controls the maximum rate of bit consumption. If Max Burst is not enabled (which means not limited), this will be 0 as the bucket is not used.
Downlink Max Burst MIR	This field displays the configured value of the Max Burst rate. This is the maximum rate at which bits can be consumed above MIR. Once excess (> MIR) bits have been consumed, the link will be throttled to MIR.
Downlink Max Burst MIR Per 500ms Interval	This field displays the configured value of the Max Burst rate at every 500 ms interval.
Uplink MIR	This field displays the active configured MIR rate per second in the SM.
Uplink Max Bucket Size	This field displays the configured maximum bucket size of the SM, which is the maximum number of bits that can be in the bucket. The bucket fills at MIR rate and can hold this number of bits, which is a configuration value.
Uplink Max Burst MIR	This field displays the configured value of the MaxBurst rate of the SM. This is the maximum rate at which bits can be consumed above MIR. Once excess (> MIR) bits have been consumed, the link will be throttled to MIR.

Table 138: MIR/Burst page attributes for SM

MIR / Burst Statistics

Note: Downlink values are configuration values only. Live downlink values will be shown on the AP.

Current Uplink Bucket Size	Uplink MIR	Uplink MIR Per 100ms Interval	Uplink Max Bucket Size	Current Max Burst Bucket Size	Uplink Max Burst MIR	Uplink Max Burst MIR Per 100ms Interval	Uplink Broadcast Credit	Uplink Broadcast MIR	Uplink Broadcast MIR Type	Downlink MIR	Downlink Max Bucket Size	Downlink Max Burst MIR
2500000000	155000000	15500000	2500000000	0	0 (Not Limited)	0 (Not Limited)	0	0	kbps	155000000	2500000000	0 (Not Limited)

Attribute	Meaning
Current Uplink Bucket Size	This field displays the number of bits in the bucket to be potentially consumed at above-MIR rates, up to Max Burst MIR rate.
Uplink MIR	This field displays the active MIR rate per second. This is the rate that the bucket is filled with bits.
Uplink MIR Per 100ms Interval	This field displays the rate that the bucket is filled with bits at every 100 ms interval.
Uplink Max Bucket Size	This field displays the maximum bucket size, which is the maximum number of bits that can be in the bucket. The bucket fills at MIR rate and can hold this number of bits, which is a configuration value.
Current Max Burst Bucket Size	If Max Burst is enabled, there is a secondary "bucket" that controls the maximum rate of bit consumption. If Max Burst is not enabled (which means not limited), this will be 0 as the bucket is not used.
Uplink Max Burst MIR	This field displays the configured value of the Max Burst rate. This is the maximum rate at which bits can be consumed above MIR. Once excess (> MIR) bits have been consumed, the link will be throttled to MIR.
Uplink Max Burst MIR per 100ms Interval	This field displays the configured value of the Max Burst rate at every 100 ms interval.
Uplink Broadcast Credit	This field displays the broadcast credit.
Uplink Broadcast MIR	This field displays the broadcast MIR rate per second.
Uplink Broadcast MIR Type	This field displays the type of the broadcast MIR.
Downlink MIR	This field displays the active configured MIR rate per second. This is the rate that the bucket is filled with bits.
Downlink Max Bucket Size	This field displays the configured maximum bucket size, which is the maximum number of bits that can be in the bucket. The bucket fills at MIR rate and can hold this number of bits, which is a configuration value.
Downlink Max Burst MIR	This field displays the configured value of the Max Burst rate. This is the maximum rate at which bits can be consumed above MIR. Once excess (> MIR) bits have been consumed, the link will be throttled to MIR.

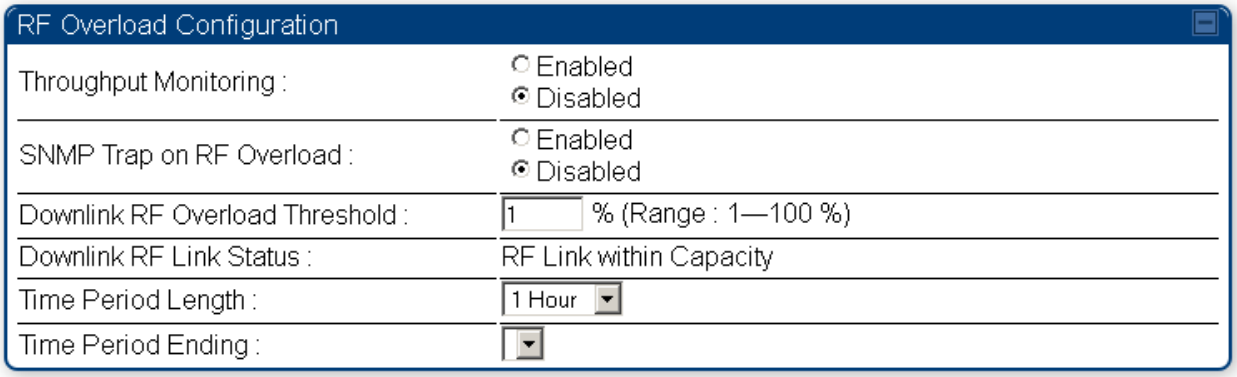
Interpreting Throughput statistics

The 450 Platform Family has a Statistics > Throughput page which shows historical information about sector or backhaul throughput and packet discards. This page is applicable for AP and BHM modules. This information can be useful to identify an overloaded sector or heavy bandwidth users. This page also shows the user throughput in terms of data rate (kbps) and packet rate (packets per second, or PPS), as well as the average packet size during the sample period.

Operators may set the AP/BHM to send an SNMP trap when it detects an RF overload condition based on a configurable threshold.

The following configuration parameters are available on the Throughput tab GUI pane and a radio reboot is not required when configuring these parameters:

Table 139: RF overload Configuration attributes – AP/BHM



Attribute	Meaning
Throughput Monitoring	This enables or disables the monitoring of sector throughput and packet discards. This parameter is disabled by default.
SNMP Trap on RF Overload	This enables or disables the sending of an SNMP trap when an AP/BHM overload condition is reached (based on Downlink RF Overload Threshold).
Downlink RF Overload Threshold	This parameter determines the overload threshold in percent of packets discarded that triggers the generation of an SNMP trap.
Downlink RF Link Status	This field displays the status of the capacity of the RF link.
Time Period Length Time Period Ending	These two configuration parameters determine what set of collection samples to show on the GUI display. The Time Period Length can be set from one to three hours. Time Period Ending allows the operator to set the end time for the set of collection samples to display.

Following configuration settings are three tables that display the statistics that are collected.

Board Performance statistics

This table contains a row that corresponds to each 1 minute statistics collection interval. Each row contains the following data aggregated for the entire AP/BHM:

- Ethernet Throughput - Statistics collected at the Ethernet port:
    - kbps in – average throughput over the collection interval in Kbps into the AP/BHM on the Ethernet Interface
    - kbps out – average throughput over the collection interval in Kbps out of the AP/BHM on the Ethernet Interface

    - PPS in – average packets per second over the collection interval into the AP/BHM on the Ethernet Interface
    - PPS out – average packets per second over the collection interval out of the AP/BHM on the Ethernet Interface
- RF Throughput - Statistics collected at the RF Interface:
    - kbps in – average throughput over the collection interval in Kbps into the AP/BHM on the RF Interface
    - kbps out – average throughput over the collection interval in Kbps out of the AP/BHM on the RF Interface
    - PPS in – average packets per second over the collection interval into the AP/BHM on the RF Interface
    - PPS out – average packets per second over the collection interval out of the AP/BHM on the RF Interface
- Aggregate Through Board – Sum of bidirectional data transferred through (not originating or terminating at) the AP/BHM:
    - kbps – average bidirectional throughput over the collection interval in Kbps
    - PPS – average bidirectional packets per second over the collection interval
    - Ave Pkt Size – Average Packet size over the collection interval of bidirectional data transferred

Board Throughput statistics

This table contains a row that corresponds to each one minute statistics collection interval. This table may be used to determine if there are problems with any of the interfaces. For example, if the Ethernet in packets is much higher than the RF out packets it could indicate a denial of service (DoS) attack on the AP/BHM. Each row contains the following data aggregated for the entire AP/BHM:

- Ethernet Statistics- Statistics collected at the Ethernet port:
    - inOctets – Number of octets (bytes) received by the AP/BHM at the Ethernet Interface over the collection interval
    - outOctets – Number of octets (bytes) sent by the AP/BHM at the Ethernet Interface over the collection interval
    - inPkts – Number of packets received by the AP/BHM at the Ethernet Interface over the collection interval
    - outPkts – Number of packets sent by the AP/BHM at the Ethernet Interface over the collection interval
    - Discards (in/out) – Number of packets that had to be discarded by the AP/BHM at the respective Ethernet Interface Queue

- RF Statistics - Statistics collected at the RF Interface:
    - inOctets – Number of octets (bytes) received by the AP/BHM at the RF Interface over the collection interval
    - outOctets – Number of octets (bytes) sent by the AP/BHM at the RF Interface over the collection interval
    - inPkts – Number of packets received by the AP/BHM at the RF Interface over the collection interval
    - outPkts – Number of packets sent by the AP/BHM at the RF Interface over the collection interval
    - Discards (in/out) – Number of packets that had to be discarded by the AP/BHM at the respective RF Interface Queue during the collection interval
    - Discards % (in/out) – Percent of the total packets received / transmitted that had to be discarded during the collection interval

LUID RF Throughput statistics

This table contains a row that corresponds to each active LUID served by the AP/BHM. Note that an LUID may be assigned 1 or 2 VCs. If the LUID is assigned 2 VCs, then the data in the table is the sum of the activity for both VCs. This table may be used to determine which LUIDs are experiencing overload so that corrective action can be taken (i.e. fixing a poor RF link or moving a heavily loaded link to a less congested AP/BHM). Each row contains counters and statistics related to the RF Interface that are updated once per minute:

- Inbound Statistics - Statistics collected at the RF Interface for the Uplink:
- octets – Number of octets (bytes) received by the AP/BHM at the RF Interface for this LUID over the collection interval
- pkts – Number of packets received by the AP/BHM at the RF Interface for this LUID over the collection interval
- Ave Pkt Size – Average size of the packets received by the AP/BHM at the RF Interface for this LUID over the collection interval
- discards – Number of packets received by the AP/BHM at the RF Interface for this LUID over the collection interval that had to be discarded because the RF In Queue was full
- discards % – Percent of the total packets received by the AP/BHM at the RF Interface for this LUID over the collection interval that had to be discarded because the RF In Queue was full
- Outbound Statistics - Statistics collected at the RF Interface for the Downlink:
- octets – Number of octets (bytes) transmitted by the AP/BHM at the RF Interface for this LUID over the collection interval
- pkts – Number of packets transmitted by the AP/BHM at the RF Interface for this LUID over the collection interval

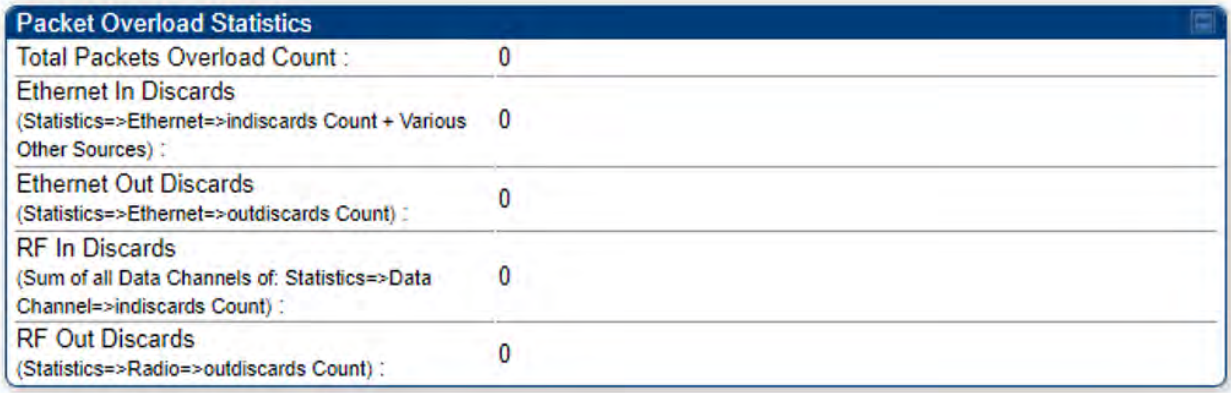
- Ave Pkt Size – Average size of the packets transmitted by the AP/BHM at the RF Interface for this LUID over the collection interval
- discards – Number of packets to be transmitted by the AP/BHM at the RF Interface for this LUID over the collection interval that had to be discarded because the RF Out Queue was full
- discards % – Percent of the total packets to be transmitted by the AP/BHM at the RF Interface for this LUID over the collection interval that had to be discarded because the RF Out Queue was full.

Interpreting Overload statistics

The Statistics > Overload page displays statistics on packet overload and resultant packet discards. Unlike the other fields, the Total Packets Overload Count is expressed in only this page. It is not a count of how many packets have been lost, but rather of how many discard events (packet loss bursts) have been detected due to overload condition.

This statistics page is applicable for all modules (AP/SM/BHM/BHS) and explained in below table.

Table 140: Overload page attributes – AP/SM/BHM/BHS



Packet Overload Statistics	
Total Packets Overload Count :	0
Ethernet In Discards (Statistics=>Ethernet=>indiscards Count + Various Other Sources) :	0
Ethernet Out Discards (Statistics=>Ethernet=>outdiscards Count) :	0
RF In Discards (Sum of all Data Channels of: Statistics=>Data Channel=>indiscards Count) :	0
RF Out Discards (Statistics=>Radio=>outdiscards Count) :	0

Attribute	Meaning
Total Packets Overload Count	This field represents the sum of all RF and Ethernet in/out discards.
Ethernet In Discards	This field represents the number of packets tossed due to the Ethernet queue being full. If a climb in this stat accompanies a climb in RF Out Discards stat, then most likely the board is at RF capacity either due to traffic exceeding the RF pipe, or interference temporarily limiting the RF throughput. If this stat climbs without the RF Out Discards stat climbing, then the radio is most likely PPS limited.
Ethernet Out Discards	This field represents the number of packets tossed due to an Ethernet out overload. This stat must not climb in normal operation because the Ethernet link is much higher capacity than the RF link. If this stat is incrementing, then either the Ethernet link is established at a low speed (i.e. 10Mbps – half duplex), or there is a problem with cabling/Ethernet hardware.

Attribute	Meaning
RF In Discards	This field indicates the number of packets tossed due to no resources available within the radio to process them. This stat also must not be increasing because the system is designed to shed packets on the RF Out interface. If this stat is incrementing the board, it is most likely congested due to high PPS rate in combination with an Ethernet Out problem, which limits packet flow off the device.
RF Out Discards	This field indicates the number of packets tossed due to RF link at capacity. This stat will increase whenever the RF link is at capacity. When the internal FPGA RF input queue overflows, this stat is incremented. If this stat is seen to be incrementing at the AP, then the sector is congested. If seen at the SM, the number of Contention Slots must be looked at to ensure that enough Contention Slots are allocated to allow for bandwidth requests to be seen at the AP.

Note

PMP 450m overload:

The 450m Series AP is designed to handle high load in terms of high throughput and high PPS. In terms of throughput, PMP 450m is designed to achieve 3x or more throughput improvement over PMP 450 and PMP 450i Series products. In terms of packets per second (PPS), PMP 450m is designed to handle more than 100k PPS.

Overload occurs when the offered load exceeds the above limits. When overload occurs, PMP 450m will start discarding packets and TCP throughput will degrade due to packet loss.

It's worth noting that Frame Utilization statistics (Statistics > Frame Utilization tab: Frame Utilization: Downlink and Uplink) are not necessarily indicative of overload condition. They show how much the TDD frame is utilized. High frame utilization depends on:

- High traffic during busy periods: those statistics will be close to 100% and almost all slots will be utilized. In this case if the Overload statistics show that packets are discarded then this is an indication of overload condition.
- High percentage of VCs with low modulation with moderate traffic. Those VCs will require more slots to service them (due to low modulation) and the frame utilization will be high. In this case the TDD frame is fully utilized but the system is at low capacity and is not in an overload condition.

PMP 450m has higher PPS than PMP 450 and PMP 450i and supports higher throughput through spatial multiplexing, therefore when a PMP 450m replaces an overloaded PMP 450 or PMP 450i AP the PMP 450m will not be overloaded under the same conditions but the frame utilization may still show close to 100%; this should not alarm the customer. The overload statistics shall be monitored on PMP 450m to see if it is overloaded or not.

Interpreting DHCP Relay statistics

The Statistics > DHCP Relay page displays requests and replies received, relayed and discarded when the AP is configured as a DHCP relay. Typically, in a working DHCP relay configuration a one-to-one ratio is established between requests and replies that are received and relayed. This statistics page is only applicable for PMP (AP and SM modules) and it is explained in below figure.

Figure 112: *DHCP Relay page attributes – AP/SM*

DHCP Relay Statistics	
Requests Received :	0
Requests Relayed :	0
Requests Discarded :	0
Replies Received :	0
Replies Relayed :	0
Replies Discarded :	0
Untrusted Message Discards :	0
Max Hop Exceeded Discards :	0
Invalid Relay Agent Address Discards :	0
Relay Info Exceeding Max Message Size (DHCP message relayed without Option 82) :	0

DHCP Relay Option 82 Data

Subscriber	LUID		Circuit ID $apmacbi$	Remote ID $smmacbi$	Vendor Specific ID $smvidbi$
			Binary Option 82 Data		
No Site Name	002	Binary	0a003ea0005b	0a003ebb016a	000000a106130401025858
		ASCII			XX

Attribute	Meaning
Requests Received	This field represents the number of DHCP relay requests received by the AP.
Requests Relayed	This field represents the number of DHCP relay requests relayed by the AP.
Requests Discarded	This field represents the number of DHCP relay requests discarded by the AP due to errors in the request.
Replies Received	This field represents the number of DHCP relay replies received by the AP.
Replies Relayed	This field represents the number of DHCP relay replies relayed by the AP.
Replies Discarded	This field represents the number of DHCP relay replies discarded by the AP due to errors in the reply.
Untrusted Message Discards	This field indicates messages that were discarded because the message already contained Option 82 information with no Relay Agent specified.
Max Hop Exceeded Discards	This field indicates messages that have been relayed too many times, exceeding the max hop count (16).

Attribute	Meaning
Invalid Relay Agent Address Discards	This field indicates messages that have been discarded because the message relay agent address is already in place (relay agent address does not equal address of the AP).
Relay Info Exceeding Max Message Size (DHCP message relayed without Option 82)	This field indicates DHCP messages too large to fit Option 82 data. These messages are sent on without Option 82 information.
Subscriber	See Device tab attributes
LUID	
Circuit ID	This field displays the option 82 data of the SM in binary and ASCII formats.
Remote ID	
Vendor Specific ID	

Interpreting Filter statistics

The Statistics > Filter page displays statistics on packets that have been filtered (dropped) due to the filters set on the Protocol Filtering page. The filter page of SM is explained in below table.

Table 141: Filter page attributes - SM

Packet Filter Statistics	
PPPoE Count :	0
All IPv4 Count :	0
All Other IPv4 Count :	0
SMB Count :	0
SNMP Count :	0
Bootp Client Count :	0
Bootp Server Count :	0
IPv4 Multicast Count :	0
All IPv6 Count :	0
All Other IPv6 Count :	0
IPv6 SMB Count :	0
IPv6 SNMP Count :	0
IPv6 Bootp Client Count :	0
IPv6 Bootp Server Count :	0
IPv6 Multicast Count :	0
ARP Count :	0
All Others Count :	0
User Defined Port1 Count :	0
User Defined Port2 Count :	0
User Defined Port3 Count :	0

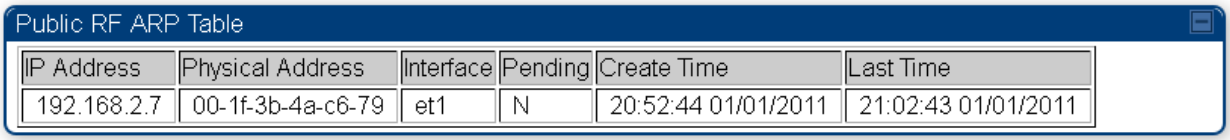
Attribute	Meaning
PPPoE Count	Number of PPPoE packets filtered.
All IPv4 Count	Number of IPv4 packets filtered.
All Other IPv4 Count	Any IPv4 message that was not SMB, SNMP, Bootp, Multicast or one of the user defined filters, that was filtered out.
SMB Count	Number of IPv4 Server Message Block (file sharing) packets filtered.

Attribute	Meaning
SNMP Count	Number of IPv4 SNMP packets filtered.
Bootp Client Count	Total number of IPv4 DHCP requests filtered.
Bootp Server Count	Total number of IPv4 DHCP replies filtered.
IPv4 Multicast Count	Number of IPv4 Multicast messages filtered.
All IPv6 Count	Number of IPv6 messages filtered.
All Other IPv6 Count	Any IPv6 message that was not SMB, SNMP, Bootp, Multicast or one of the user defined filters, that was filtered out.
IPv6 SMB Count	Number of IPv6 Server Message Block (file sharing) packets filtered
IPv6 SNMP Count	Number of IPv6 SNMP messages filtered
IPv6 Bootp Client Count	Total number of IPv6 DHCP replies filtered
IPv6 Bootp Server Count	Total number of IPv6 DHCP replies filtered
IPv6 Multicast Count	Number of IPv6 Multicast messages filtered
ARP Count	Total number of ARP packets filtered.
All other Count	The count of any messages that did not fit above that were filtered out
User Defined Port1 Count	Number of packets defined by the user port1 that were filtered.
User Defined Port2 Count	Number of packets defined by the user port2 that were filtered.
User Defined Port3 Count	Number of packets defined by the user port3 that were filtered.

Viewing ARP statistics

The Statistics > ARP page in a SM module correlated the IP address of the Ethernet-connected device to its MAC address and provides data about the connection.

Figure 113: *ARP page of the SM*

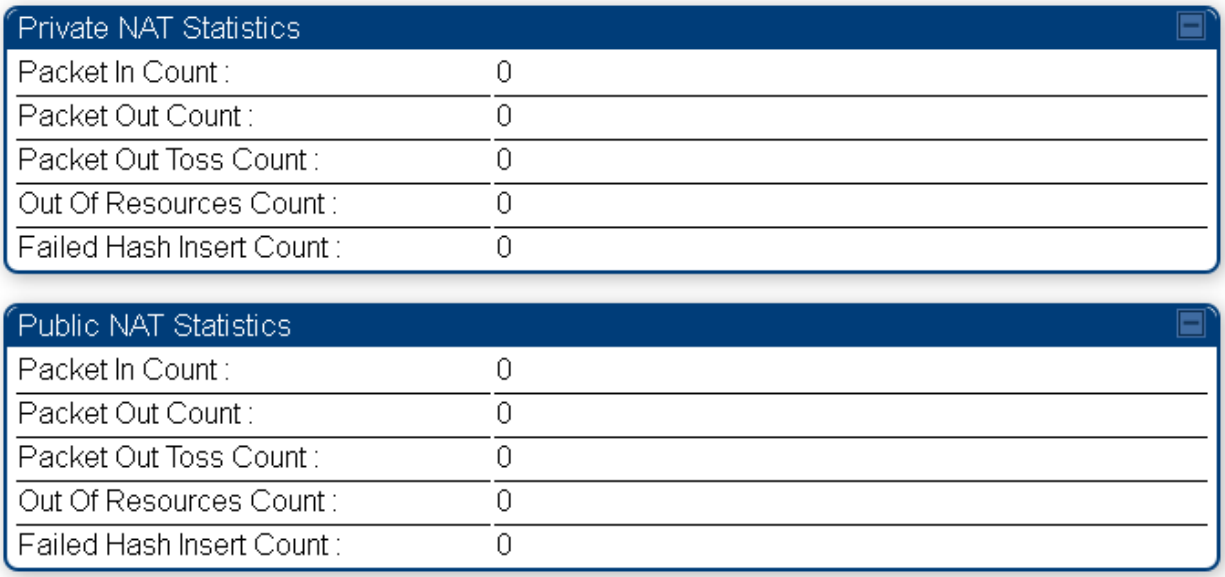

Public RF ARP Table

IP Address	Physical Address	Interface	Pending	Create Time	Last Time
192.168.2.7	00-1f-3b-4a-c6-79	et1	N	20:52:44 01/01/2011	21:02:43 01/01/2011

Viewing NAT statistics

When NAT is enabled on a SM, statistics are kept on the Public and Private (WAN and LAN) sides of the NAT and displayed on the **Statistics > NAT Stats** page. The NAT page of SM is explained in below table.

Table 142: NAT page attributes - SM



Private NAT Statistics	
Packet In Count :	0
Packet Out Count :	0
Packet Out Toss Count :	0
Out Of Resources Count :	0
Failed Hash Insert Count :	0

Public NAT Statistics	
Packet In Count :	0
Packet Out Count :	0
Packet Out Toss Count :	0
Out Of Resources Count :	0
Failed Hash Insert Count :	0

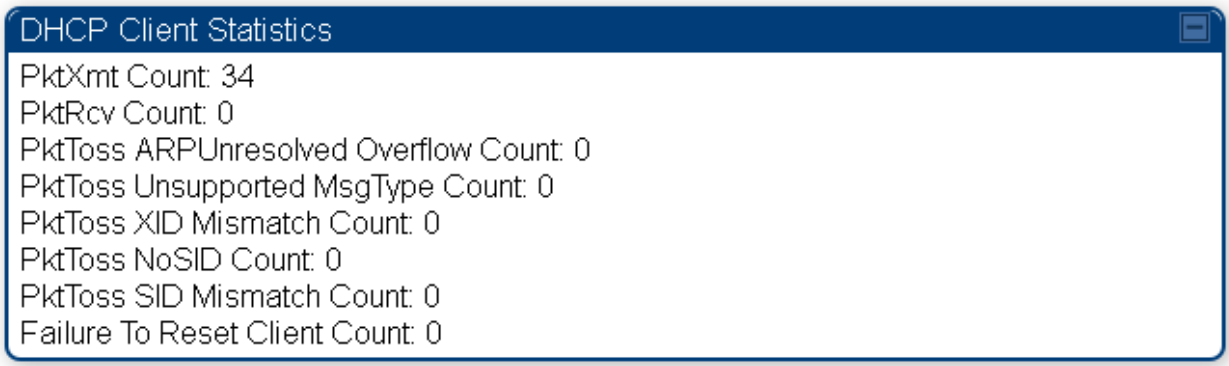
Attribute	Meaning
Private NAT Statistics, Packet In Count	This field represents the number of packets received on the SM's LAN/Ethernet interface
Private NAT Statistics, Packet Out Count	This field represents the number of packets sent from the SM's LAN/Ethernet interface
Private NAT Statistics, Packet Out Toss Count	This field represents the number of packets that we not sent from the SM's LAN/Ethernet interface due to addressing issues.
Private NAT Statistics, Out of Resources Count	This field represents the number of times the NAT table for the SM's LAN/Ethernet interfaces has been filled.
Private NAT Statistics, Failed Hash Insert Count	This field represents the number of times that the device failed to insert an address binding into the NAT hash table.
Public NAT Statistics, Packet In Count	This field represents the number of packets received on the SM's WAN/wireless interface
Public NAT Statistics, Packet Out Count	This field represents the number of packets sent from the SM's WAN/wireless interface
Public NAT Statistics, Out of Resources Count	This field represents the number of packets that we not sent from the SM's WAN/wireless interface due to addressing issues.
Public NAT Statistics, Failed Hash Insert Count	This field represents the number of times the NAT table for the SM's WAN/wireless interfaces has been filled.

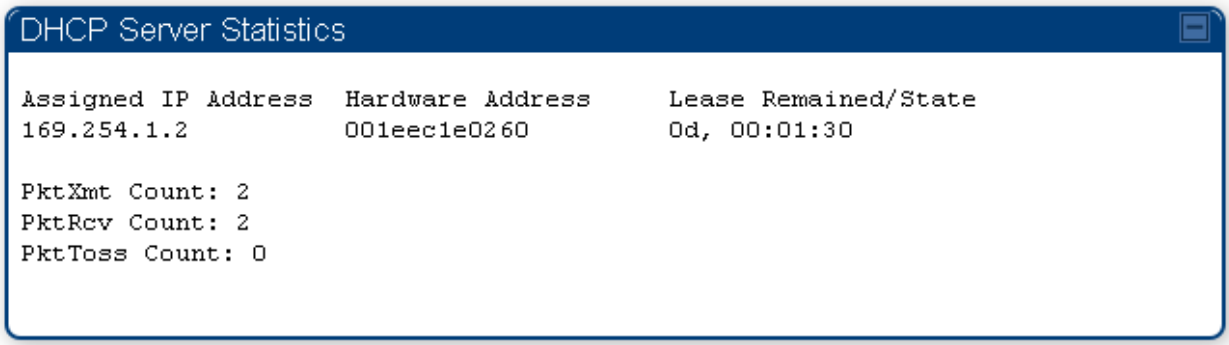
Viewing NAT DHCP Statistics

The Statistics > NAT DHCP page displays NAT enabled DHCP client statistics. This is statistics page is applicable for SM only.

When NAT is enabled on a SM with DHCP client (DHCP selected as the Connection Type of the WAN interface) and/or DHCP Server, statistics are kept for packets transmitted, received and tossed, as well as a table of lease information for the DHCP server (Assigned IP Address, Hardware Address and Lease Remained/State).

Table 143: NAT DHCP Statistics page attributes - SM





Attribute	Meaning
PktXmt Count	Represents the number of DHCP packets transmitted from the client
PktRcv Count	This field represents the number of DHCP packets received by the client
PktToss ARPUnresolved Overflow Count	This field represents the number of packets tossed due to failed attempts to resolve an IP address into a physical MAC address
PktToss Unsupported MsgType Count	This field represents the number of packets tossed due to the receipt of an unsupported message type (cannot be interpreted by DHCP client)
PktToss XID Mismatch Count	The field represents the number of packets that were tossed due to a transaction ID mismatch
PktToss NoSID Count	This field represents the number of packets that were tossed due to lack of a DHCP session ID

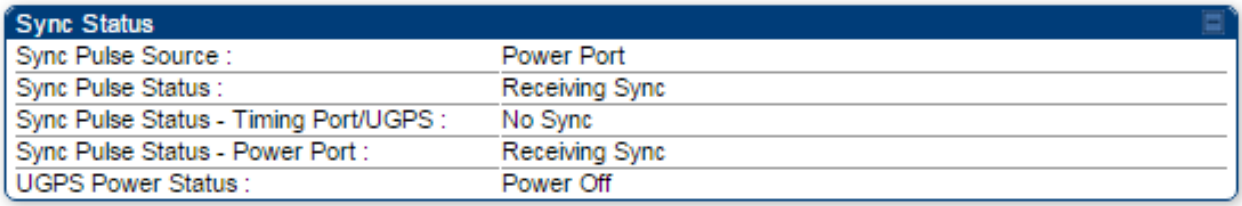
Attribute	Meaning
PktToss SID Mismatch Count	Represents the number of packets tossed due to a session ID mismatch
Failure to Reset Client Count	This field represents the number of times the DHCP client was unable to be reset (resulting in no IP address being served).

Interpreting Sync Status statistics

The Statistics > Sync Status page of AP is only displayed when the Sync Input is set to AutoSync or AutoSync+Free Run.

The Sync Status page is explained in below table.

Table 144: Sync Status page attributes - AP



Sync Status	
Sync Pulse Source :	Power Port
Sync Pulse Status :	Receiving Sync
Sync Pulse Status - Timing Port/UGPS :	No Sync
Sync Pulse Status - Power Port :	Receiving Sync
UGPS Power Status :	Power Off

Attribute	Meaning
Sync Pulse Source	This field indicates the status of the synchronization source: • Searching indicates that the unit is searching for a GPS fix • Timing Port/UGPS indicates that the module is receiving sync via the timing AUX/SYNC timing port • Power Port indicates that the module is receiving sync via the power port (Ethernet port).
Sync Pulse Status	This field indicates synchronization source pulse status.
Sync Pulse Status - Timing Port/UGPS	This field indicates synchronization pulse status over Timing Port/UGPS port.
Sync Pulse Status - Power Port	This field indicates synchronization pulse status over power port.
UGPS Power Status	This field indicates UGPS power up status (on or off).

This information may be helpful in a decision of whether to climb a tower to diagnose a perceived antenna problem.

Interpreting PPPoE Statistics for Customer Activities

The page can be access under Statistics > PPPoE of SM GUI.

When the PPPoE feature is enabled on the SM, PPPoE statistics provide data about activities of the customer.

The PPPoE Statistics of SM is explained in below table.

Table 145: PPPoE Statistics page attributes - SM

PPPoE Statistics	
IP address :	0.0.0.0
PPPoE Session Status :	Connecting
PPPoE AC Name :	
PPPoE Service Name :	
PPPoE Session ID :	0
PPPoE Session Uptime :	00:00:00
PPPoE Session Idle Time :	00:00:00
PPPoE Session MTU :	0
Primary DNS Address :	0.0.0.0
Secondary DNS Address :	0.0.0.0
PPPoE Control Bytes Sent :	168
PPPoE Control Bytes Received :	0
PPPoE Data Session Bytes Sent :	0
PPPoE Data Session Bytes Received :	0

Attribute	Meaning
IP address	This field displays the IP address of the PPPoE session initiator (situated below the SM)
PPPoE Session Status	This field displays the operational status of the PPPoE Session
PPPoE AC Name	This field displays access concentrator name used in the PPPoE session
PPPoE Service Name	This field displays the PPPoE service name associated with the PPPoE server in use
PPPoE Session ID	This field displays the current PPPoE session ID
PPPoE Session Uptime	This field displays the total session uptime for the PPPoE session
PPPoE Session Idle Time	This field displays the total idle time for the PPPoE session
PPPoE Session MTU	This field displays Maximum Transmission Unit configured for the PPPoE session
Primary DNS Address	This field displays the primary DNS server used by the PPPoE session
Secondary DNS Address	This field displays the secondary DNS server used by the PPPoE session
PPPoE Control Bytes Sent	Displays the total number of PPPoE session control bytes sent from SM
PPPoE Control Bytes Received	This field displays the total number of PPPoE session control bytes received by the SM
PPPoE Data Session Bytes Sent	This field displays the total number of PPPoE data session (non-control/non-session management user data) sent by the SM
PPPoE Data Session Bytes Received	This field displays the total number of PPPoE data session (non-control/non-session management user data)

Interpreting Bridge Control Block statistics

The Statistics > Bridge Control Block page displays statistics of Bridge FEC, Bridge ratio and Bridge error. The page is applicable for all modules (AP/SM/BHM/BHS). The Bridge Control Block Statistics page is explained in below table.

Table 146: Bridge Control Block page attributes – AP/SM/BHM/BHS

Bridge FEC Stats	
FEC bin :	437
FEC bout :	24
FEC btoss :	0
FEC btosscap :	0
FEC uin :	3915
FEC uout :	5745
FEC utoss :	0
FEC utosscap :	0

Bridge Eth Aux Stats	
Eth Aux bin :	0
Eth Aux bout :	0
Eth Aux btoss :	0
Eth Aux btosscap :	0
Eth Aux uin :	0
Eth Aux uout :	0
Eth Aux utoss :	0
Eth Aux utosscap :	0

Bridge Radio Stats	
RF bin :	3
RF bout :	441
RF unknown ucast floods :	0
RF btoss :	0
RF btosscap :	0
RF uin :	331
RF uout :	9
RF utoss :	0
RF utosscap :	0

Bridge Error Stats	
ErrNI1QSend :	0
ErrNI2QSend :	0
ErrBridgeFull :	0
ErrSendMsg :	0
ErrApFecQSend :	0
ErrApRfQSend :	0

Attribute	Meaning
Bridge FEC Stats	
FEC bin	This field indicates the number of broadcast packets received by the bridge control block on the Main Ethernet interface
FEC bout	This field indicates the number of broadcast packets sent by the bridge control block on the Main Ethernet interface
FEC btoss	This field indicates the number of broadcast packets tossed out by the bridge control block on the Main Ethernet interface

Attribute	Meaning
FEC btosscap	This field indicates the number of broadcast packets tossed out at the Main Ethernet interface due to MIR cap being exceeded.
FEC uin	This field indicates the number of unicast packets received by the bridge control block on the Main Ethernet interface
FEC uout	This field indicates the number of unicast packets sent by the bridge control block on the Main Ethernet interface
FEC utoss	This field indicates the number of unicast packets tossed by the bridge control block on the Main Ethernet interface
FEC utosscap	This field indicates the number of unicast packets tossed out at the Main Ethernet interface due to MIR cap being exceeded.
Bridge Eth Aux Stats	
FEC bin	This field indicates the number of broadcast packets received by the bridge control block on the Aux Ethernet interface
FEC bout	This field indicates the number of broadcast packets sent by the bridge control block on the Aux Ethernet interface
FEC btoss	This field indicates the number of broadcast packets tossed out by the bridge control block on the Aux Ethernet interface
FEC btosscap	This field indicates the number of broadcast packets tossed out at the Aux Ethernet interface due to MIR cap being exceeded.
FEC uin	This field indicates the number of unicast packets received by the bridge control block on the Aux Ethernet interface
FEC uout	This field indicates the number of unicast packets sent by the bridge control block on the Aux Ethernet interface
FEC utoss	This field indicates the number of unicast packets tossed by the bridge control block on the Aux Ethernet interface
FEC utosscap	This field indicates the number of unicast packets tossed out at the Aux Ethernet interface due to MIR cap being exceeded.
Bridge Radio Stats	
RF bin	This field indicates the number of broadcast packets received by the bridge control block on the radio interface
RF bout	This field indicates the number of broadcast packets sent by the bridge control block on the radio interface
RF btoss	This field indicates the number of broadcast packets tossed by the bridge control block on the radio interface
RF btosscap	This field indicates the number of broadcast packets tossed out at the radio interface due to MIR cap being exceeded.