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 on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 Configuration Source on page 7-72
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 on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 • Configuration Source on page 7-72
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 on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 Configuration Source on page 7-72
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 on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 • Configuration Source on page 7-72
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.

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.
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.
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	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

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.

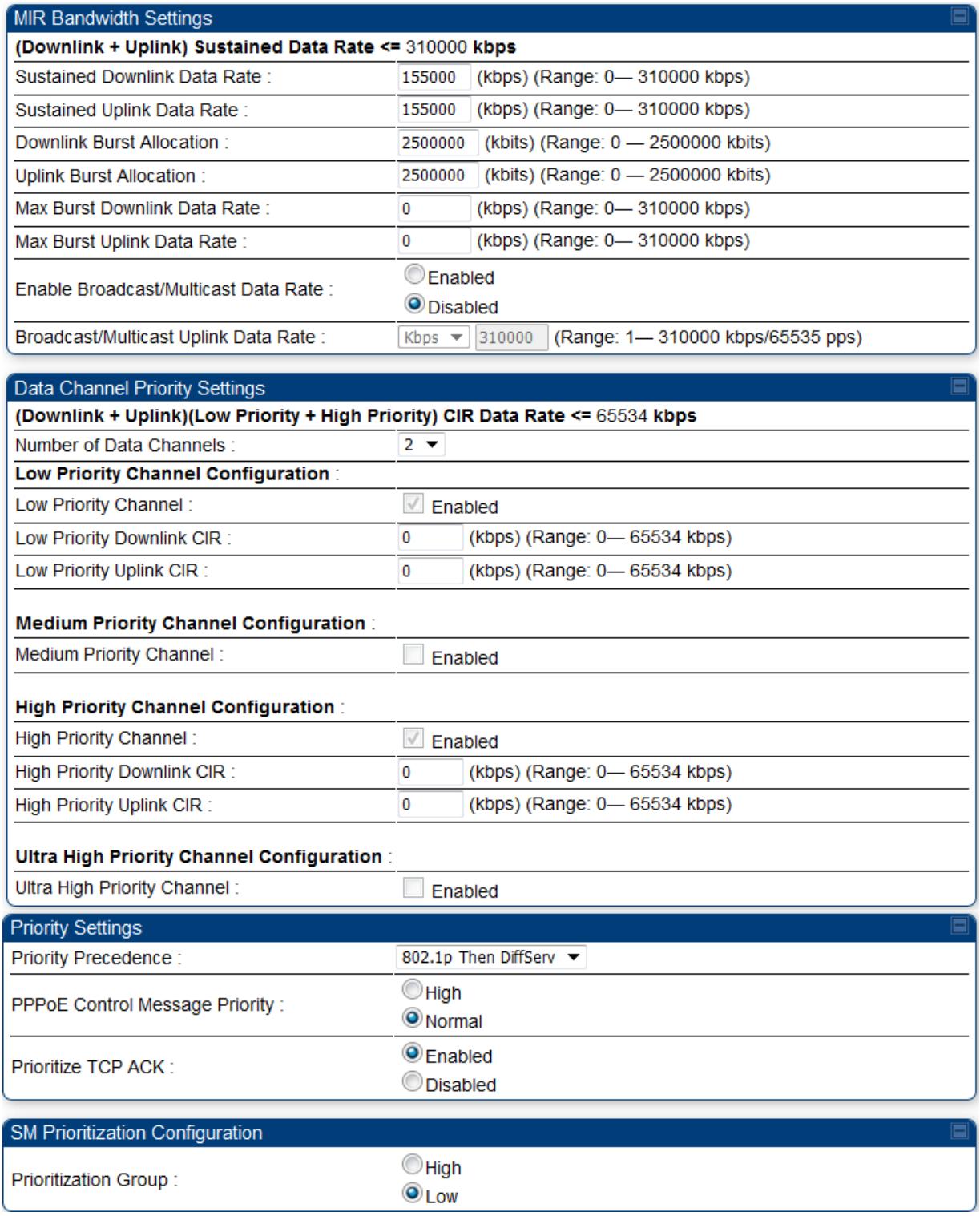
Data Channel Allocation - Low Priority	This parameter allows to configure the percentage of frame space allocated for low priority QoS level.

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.

Quality of Service (QoS) page of SM

The QoS page of SM is explained in Table 192.

Table 192 QoS page attributes - SM



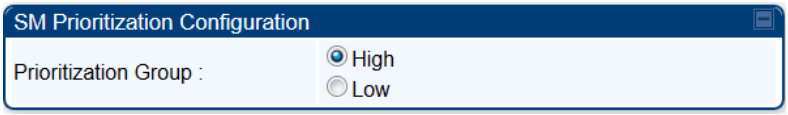
Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 • Configuration Source on page 7-72
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 on Page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 • Configuration Source on page 7-72
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 on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 Configuration Source on page 7-72
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 on page 7-228 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-230 • Configuration Source on page 7-72
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) on page 7-229 • Setting the Configuration Source on page 7-237
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) on page 7-229 • Setting the Configuration Source on page 7-237
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) on page 7-229 • Setting the Configuration Source on page 7-237
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) on page 7-229 • Setting the Configuration Source on page 7-237
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. See • SM Prioritization

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 Figure 161.

Figure 161 SM Prioritization on SM



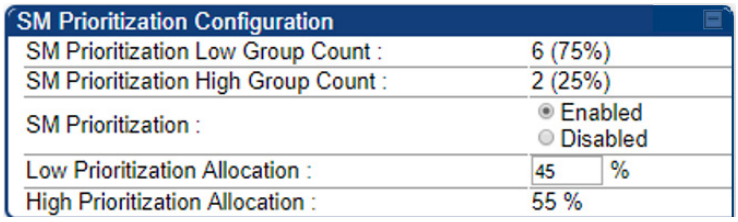
The feature does not take effect, however, until SM Prioritization is enabled on the AP, because the scheduler runs on the AP. Prioritization Allocation percentages per group are configured on the AP to determine how many timeslot resources are dedicated to each priority group.

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 Figure 162.

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 162 SM Prioritization on AP



In the example shown in Figure 162, 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 Figure 162, 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)

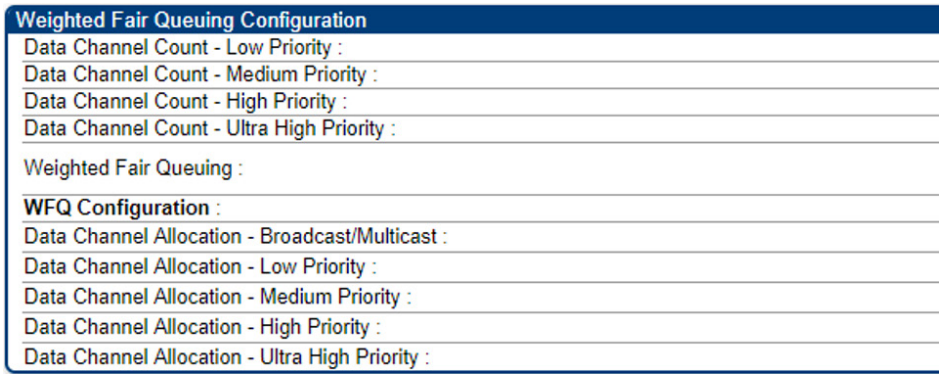
This feature lets the user assign a percentage of air interface resources to each of the Data Channel levels. The WFQ apply both to the DL and the UL. Note that there is no BC/MC traffic in the UL direction.

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.

Figure 163 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 163 Weighted Fair Queuing Configuration



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

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.

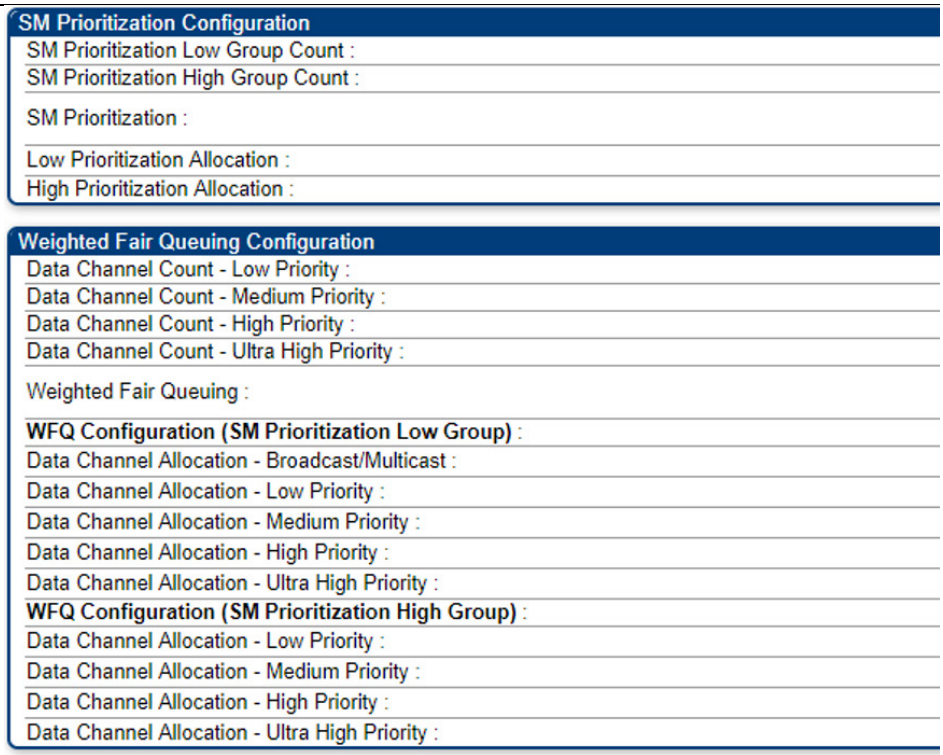
Using the example configuration show in Figure 163, there are 8 high priority Data channels. If 5 of those 8 Data channels have a CIR configured, then the Cambium scheduler will prioritize traffic on those 5 Data channels up to their CIR limits, for those 26% of the timeslots allocated to that QoS level. 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

Figure 164 shows a WFQ configuration with the SM Prioritization feature also enabled.

Figure 164 WFQ with SM Prioritization



In the example shown in Figure 164, 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 Figure 164, 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).

- High-priority Bandwidth on page 7-230
- Configuration Source on page 7-72

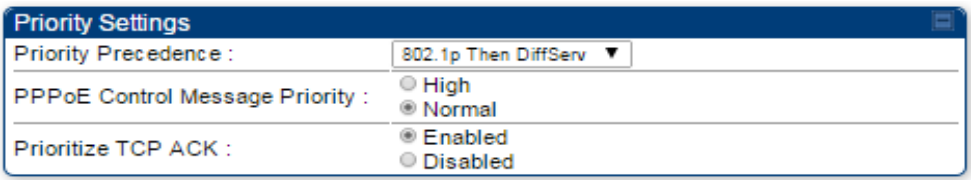
High Priority Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-229 • Setting the Configuration Source on page 7-237

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) on page 7-229 • Setting the Configuration Source on page 7-237
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 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.

Quality of Service (QoS) page of BHM

The QoS page of BHM is explained in Table 193.

Table 193 QoS page attributes - BHM



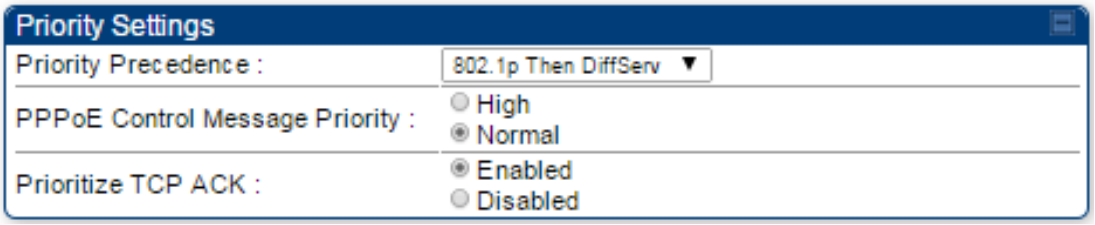
Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHM to utilize the high priority channel for PPPoE control messages. Configuring the BHM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. 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**.

Quality of Service (QoS) page of BHS

The QoS page of BHS is explained in Table 194.

Table 194 QoS page attributes - BHS

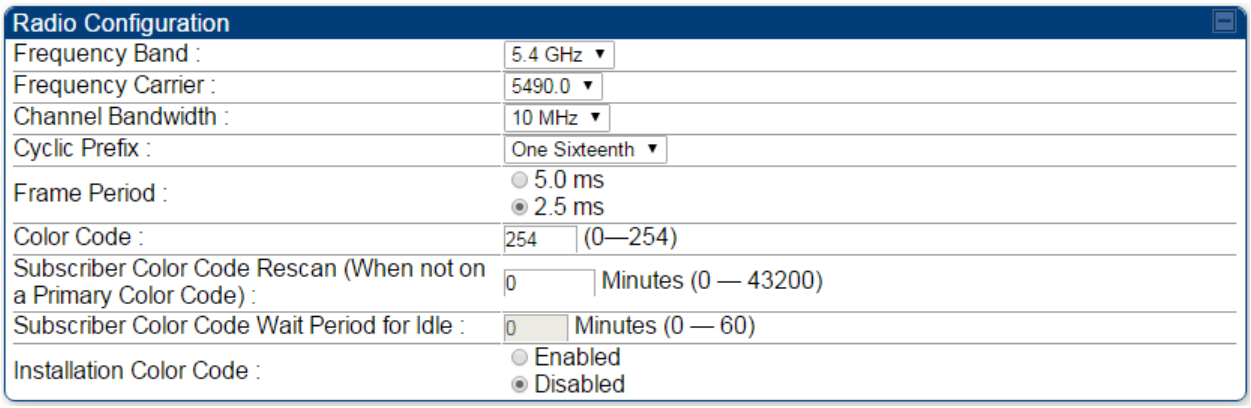


Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHS to utilize the high priority channel for PPPoE control messages. Configuring the BHS in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. 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**.

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 165 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 on page 7-258.

Configuration Steps

Procedure 23 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.

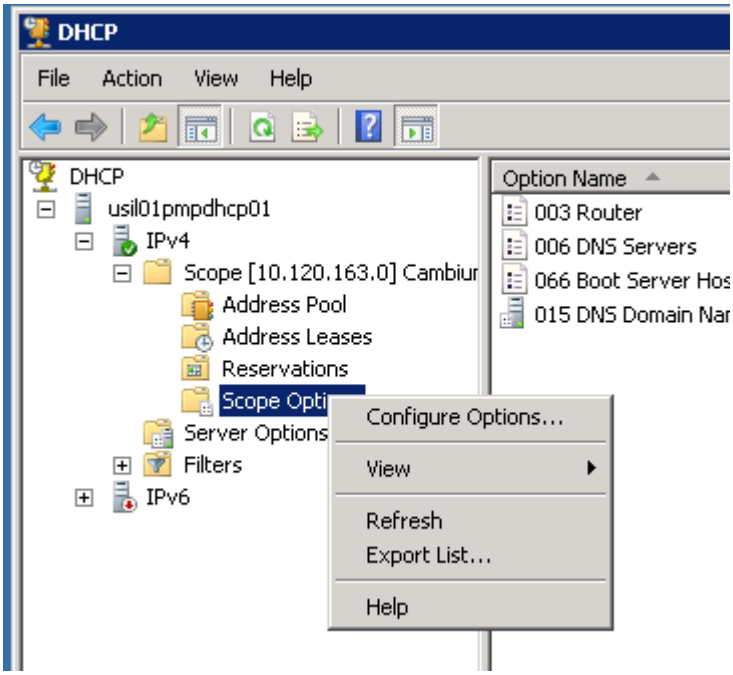
DHCP server configuration

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

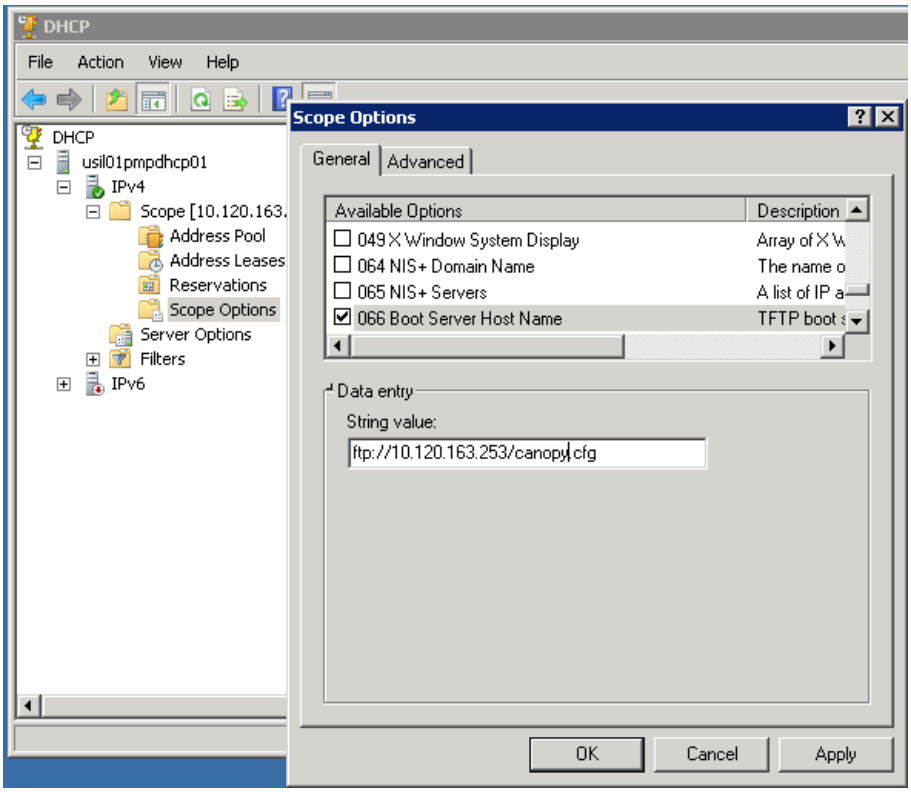
The following example explains how to make the change for Windows Server 2008. Adapt it to your specific DHCP server.

Procedure 24 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.

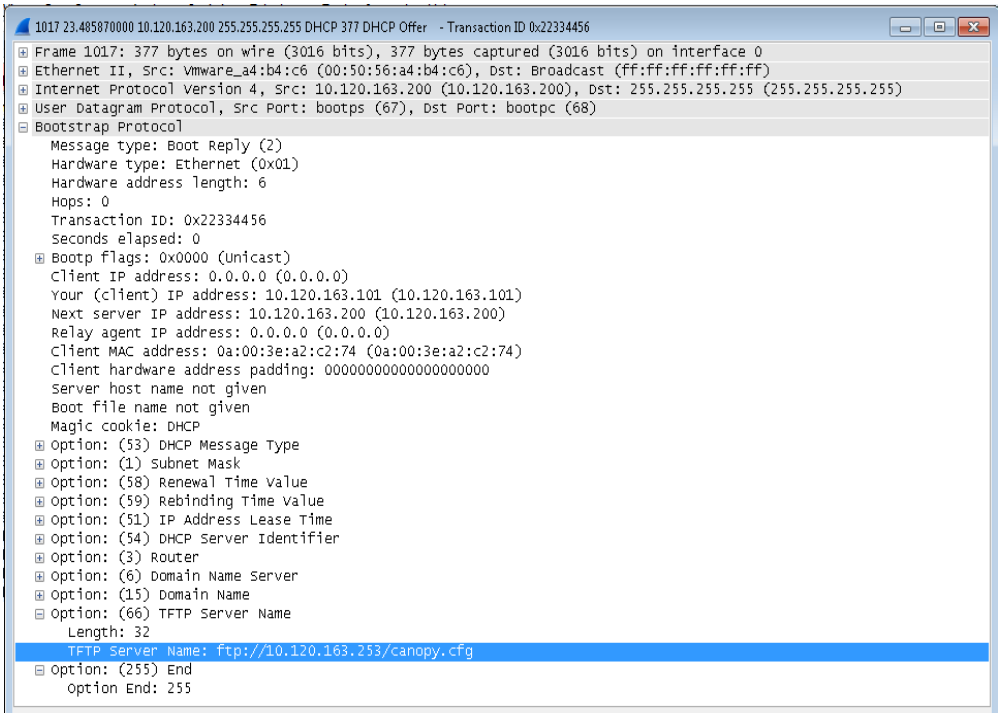
For example:

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.



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.

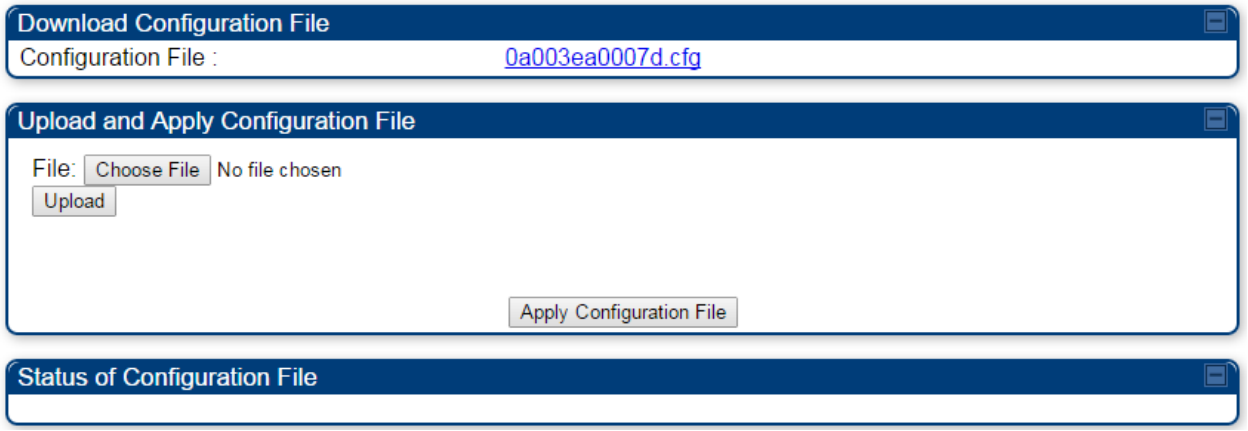
The exported configuration file contains the complete configuration including all the default values. To keep a backup of the current configuration, the file can be saved as-is and imported later.

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 (Refer Special Headers for configuration file on page 7-264).

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 166 Configuration File upload and download page



The DHCP server configuration procedure is as follows:

Procedure 25 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 26 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 27 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 "r**ebootIfRequired**" 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.

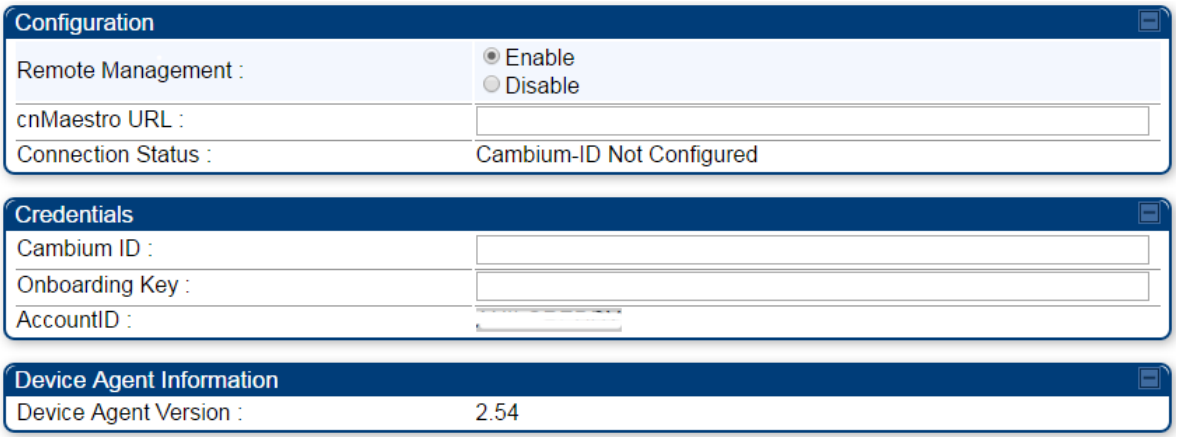
Onboarding

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 Table 195.

Table 195 Configuring cnMaestro



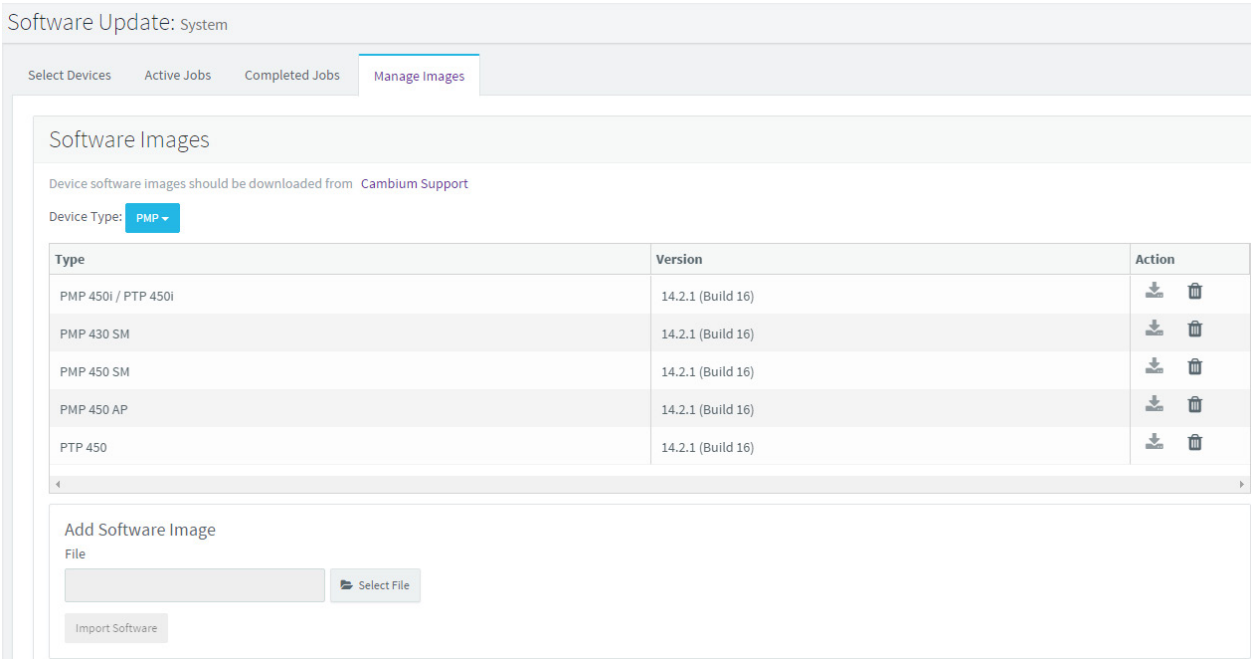
Attribute	Meaning
Remote Management	This field enables/disables remote management of 450 Platform Family products.
cnMaestro URL	This field allows to enter cnMaestro URL e.g. https://cloud.cambiumnetworks.com Or cnMaestro on premises URL
Connection Status	This field indicates cnMaestro connectivity status.
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™

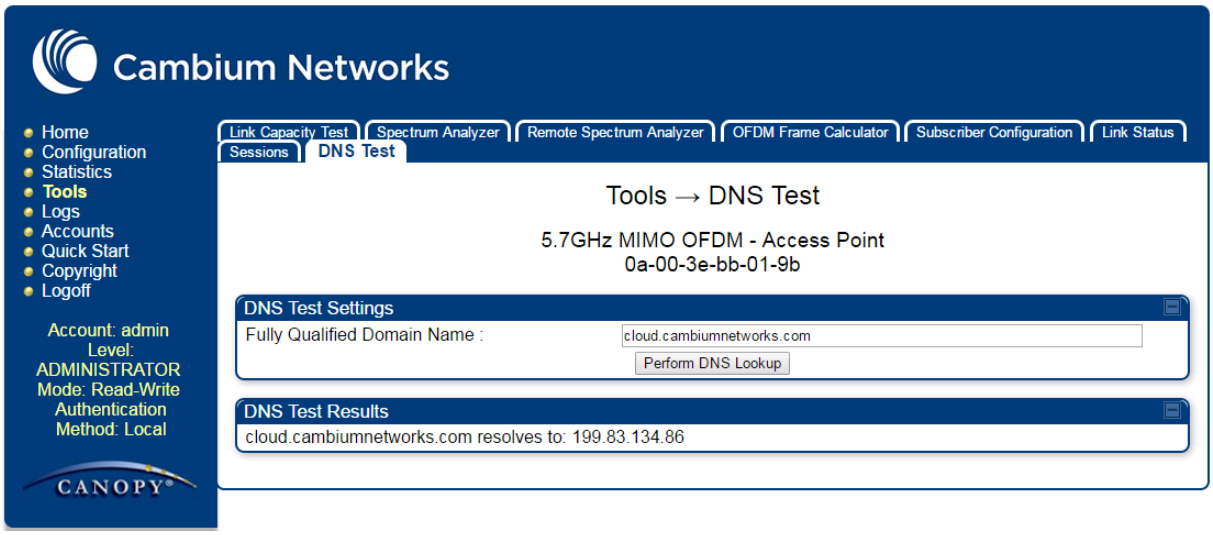
- Devices types must be PMP 450m Series, PMP/PTP 450 Series, PMP/PTP 450i/450b Series or PMP 430 Series SMs (interoperability mode only).
- Minimum required software version of 14.2.1. Device software images can be downloaded from http://support.cambiumnetworks.com or from the On Premises cnMaestro server 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 Figure 167.

Figure 167 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 Figure 168.

Figure 168 DNS Test for cnMaestro™ connectivity



- If the SM is in Bridge mode, then LAN1 must have public 7-267equest7-267ility 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

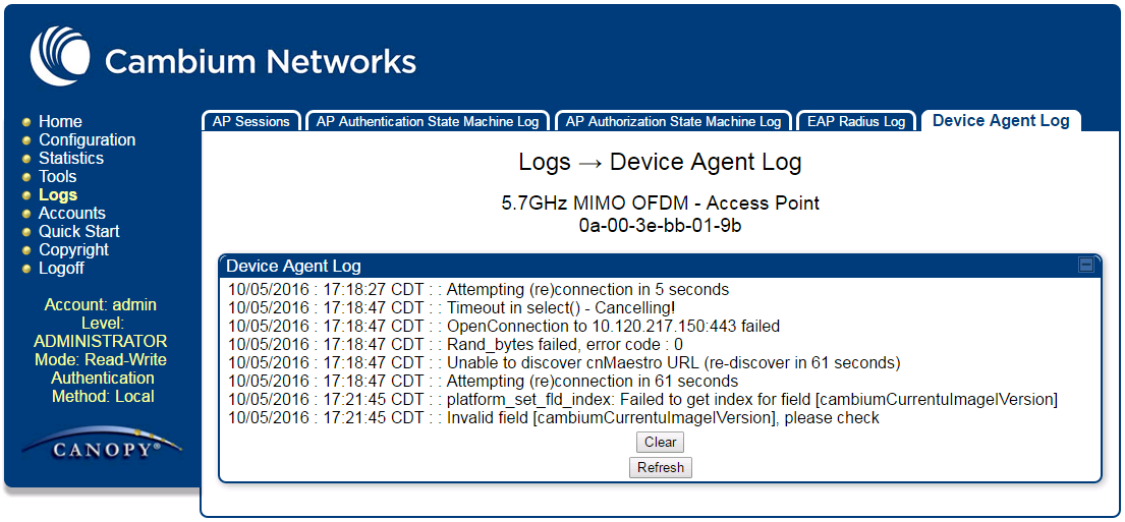
The device discovery order is as follows in On Permises cnMaestro™ Server. If any of the options is not configured, the discovery method will fallback to the next option:

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 Figure 169. 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 169 Device Agent Logs

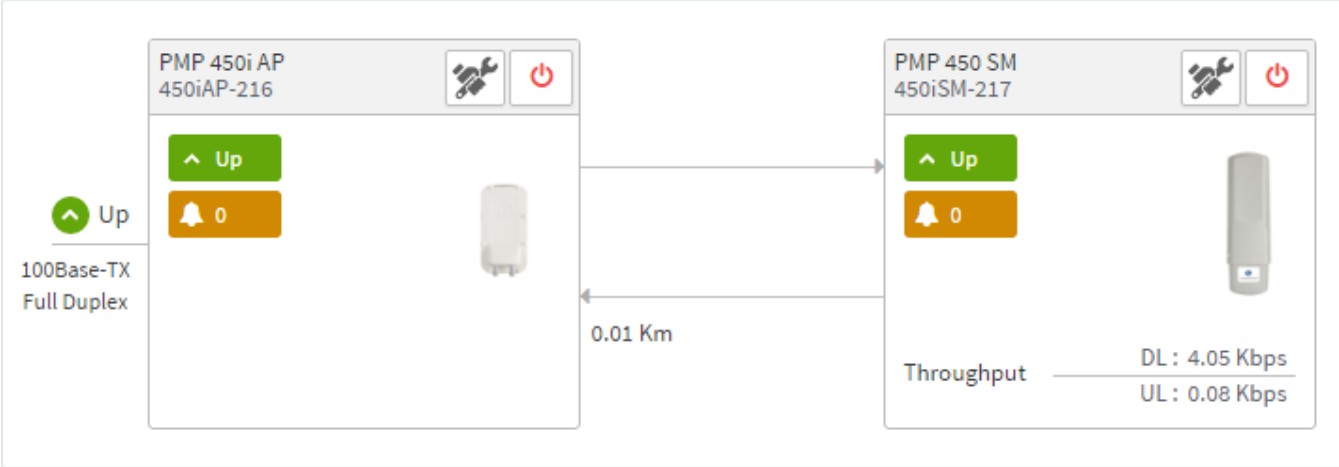


Monitoring Tools for PMP Devices on cnMaestro™

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 170 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

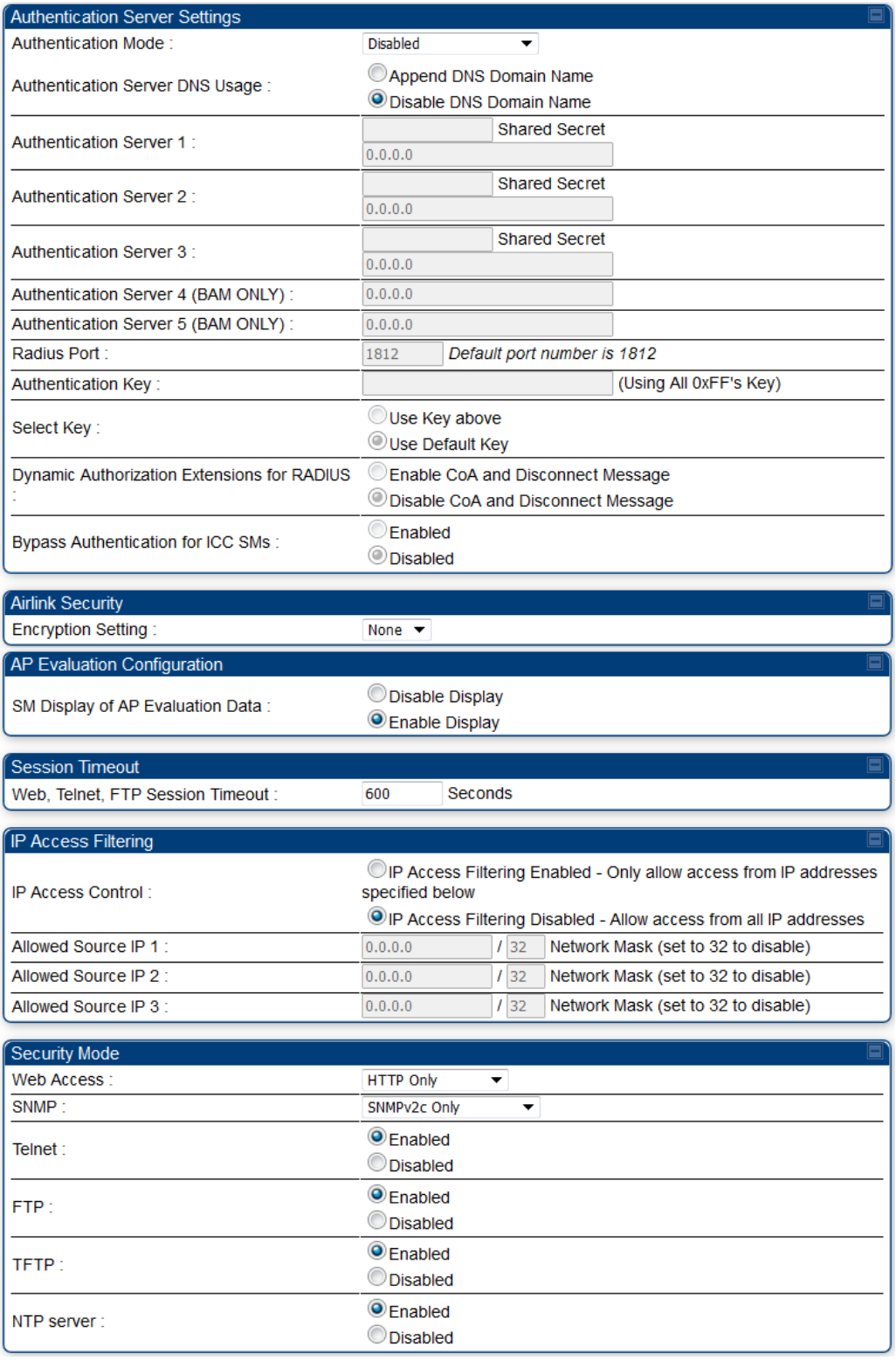
On the AP's **Configuration > Security** tab, select the **RADIUS AAA Authentication Mode**. The following describes the other **Authentication Mode** options for reference, and then the **RADIUS AAA** option.

- **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).

Table 196 Security tab attributes



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: **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 **Error! Hyperlink reference not valid.**IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https1://<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 communication version. It can be selected from drop-down list : • **SNMPv2c Only** – Enables SNMP v2 community 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

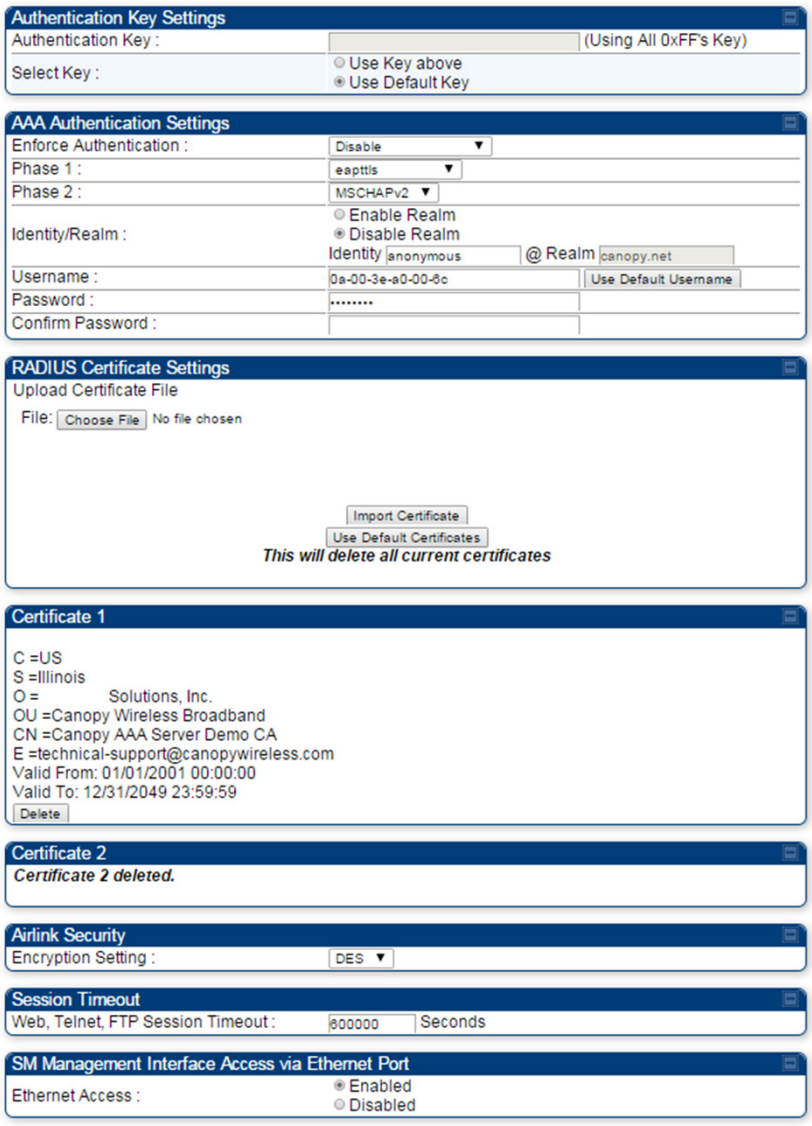
If it is desired that a SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set **Enforce Authentication** to **AAA**. With this enabled, SM does not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected.

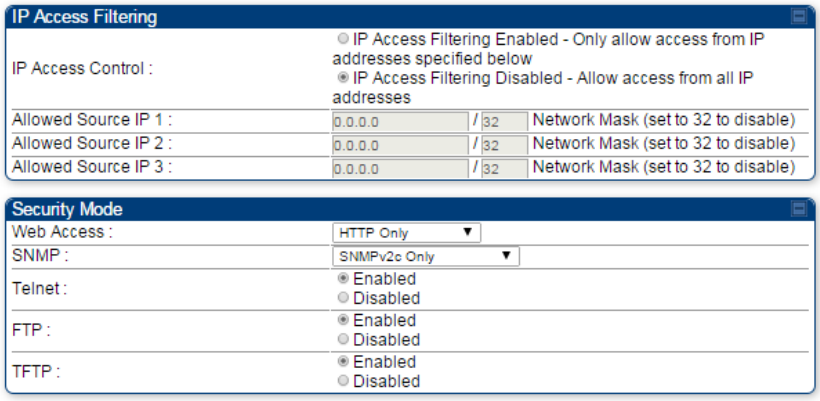
If it is desired that a SM use the authentication method configured on the AP it is registering to, set **Enforce Authentication** to **Disabled.** With **Enforce Authentication** disabled, a SM will attempt to register using whichever **Authentication Mode** is configured on the AP it is attempting 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 197 SM Security tab attributes





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 Confirm 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.
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
Allowed Source IP 1 Allowed Source IP 2 Allowed Source IP 3	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.
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 **Error! Hyperlink reference not valid.**IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via **Error! Hyperlink reference not valid.**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 communication version. It can be selected from drop-down list :

	• **SNMPv2c Only** – Enables SNMP v2 community 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.

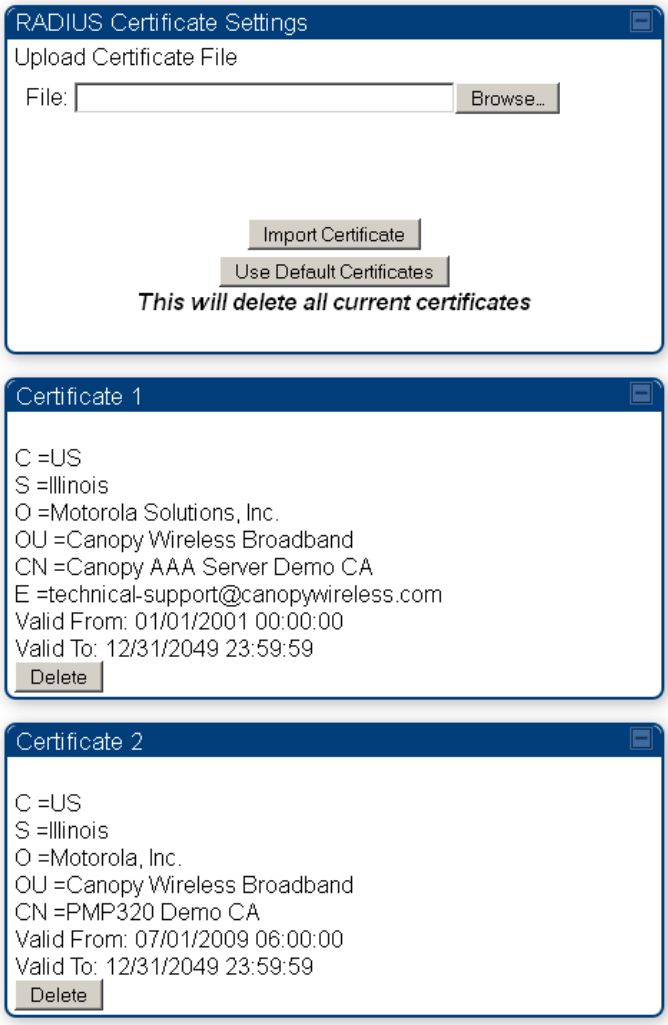
When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used.

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 171 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 Table 198. 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 Table 198).

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 Table 198). 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 198 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Required	Value	
MS-MPPE-Send-Key*	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key*	26.311.17	-	Y	-	
-				-	-
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 Uplink 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
26.161.6		integer	N	0-100000 kbps	

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
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-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Cambium-Canopy-DHCP-State	26.161.31	integer	N	1-Enable	
Configuration > IP > DHCP state				1	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-UserMode	26.161.51	integer	N	1=Read-Only 0=Read-Write	
Account > Add User > User Mode				0	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 Table 198 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 28 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 29 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

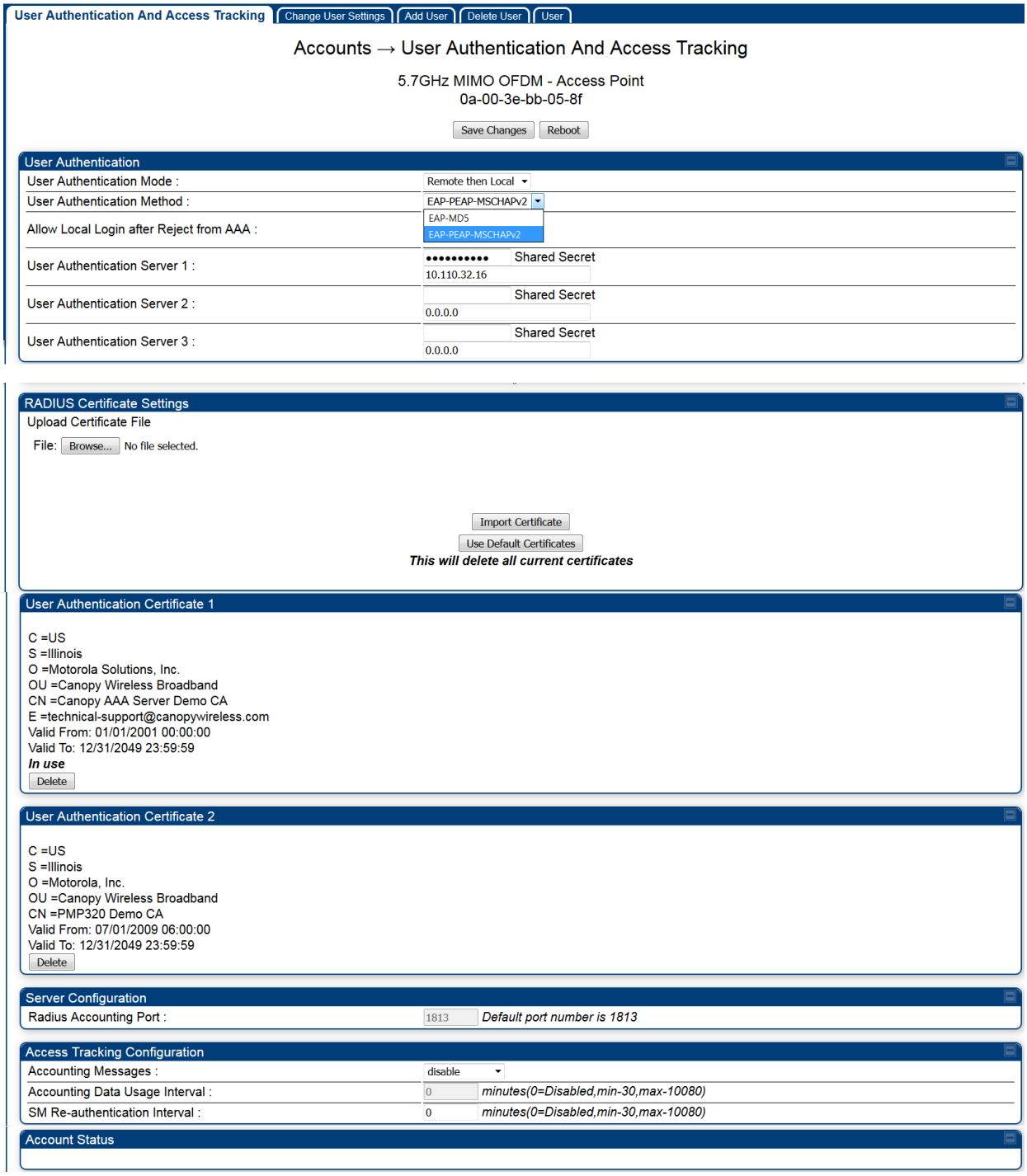
User Authentication Server 2

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.

Table 199 AP 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. deviceAccess – accounting messages regarding device access are sent to the RADIUS server (see Table 201). dataUsage – accounting messages regarding data usage are sent to the RADIUS server (see Table 201). 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 7-290 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 172 User Authentication and Access Tracking tab of the SM

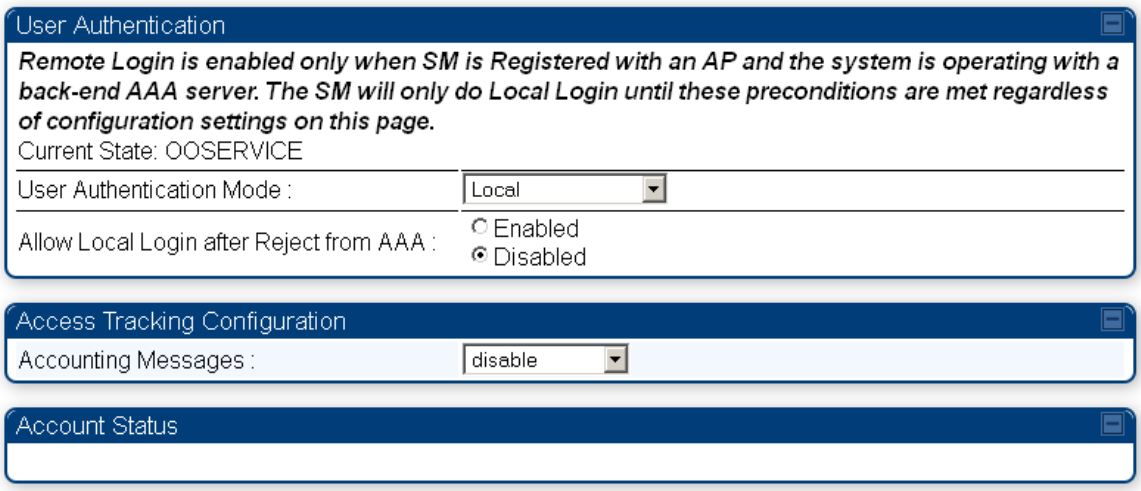
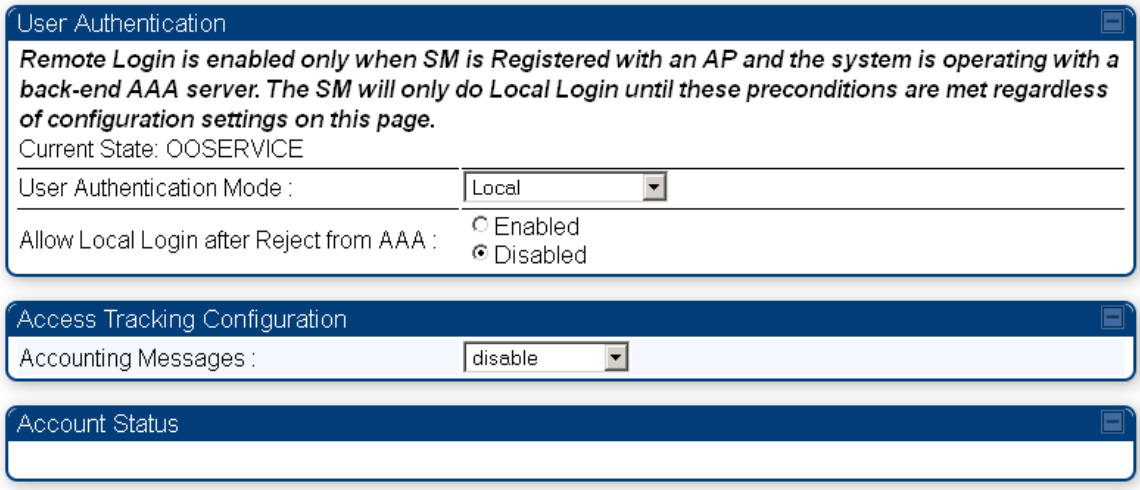


Table 200 SM User Authentication and Access Tracking attributes



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 • deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 201).

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 201 Device data accounting RADIUS attributes

Sender	Message	Attribute	Value	Description
AP		Acct-Status-Type	1 - Start	

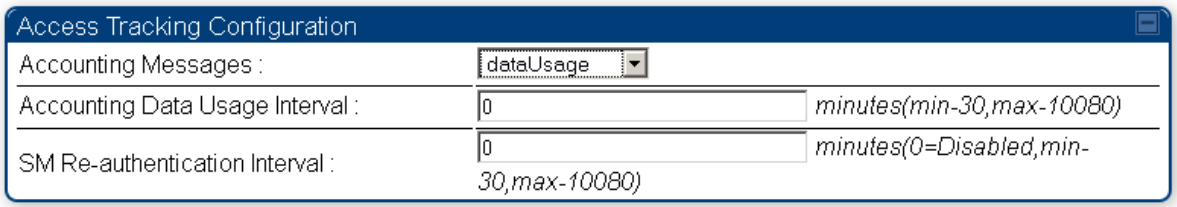
Sender	Message	Attribute	Value	Description
	Accounting-Request	Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	This message is sent every time a SM registers with an AP, and after the SM stats are cleared.
		Event-Timestamp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

Sender	Message	Attribute	Value	Description
		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	
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.	

Sender	Message	Attribute	Value	Description
		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 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 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 173 RADIUS accounting messages configuration



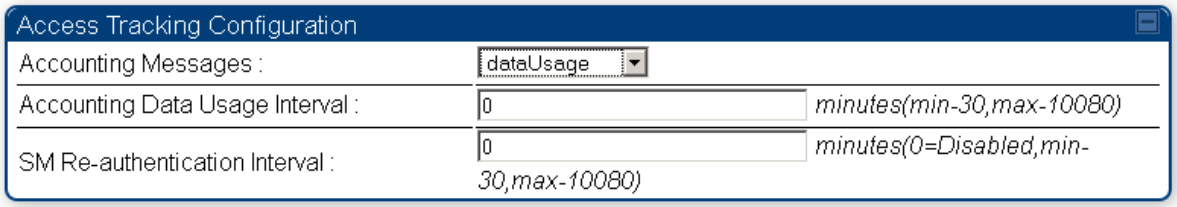
The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify 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 174 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:

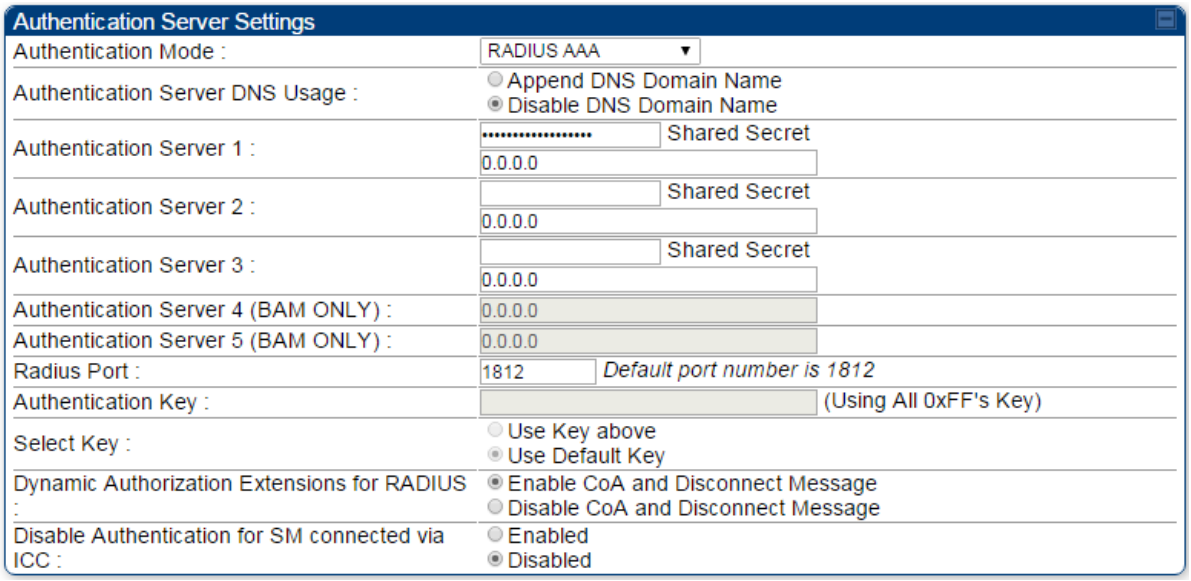
- **Success**: The SM continues normal operation
- **Reject**: The SM de-registers and will attempt network entry again after 1 minute and then if rejected will attempt re-entry every 15 minutes
- **Timeout or other error**: The SM remains in session and attempt 5 times to re-authenticate with the RADIUS-REQUEST 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 175 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.

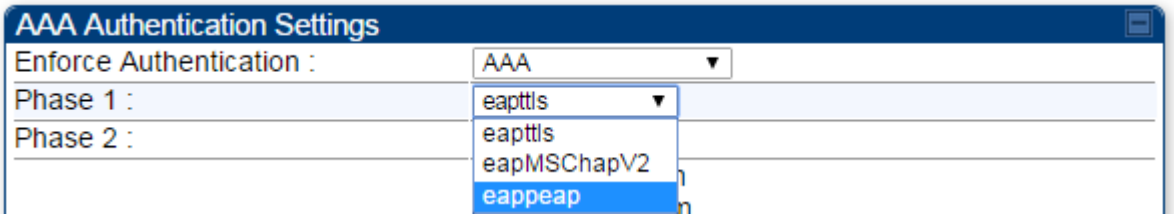
This feature is not supported on hardware board type P9 or lower platforms.

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 176 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.

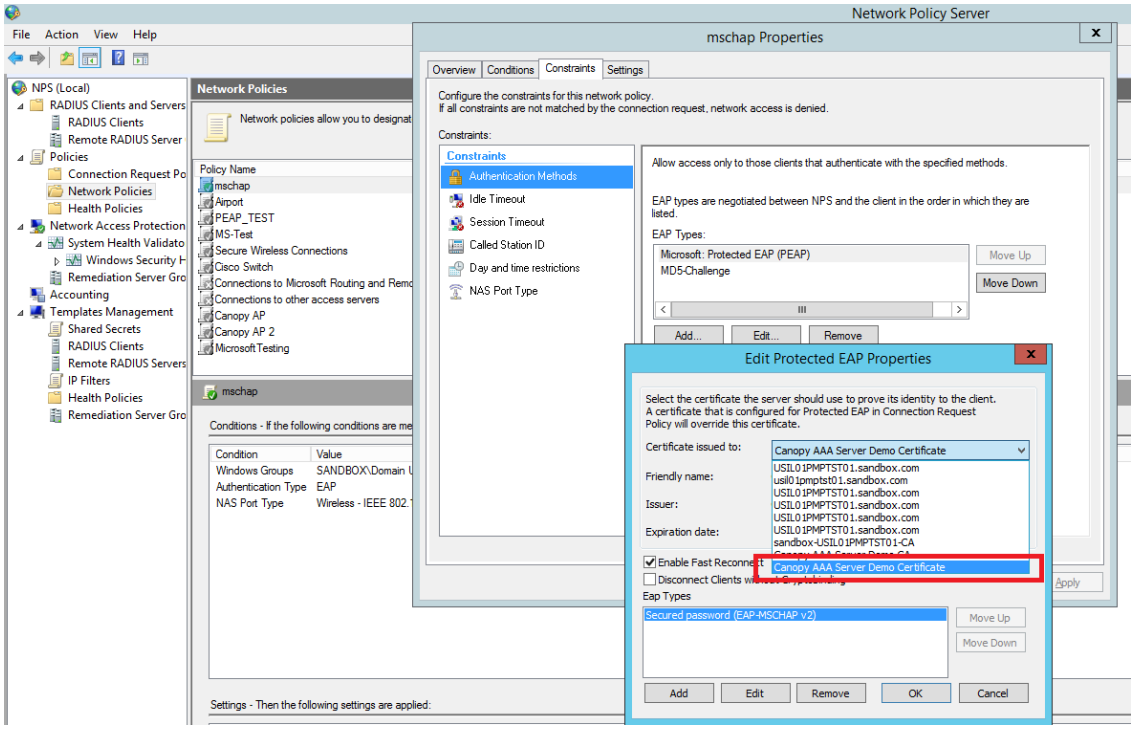
1. Copy the certificate which is configured in SM under **Configuration > Security -> Certificate1** to Windows Server machine.
2. Right click and select 'Install Certificate'. This will install the certificate and it's ready for use. This certificate will be used while configuring PEAP-MSCHAPv2 in NPS.

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 177 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:

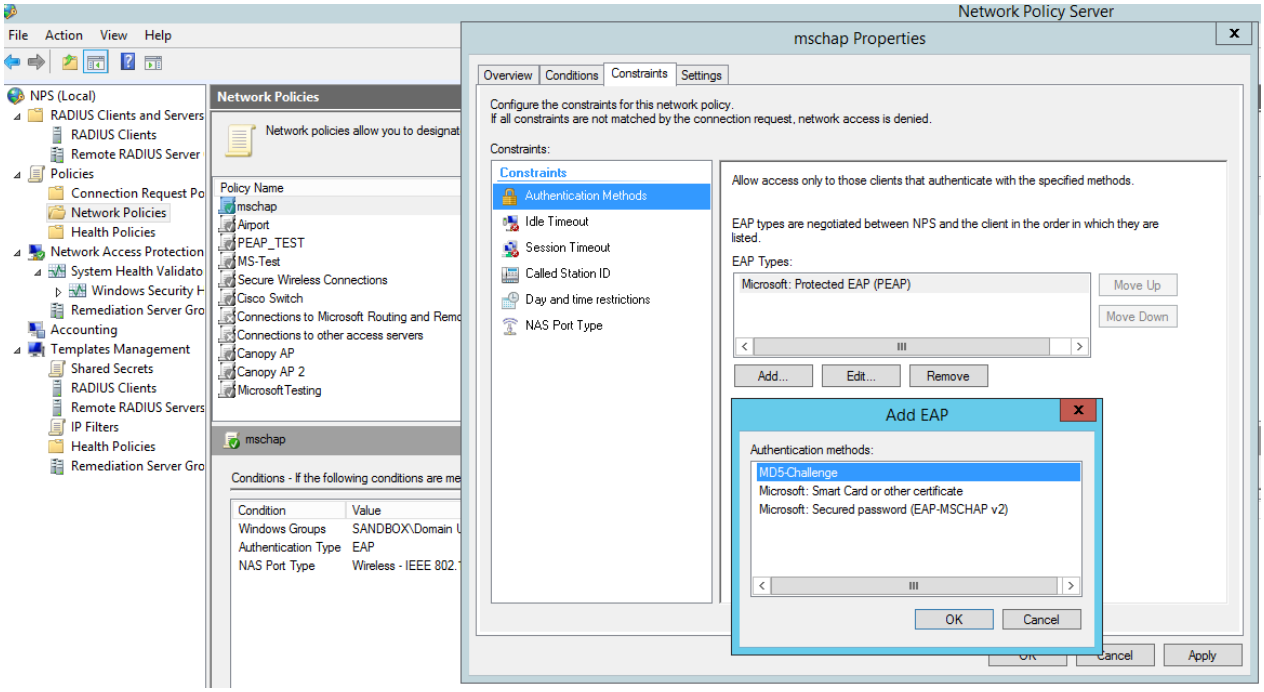
1. Follow the instructions:

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

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

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

Figure 178 Selecting MD5 from NPS console

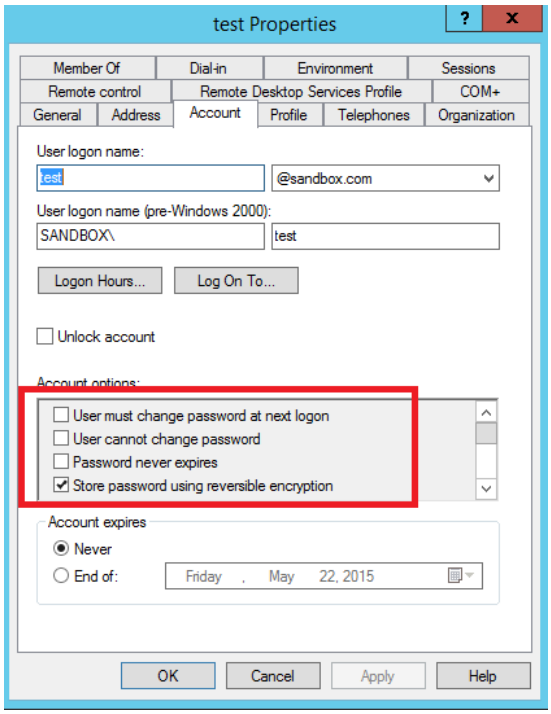


- **User Configuration in Active Directory**

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

Make sure user property is configured as shown below.

Figure 179 User configuration



○ RADIUS VSA Configuration

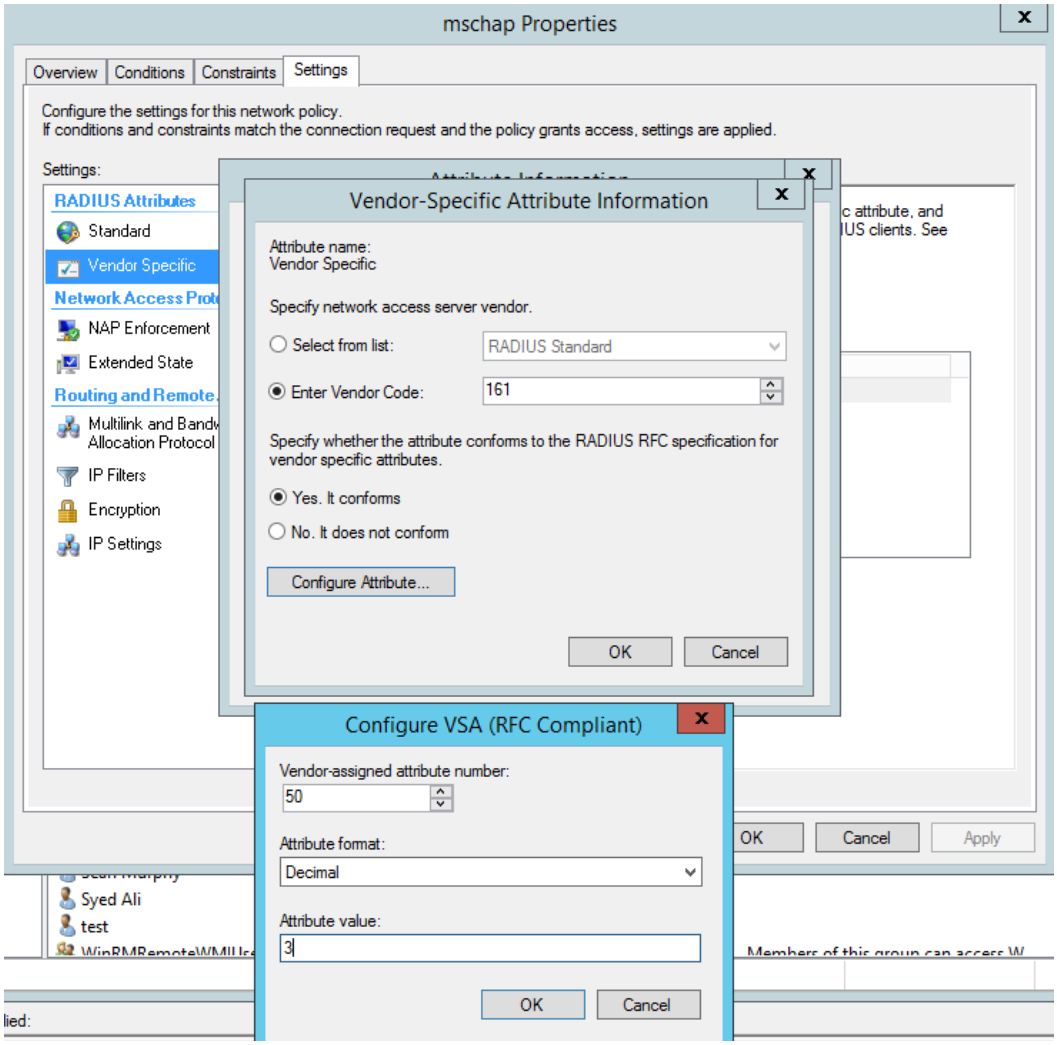
Before using VSA, the **Cambium-Canopy-UserLevel(50)** VSA must be configured with some access level say ADMIN(3).

Follow below link for configuring VSA:

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

The Cambium's vendor code is 161.

Figure 180 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

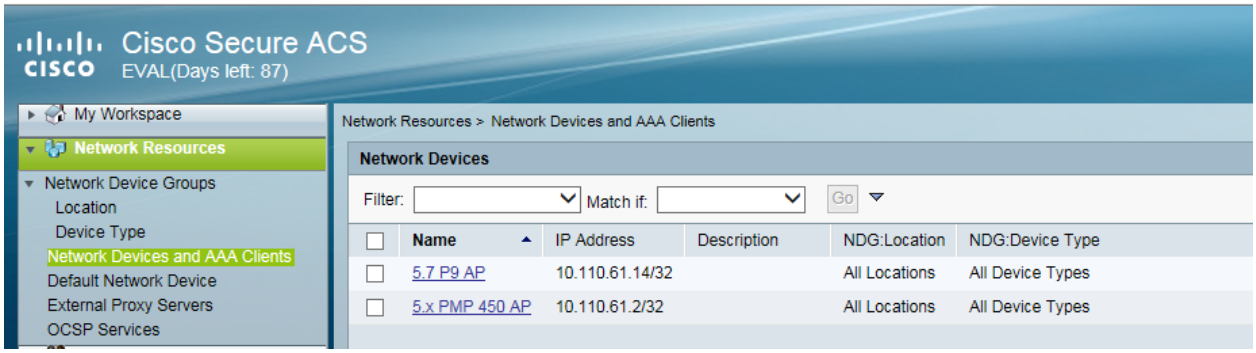
Cisco ACS RADIUS Server Support

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**

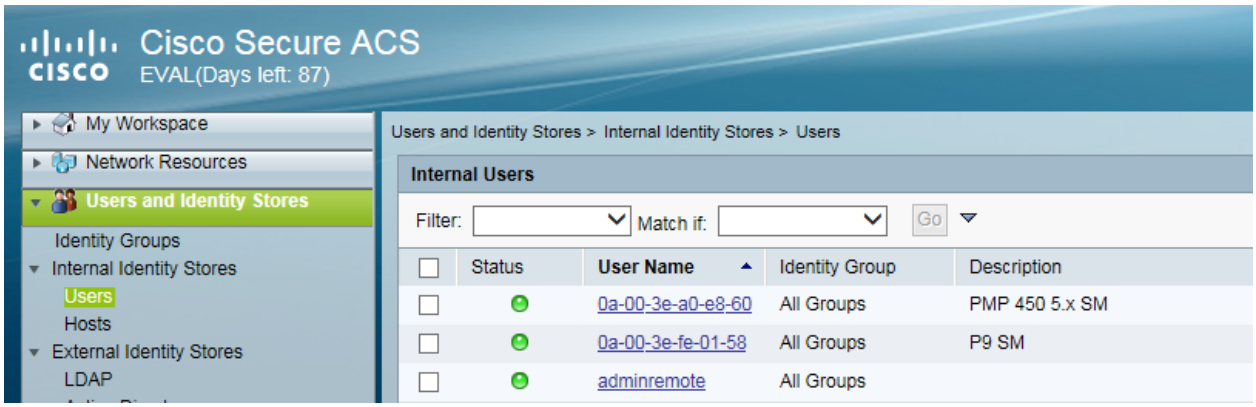
Adding RADIUS client

Figure 181 Adding RADIUS client



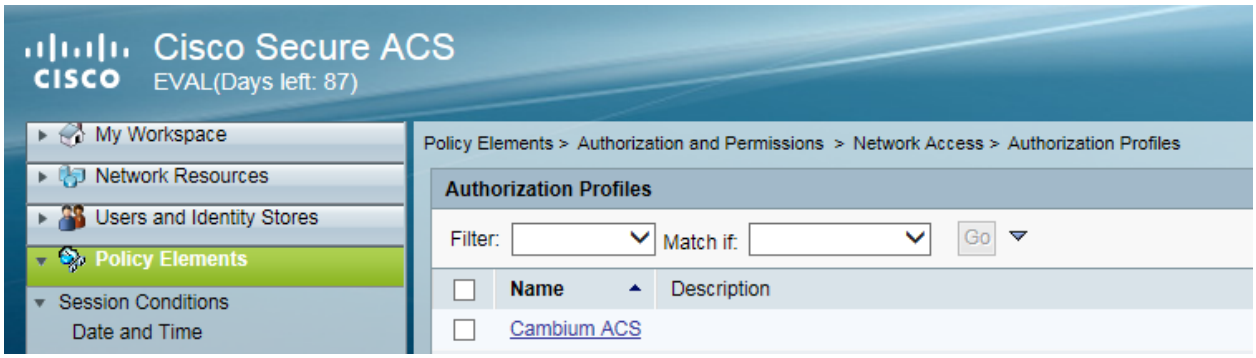
Creating Users

Figure 182 Creating users



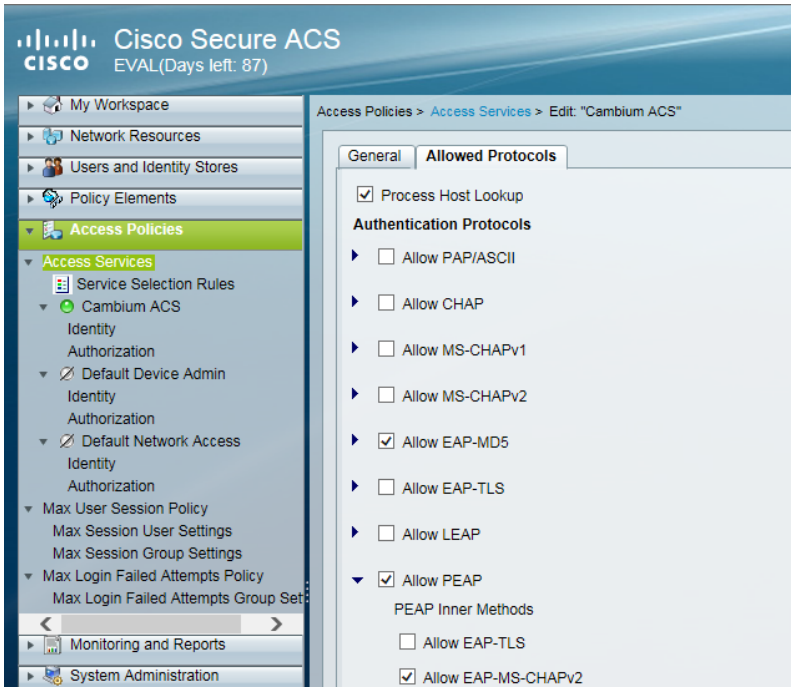
Creating RADIUS instance

Figure 183 Creating RADIUS instance



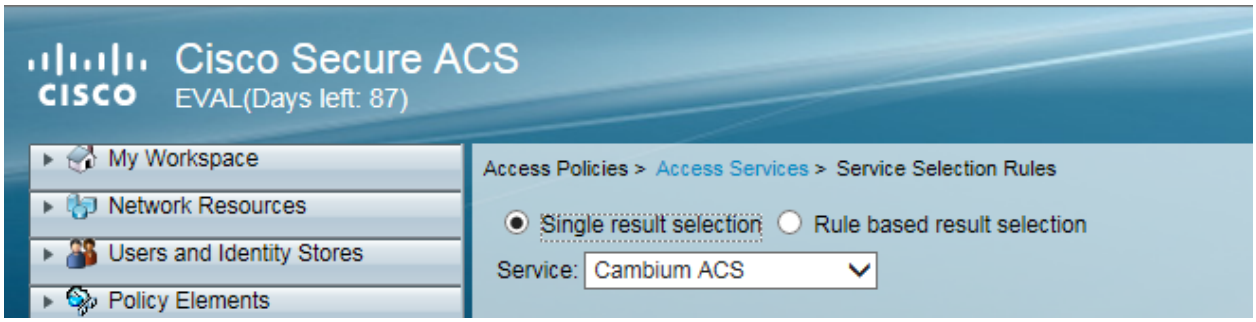
RADIUS protocols

Figure 184 RADIUS protocols



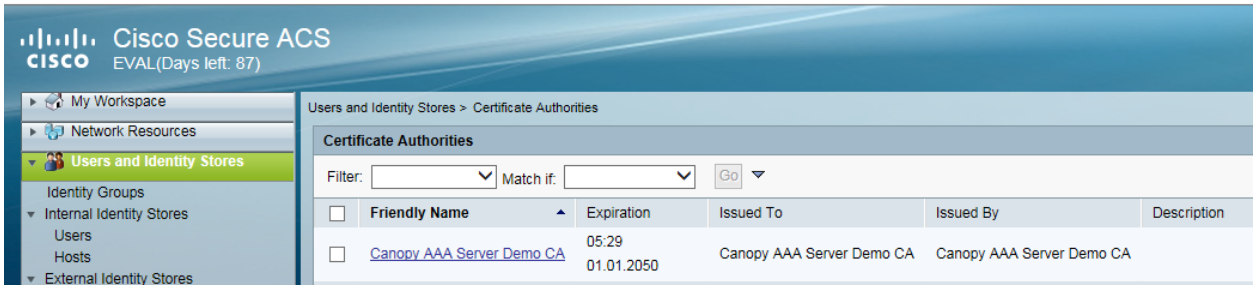
Service selection

Figure 185 Service selection



Adding Trusted CA

Figure 186 Adding Trusted CA



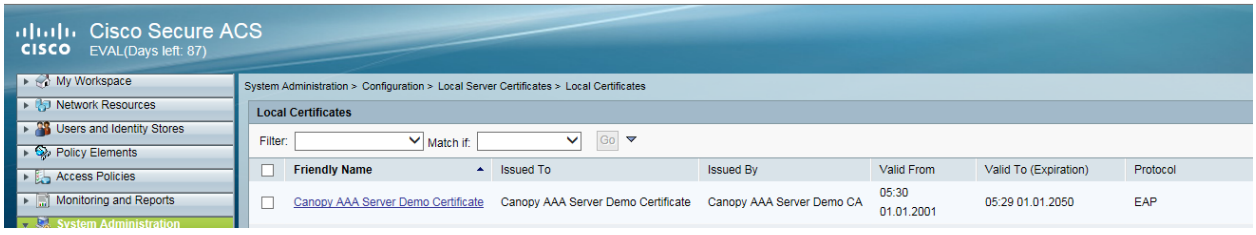
Note that certificate has to be in DER form, so if you have in PEM format convert using openssl.

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

Installing Server Certificate

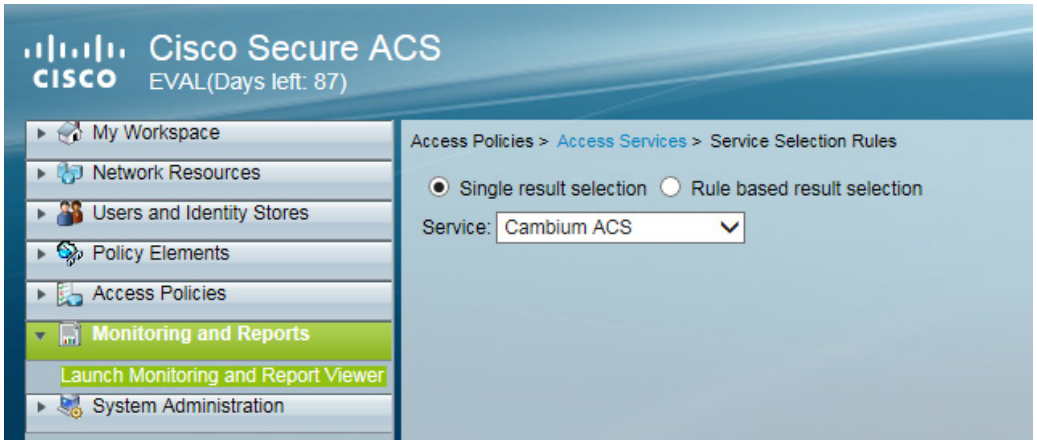
After installing trusted CA, you need to add a server certificate which will be used for TLS tunnel. Generally you have to install same certificate which is installed in your AP, so that AP can trust the radius server.

Figure 187 Installing Server Certificate



Monitoring Logs

Figure 188 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.

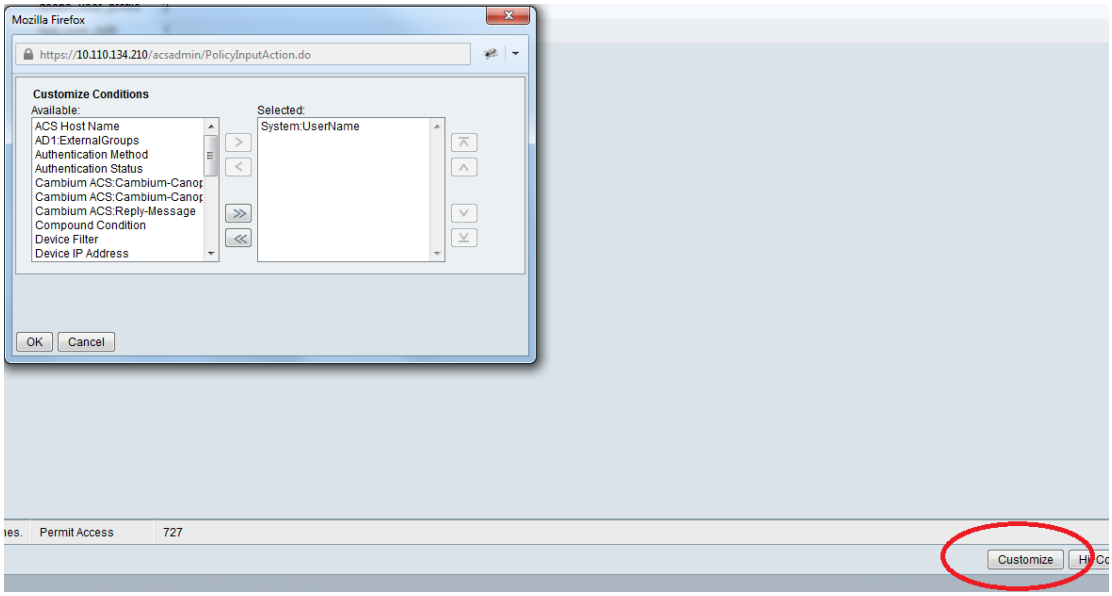
Figure 189 VSA list

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

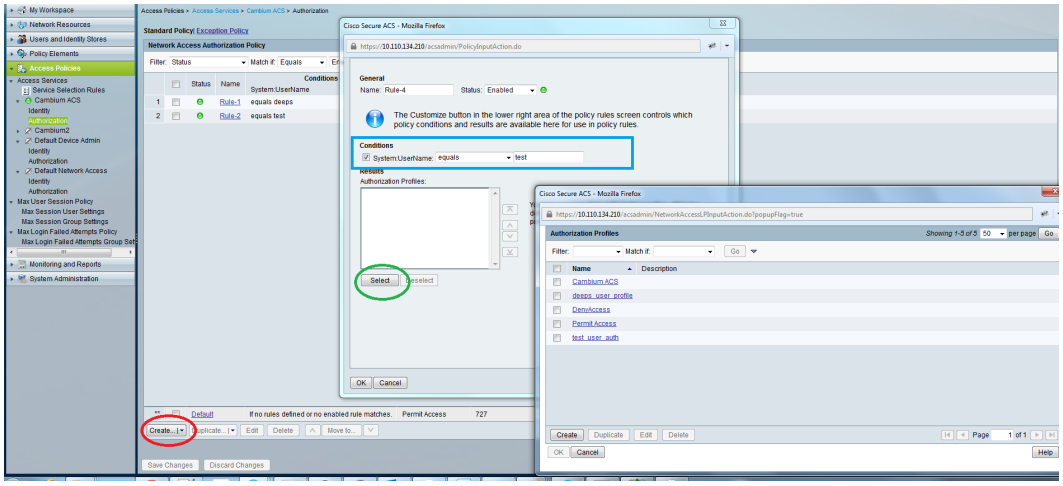
Using VSA for users

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

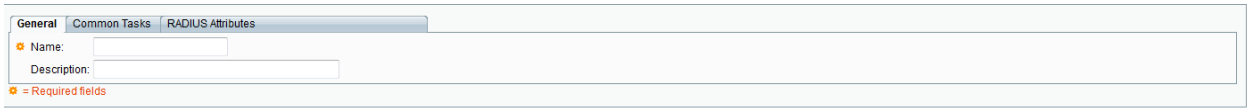
1. Change condition to User name



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

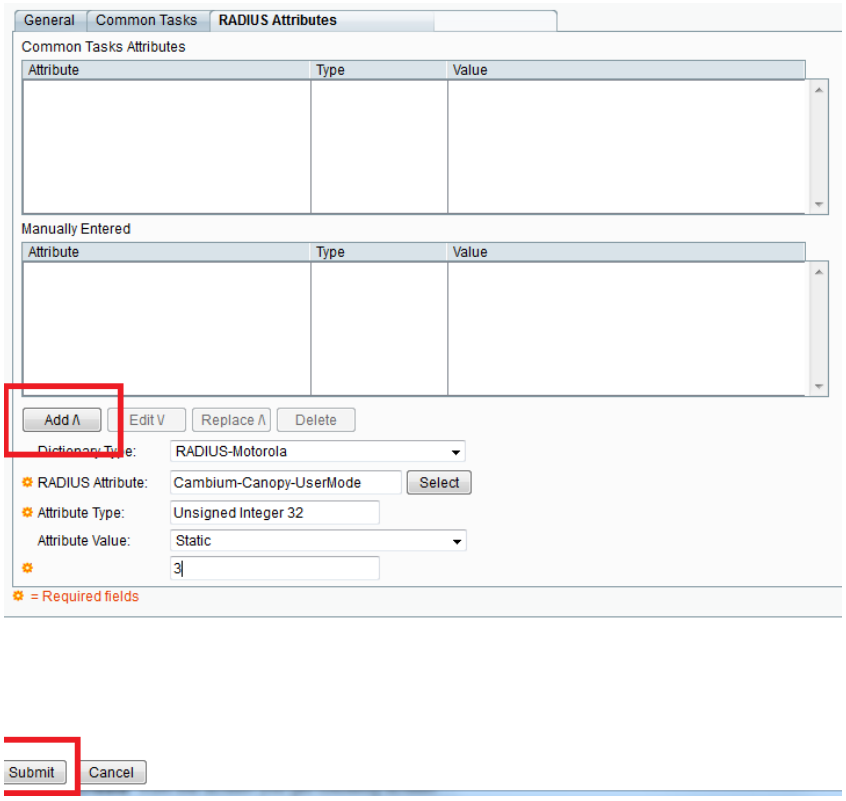


3. Click Create from the screen you get following screen



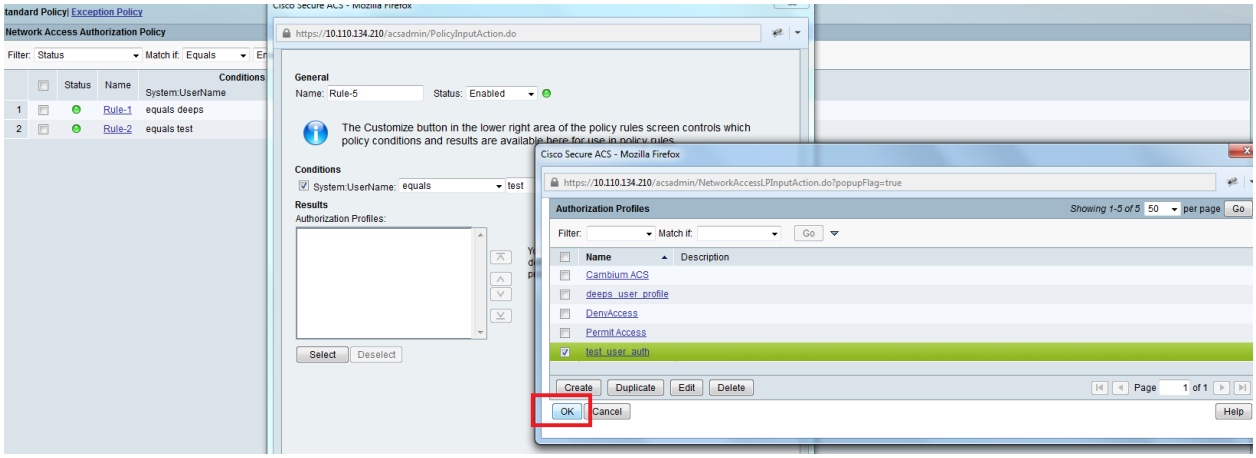
Chose some name and then move to RADIUS Attributes tab

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



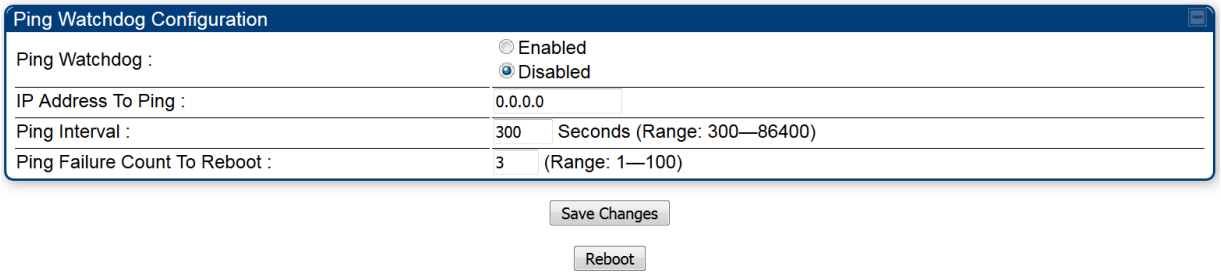
6. Finally press Save Changes and you are ready to use it.

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 202 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 8: Tools

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

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).

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.

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 30 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.

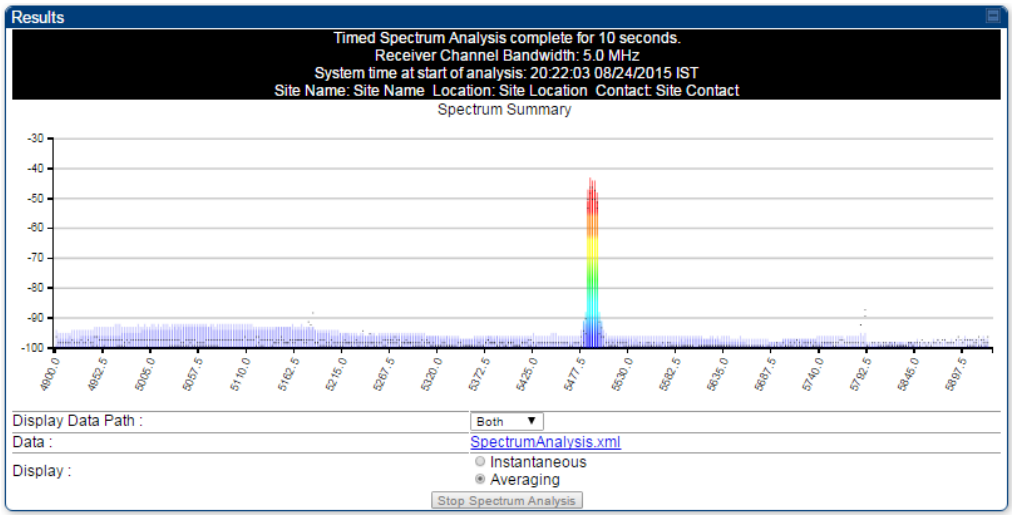
3 Access the **Tools > Spectrum Analyzer** web page of the AP/SM/BH.

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 190 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 Figure 190.

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

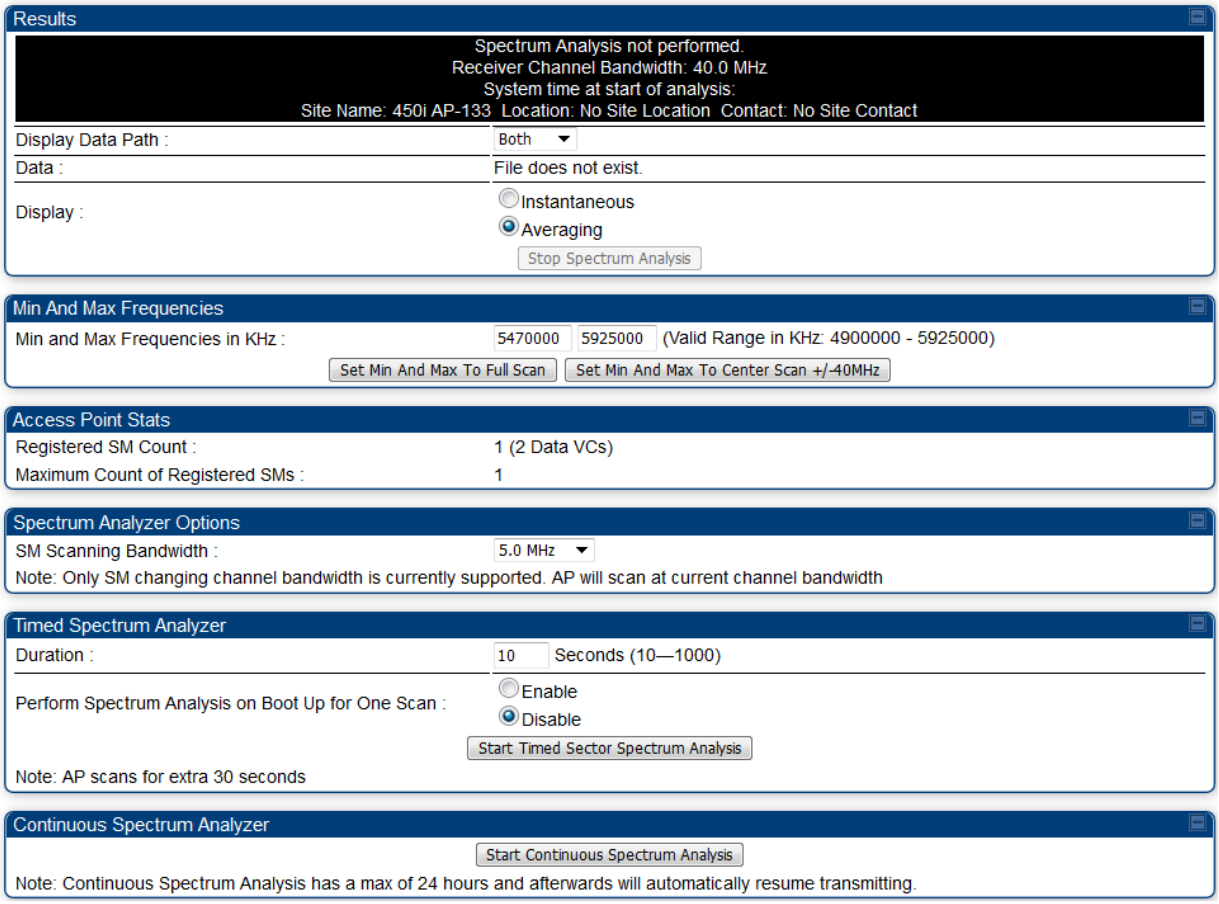
When the mouse is positioned over a bar, the receive power level, frequency, maximum and mean receive power levels are displayed above the graph

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 Table 203.

Table 203 Spectrum Analyzer page attributes - AP



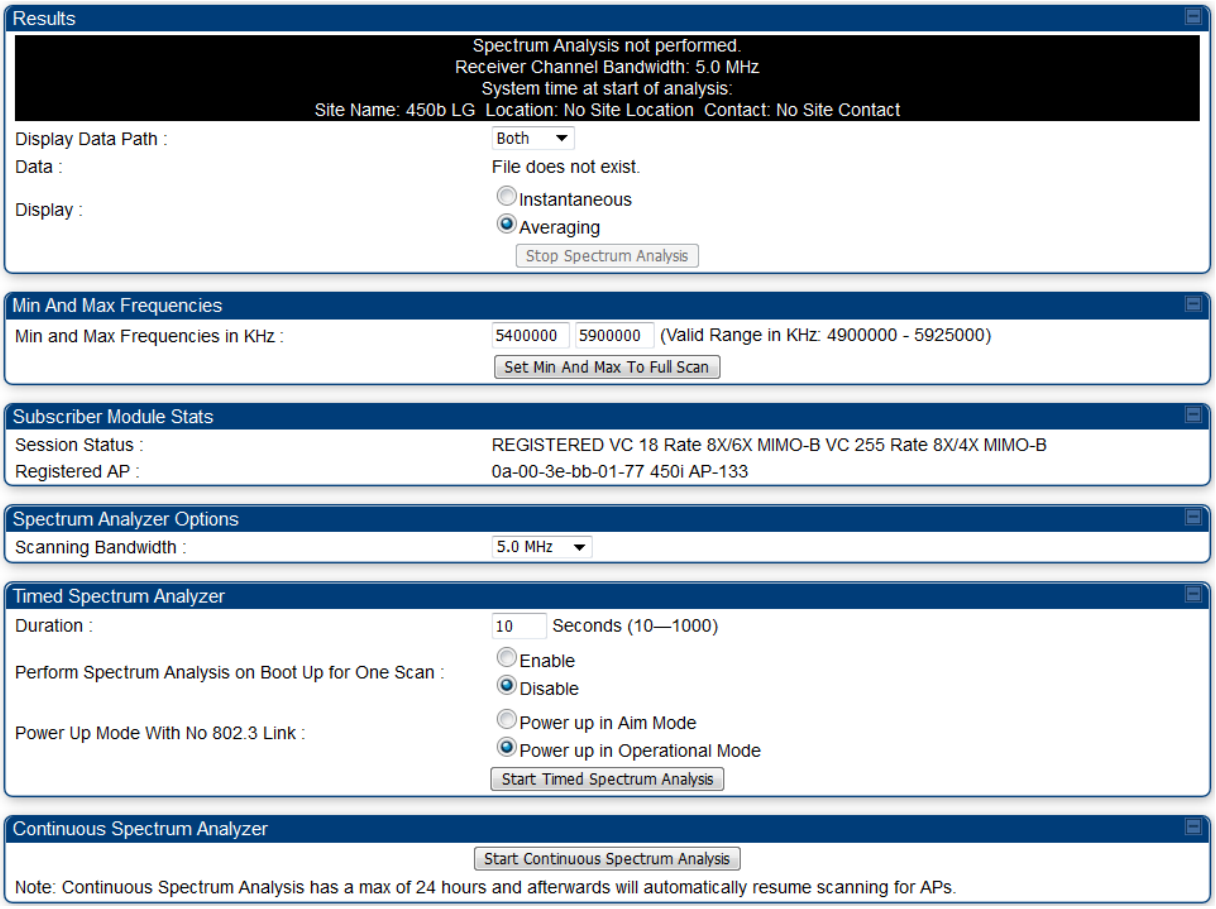
Attribute	Meaning
Display Data Path	**Both** means that the vertical and horizontal paths are displayed or an individual path may be selected to display only a single-path reading.
Data	For ease of parsing data and to facilitate automation, the spectrum analyzer results may be saved as an XML file. To 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.

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.
SM Scanning Bandwidth	This field allows to select SM's scanning bandwidth.
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 Table 204.

Table 204 Spectrum Analyzer page attributes - SM



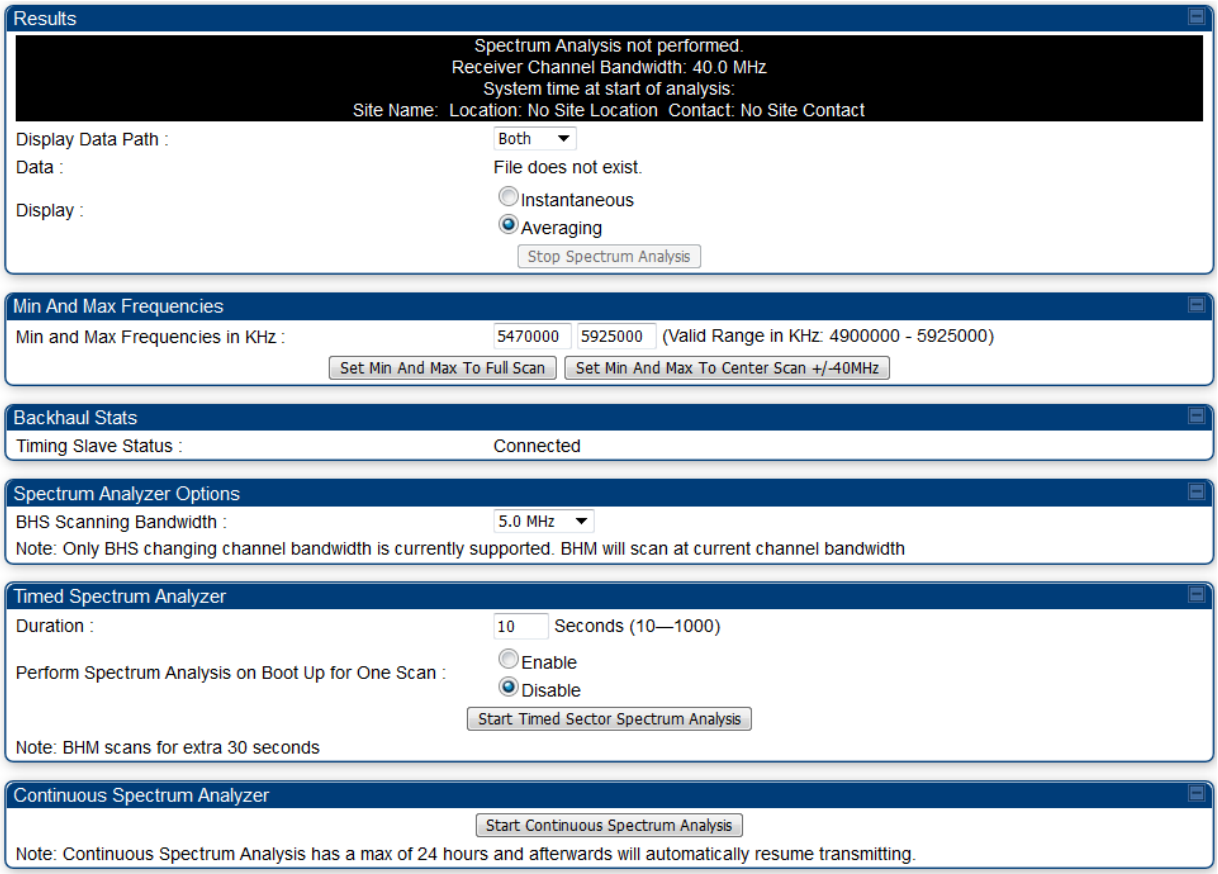
Attribute	Meaning
Display Data Path	Refer Table 203 on page 8-5
Data	Refer Table 203 on page 8-5
Display	Refer Table 203 on page 8-5
Min and Max Frequencies in KHz	To scan min to max range of frequencies, enter min and max frequencies in KHz and press **Set Min and Max to Full Scan** button. To scan +/- 40 MHz from center frequency, enter center frequency in KHz and press **Set Min And Max To Center Scan +/- 40KHz** 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 Table 203 on page 8-5
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 Table 205.

Table 205 Spectrum Analyzer page attributes - BHM



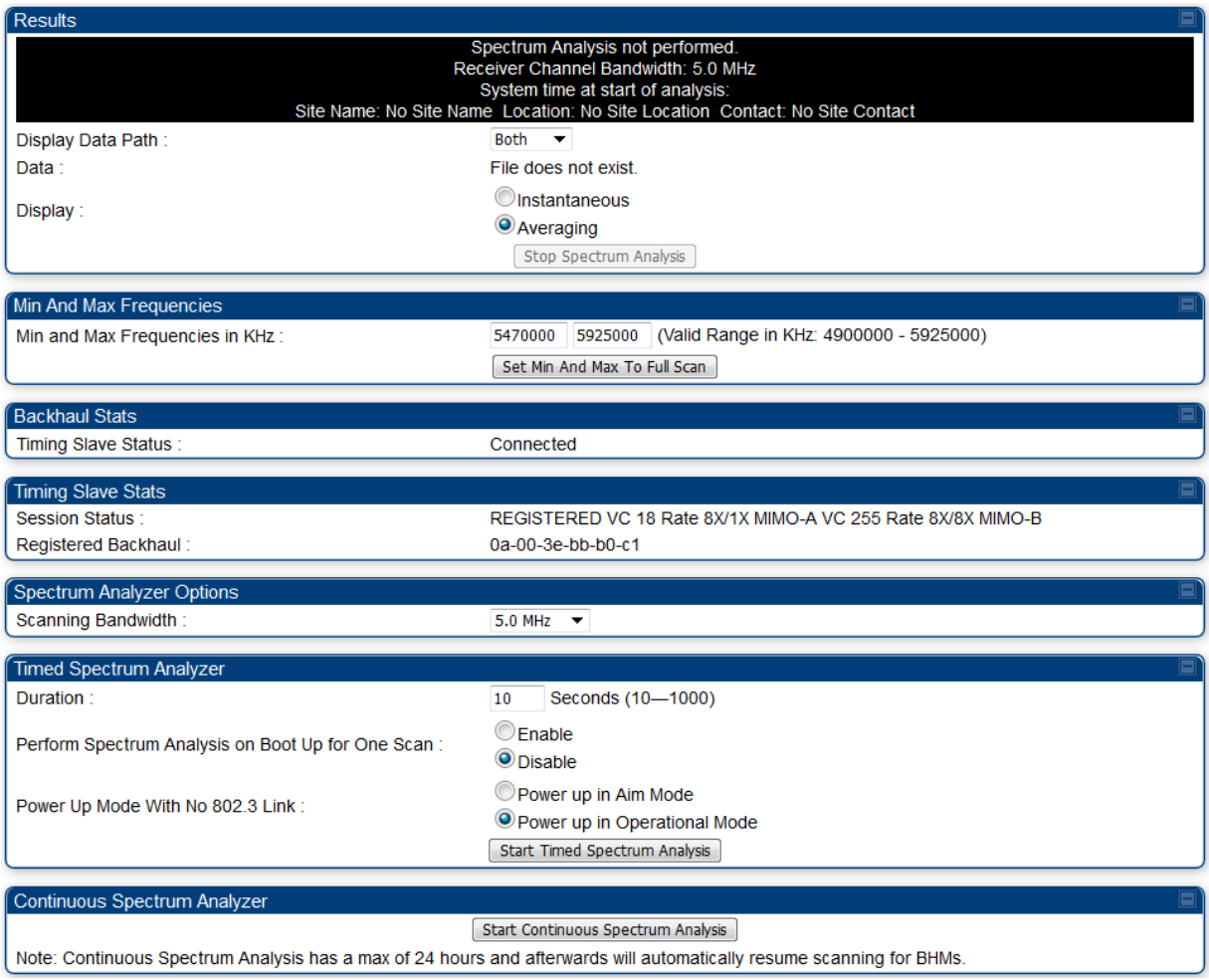
Attribute	Meaning
Data	Refer Table 203 on page 8-5
Display	Refer Table 203 on page 8-5
Duration	Refer Table 203 on page 8-5
Min and Max Frequencies in KHz	Enter minimum and maximum frequencies to be scanned.
Set Min And Max to Full Scan	On the button press, it sets minimum and maximum allowed frequencies 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.

BHS Scanning Bandwidth	This field allows to select BHS's scanning bandwidth.
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 Table 206.

Table 206 Spectrum Analyzer page attributes - BHS

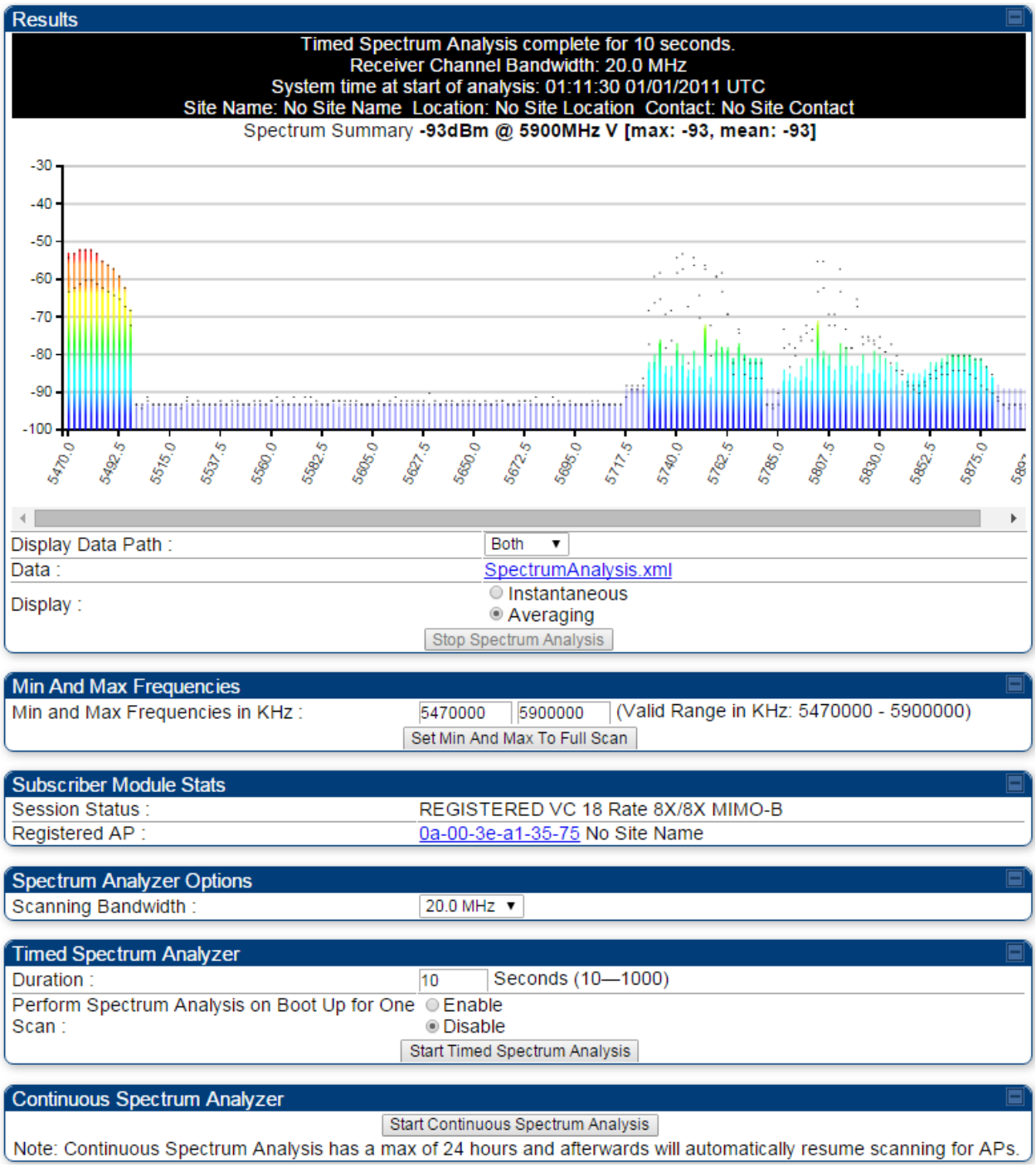


Attribute	Meaning
Data	Refer Table 203 on page 8-5
Display	Refer Table 203 on page 8-5
Session Status	This field displays current session status and rates. The session states can be Scanning, Syncing, Registering or Registered.
Registered Backhaul	This field displays MAC address of BHM and PTP model number
Duration	Refer Table 203 on page 8-5
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 Table 203 on page 8-5

Spectrum Analyzer page result of PMP 450 SM

Figure 191 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 31 Remote Spectrum Analyzer procedure

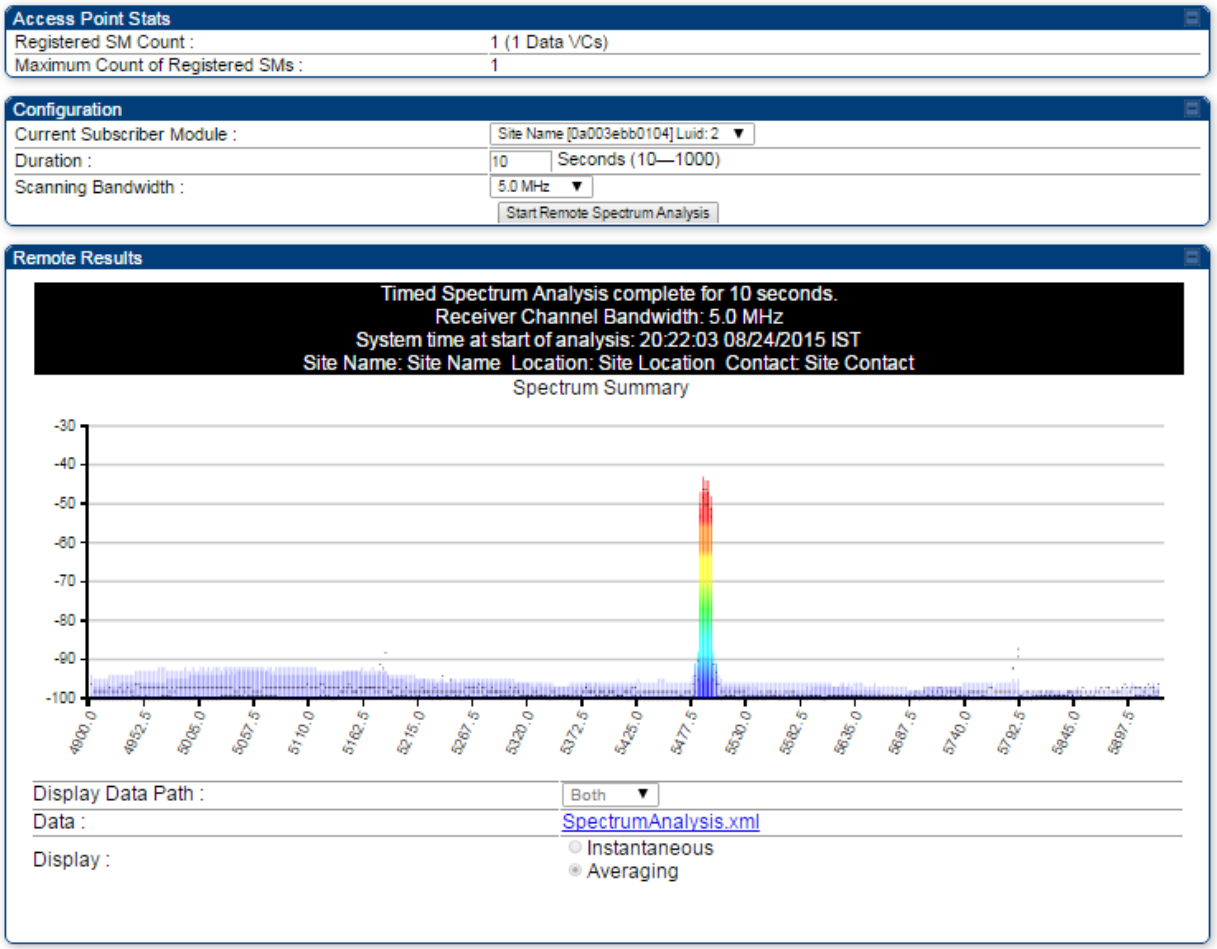
1. The AP/BHM de-registers the target SM/BHS.
2. The SM/BHS scans (for the duration set in the AP/BHM tool) to collect data for the bar graph.
3. The SM/BHS re-registers to the AP/BHM.
4. The AP/BHM displays the bar graph.

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 Table 207.

Table 207 Remote Spectrum Analyzer attributes - AP

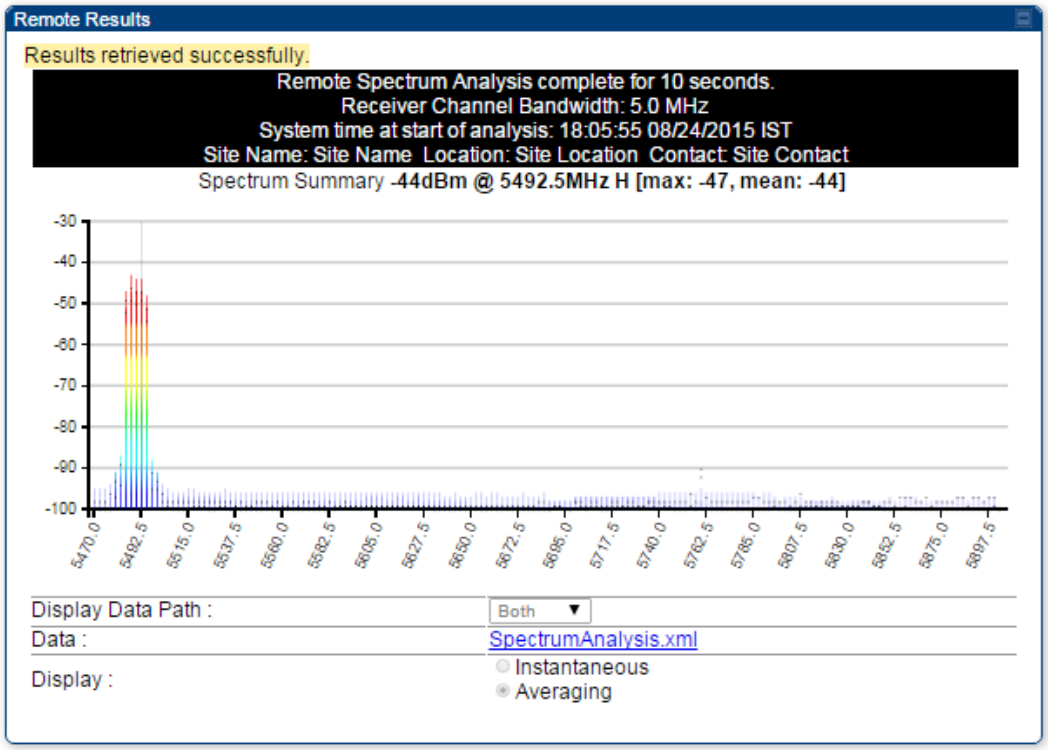


Attribute	Meaning
Registered SM Count	This field displays the number of SMs that were registered to the AP before the SA was started. This helps the user know all the SMs re-registered after performing a SA.
Maximum Count of Registered SMs	This field displays the largest number of SMs that have been 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 SM with which the Link Capacity Test is run.
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 Table 208.

Table 208 Remote Spectrum Analyzer attributes - BHM



Attribute	Meaning
Duration	Refer Table 203 on page 8-5

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.

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.

Figure 192 Alignment Tool tab of SM – Receive Power Level > -70 dBm

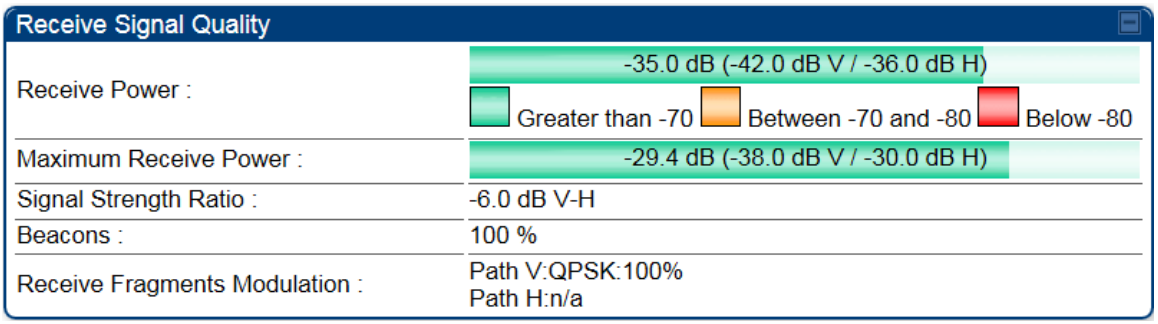


Figure 193 Alignment Tool tab of SM – Receive Power Level between -70 to -80 dBm

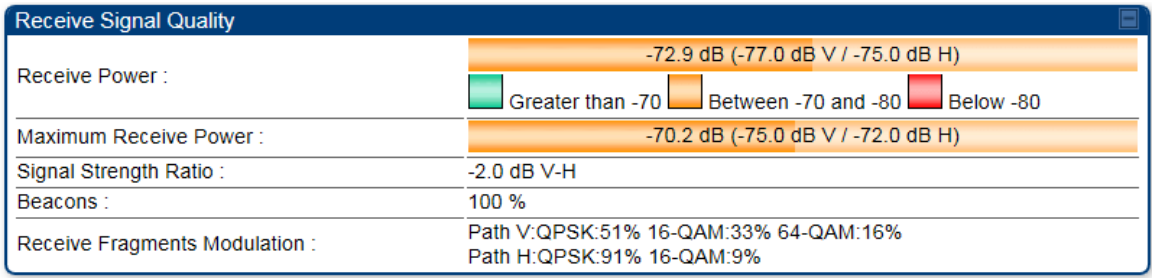
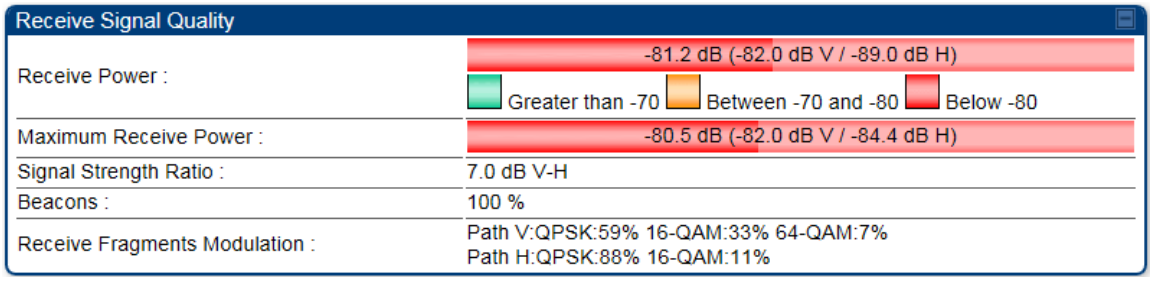


Figure 194 Alignment Tool tab of SM – Receive Power Level < -80 dBm



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 on page 2-20.

Note

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

Refer Table 25 SM/BHS LED descriptions on page 2-21 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 Table 209.

Table 209 Aiming page attributes – SM

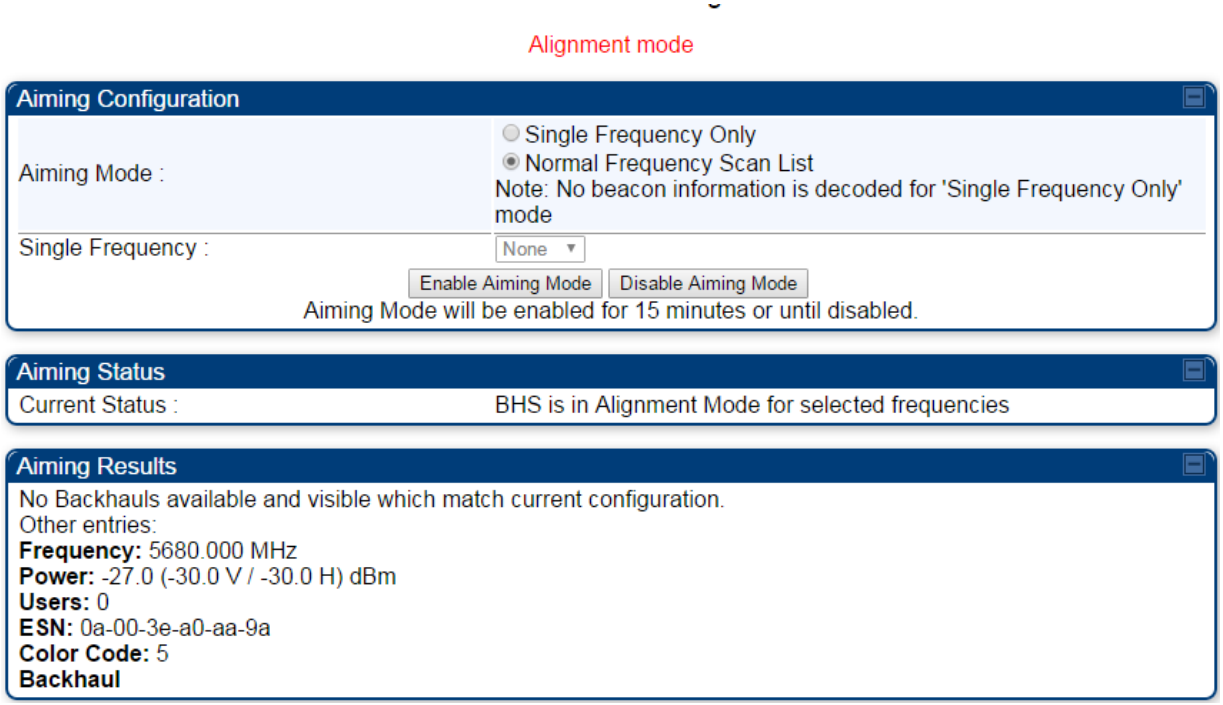
Attribute	Meaning
Aiming Mode	**Single Frequency Only:** scans only selected single frequency. **Normal Frequency Scan List: scans:** scans all frequency of scan list.
Single Frequency	Select a particular frequency from drop-down menu for scanning.
Scan Radio Frequency Only Mode	**Enabled**: the radio is configured to "aiming" or "alignment" mode, wherein the LED panel displays an indication of receive power level. See Table 25 SM/BHS LED descriptions on page 2-21. **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. **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 Table 210.

Table 210 Aiming page attributes - BHS

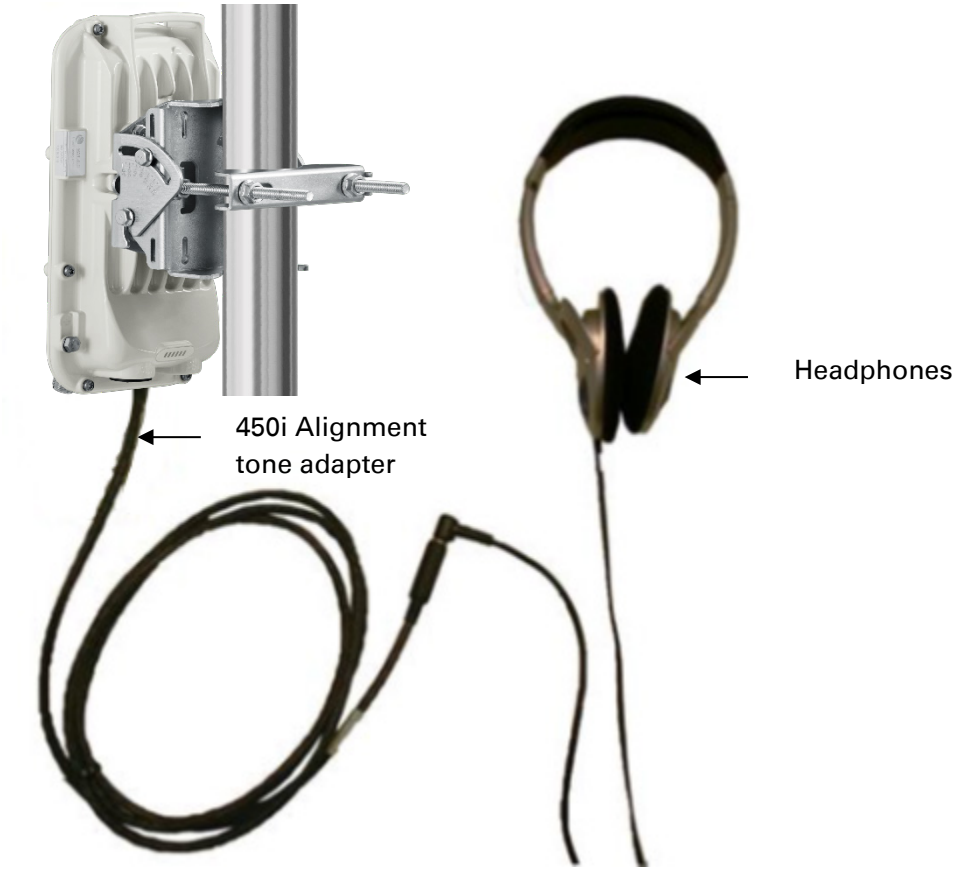


Attribute	Meaning
Refer Table 161 for Atributes details.	

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 on page 8-17, Using the Link Capacity Test tool on page 8-23 and Using AP Evaluation tool on page 8-34.

Figure 195 PMP/PTP 450i Series link alignment tone



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 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 211 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 SM's at the same time, or from multiple SM's 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.

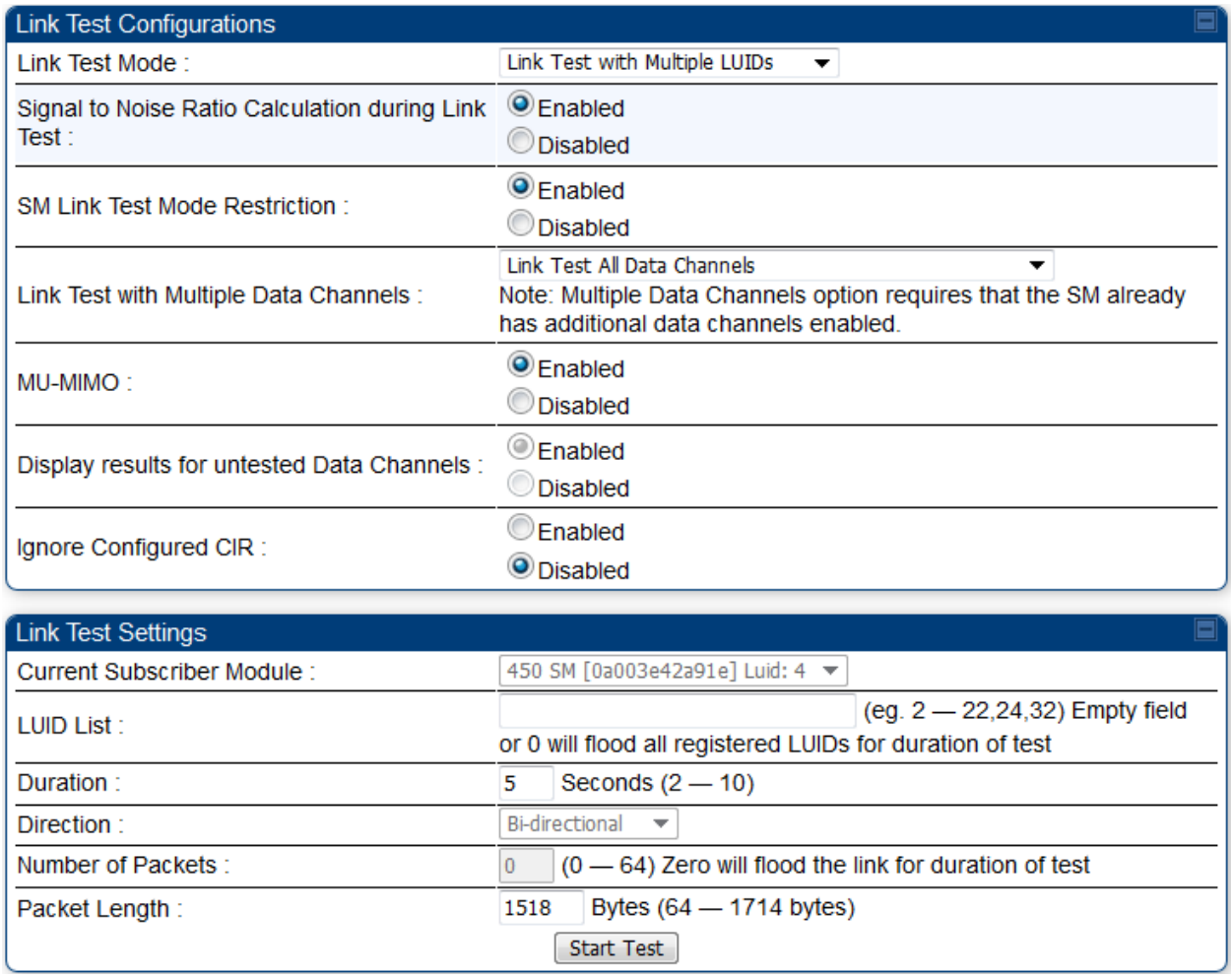
This new link test can be found under **Tools > Link Capacity Test**

Link Test with Multiple LUIDs

Note

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

Figure 196 Link Capacity Test – PMP 450m Series AP



Procedure 32 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 Select Link Test Mode –

Options are: **Link Test with Multiple LUIDs**, **Link Test without Bridging**, **Link Test with Bridging**, **Link Test with Bridging and MIR**, **Extrapolated Link Test**

All options except for the Link Test with Multiple LUIDs are available also for the 450 and 450i APs.

3 Set **Signal to Noise Ratio Calculation during Link Test** attribute to **Enabled** or **Disabled**.

4 Set the **SM Link Test Mode Restriction** attribute to **Enabled** or **Disable**d. Setting this to enabled, prevents activation of SM initiated link tests.

5 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**.

6 Set the **MU-MIMO** attribute to **Enabled** or **Disabled**.

Note: The MU-MIMO feature is enabled on the Low Priority Data Channel only

7 The **Display results for untested Data Channels** attribute is **Enabled** by default.

8 Set the **Ignore Configured CIR** attribute to **Enabled** or **Disabled**.

Link Test Settings parameters

6 Select the subscriber module to test using the **Current Subscriber Module** parameter.
Note: This parameter is not available in BHM.

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** – 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 **1518** to send 1518-byte packets during the test.

12 Click the **Start Test** button.

Figure 197 Link Test with Multiple LUIDs (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

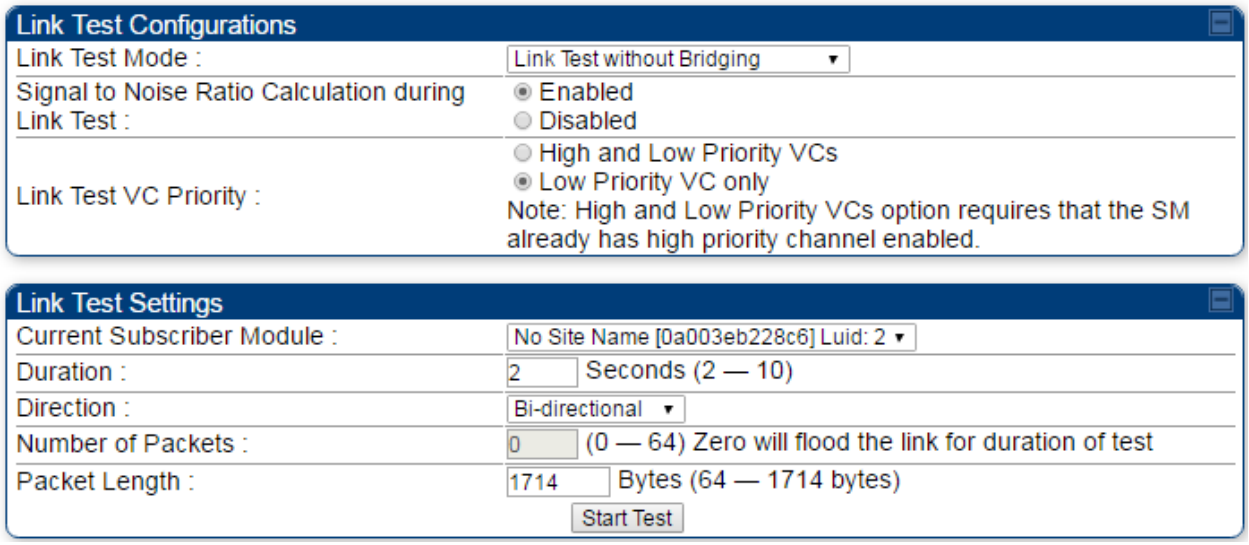
Link Test ran on 08:31:56 07/12/2018 UTC

Currently transmitting at:

8X/8X MIMO-B

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

Figure 198 Link Capacity Test – PMP 450/450i Series AP



Refer Link Test with Multiple on page 8-24 for Link Test procedure.

Figure 199 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 33 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 200 Extrapolated Link Test results

Current Results Status

Stats for LUID: 2 Test Duration: 2 Pkt Length: 1714 Test Direction Bi-Directional

Extrapolated Link Test

Downlink	Uplink	Aggregate
48.66 Mbps	7.78 Mbps	56.44 Mbps

Transmit modulation Down: 4X Up: 2X
Efficiencies Down:99 Up:100
Slots carrying data: Downlink/Uplink: 60/19

Note: Extrapolated Link Test just sends over a few packets measuring their quality and extrapolates that to what the expected throughput would be. This is just an approximation to have minimal service impact.

Efficiency

Downlink				Uplink			
Efficiency	Fragments count		Signal to Noise Ratio	Efficiency	Fragments count		Signal to Noise Ratio
	Actual	Expected			Actual	Expected	
99%	2049	2044	22 dB V 22 dB H	100%	2009	2009	0 dB V 0 dB H

Link Quality

Downlink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors
V	QPSK	426	50%	0.000
V	16-QAM	425	50%	0.000
H	QPSK	425	50%	0.000
H	16-QAM	425	50%	0.000

Uplink

RF Path	Modulation	Fragments	Modulation Percentage	Average Corrected Bit Errors

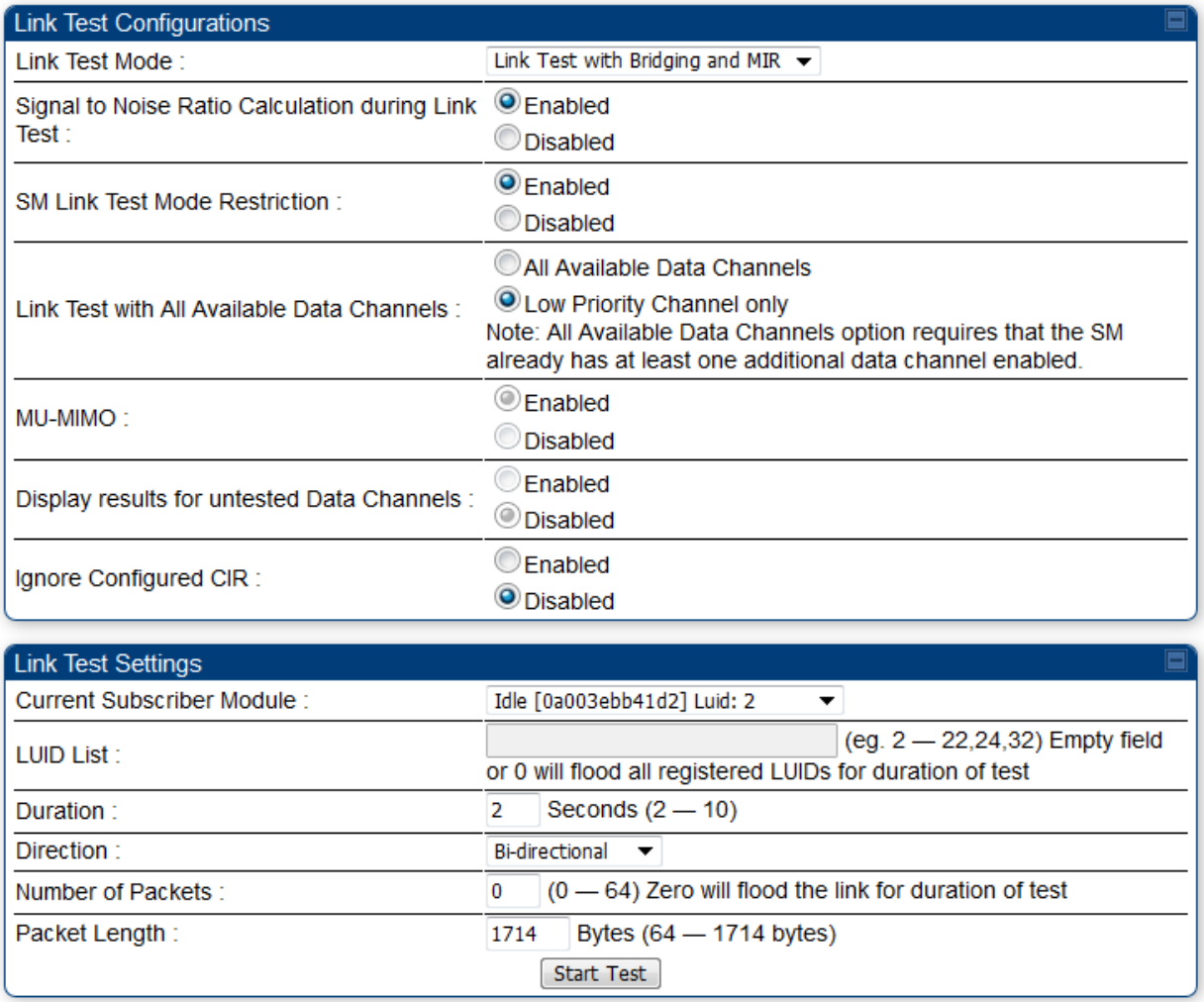
Link Test ran on 00:08:25 01/01/2011 UTC

Currently transmitting at:
VC 18 Rate 8X/6X MIMO-B

Link Capacity Test page of AP

The Link Capacity Test page of AP is explained in Table 212.

Table 212 Link Capacity Test page attributes – 450m AP



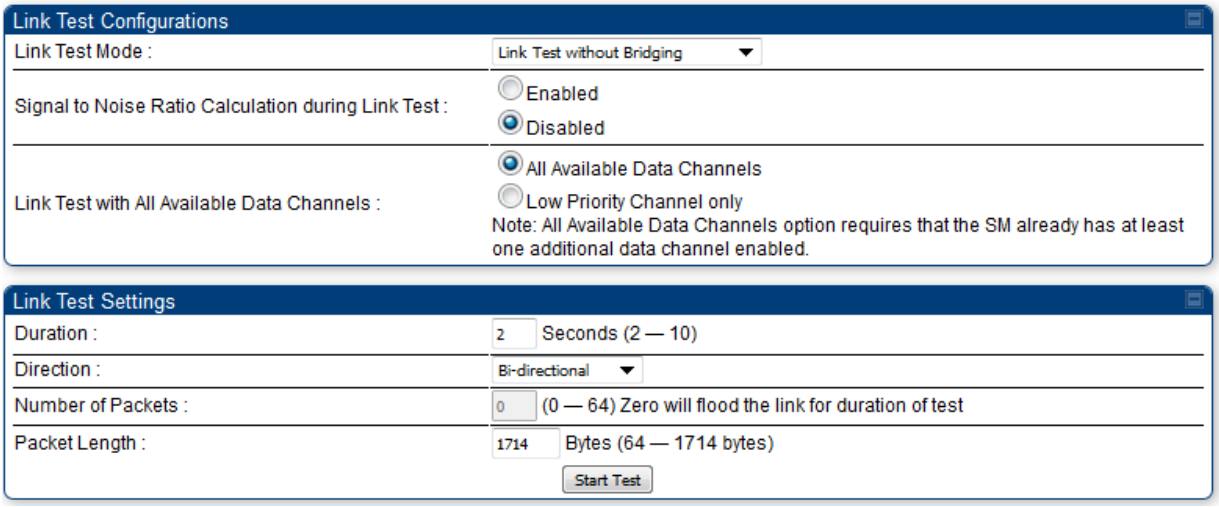
Attribute	Meaning
Link Test Mode	Select Link Test Mode from drop-down menu: • Link Test with Multiple LUIDs (PMP 450m Series AP only) • Link Test without Bridging • Link Test with Bridging • Link Test with Bridging and MIR • Extrapolated Link Test
Signal to Noise Ratio Calculation during Link Test	Enable 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 VC's" 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.
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.
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 Table 213.

Table 213 Link Capacity Test page attributes – BHM/BHS



Attribute	Meaning
Link Test Mode	See Table 212 on page 8-31
Signal to Noise Ratio Calculation during Link Test	See Table 212 on page 8-31
Link Test with All Available Data Channels	See Table 212 on page 8-31
Duration	See Table 212 on page 8-31
Direction	See Table 212 on page 8-31
Number of Packets	See Table 212 on page 8-31
Packet Length	See Table 212 on page 8-31

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

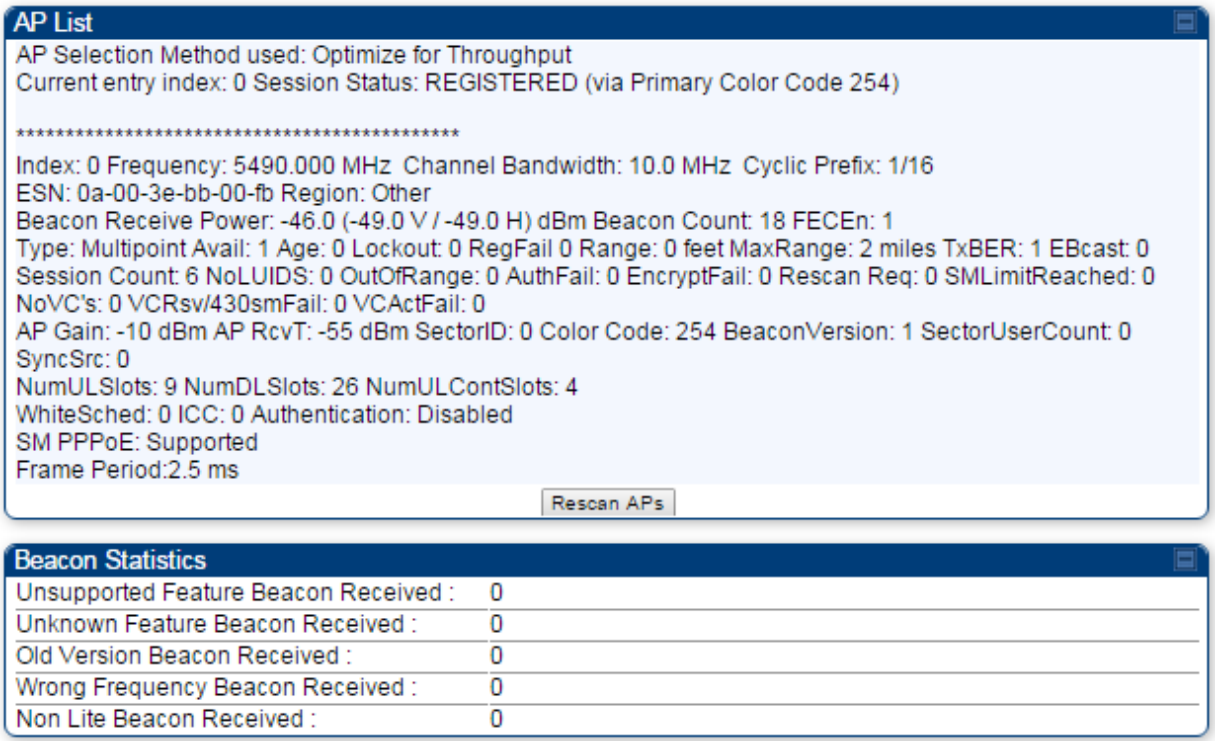
The data for this page may be suppressed by the **SM Display of AP Evaluation Data** setting in the **Configuration > Security** tab of the AP.

The AP Eval results can be accessed via SNMP and config file.

AP Evaluation page

The AP Evaluation page of AP is explained in Table 214.

Table 214 AP Evaluation tab attributes - AP



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.
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.

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. 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.

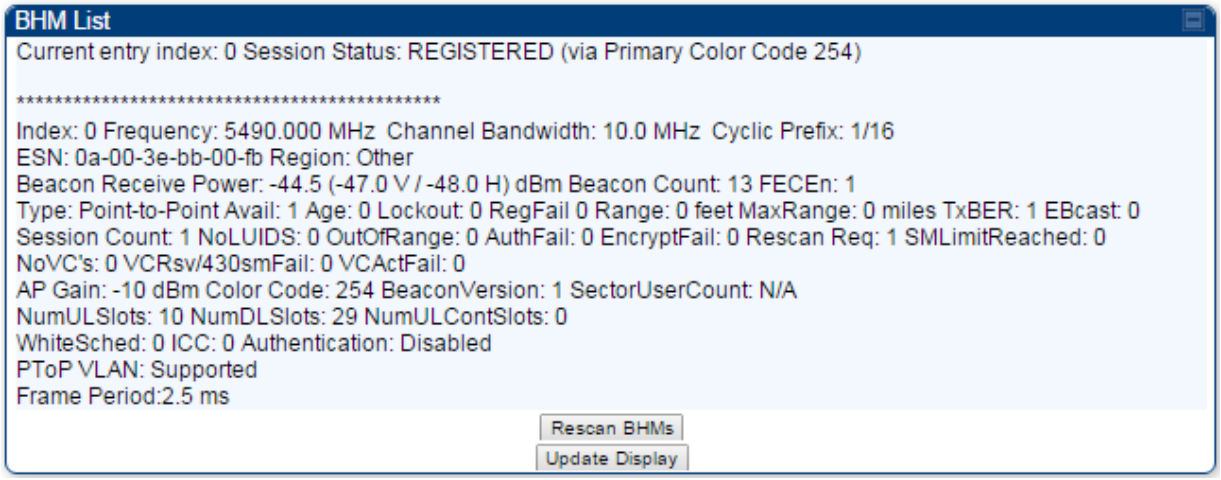
Using BHM Evaluation tool

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 Table 215.

Table 215 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.

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.
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.
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

http://www.cambiumnetworks.com/solution-papers

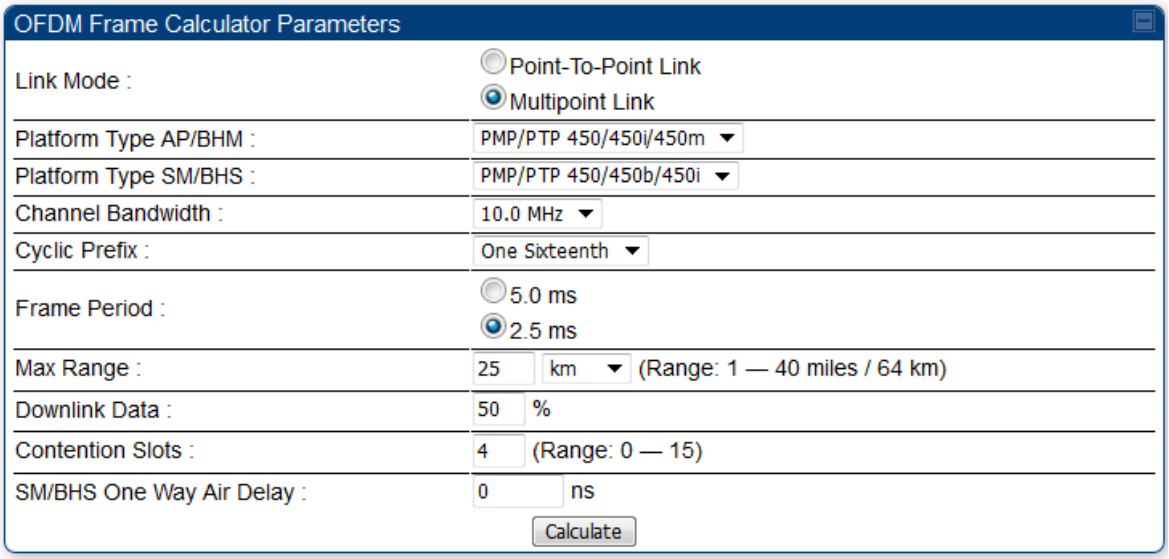
The co-location is also supported for 900 MHz PMP 450i APs (OFDM) and PMP 100 APs (FSK). Please refer *Co-location of PMP 450 and PMP 100 systems in the 900 MHz band and migration recommendations* document for details.

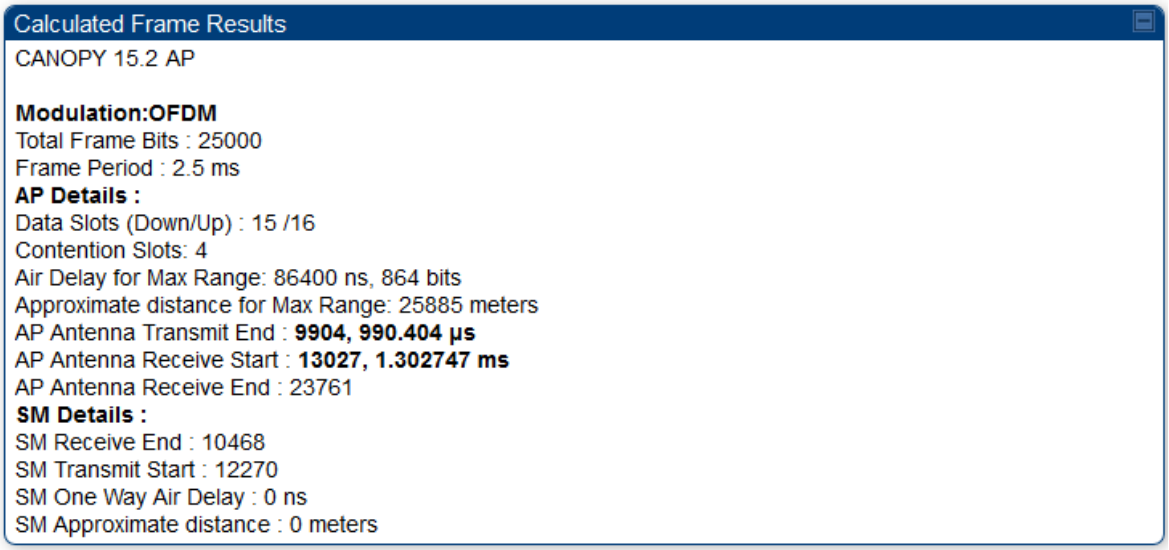
Caution

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 Table 216.

Table 216 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.
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 in Using the Frame Calculator on page 8-45, 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 217 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 34 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.

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.

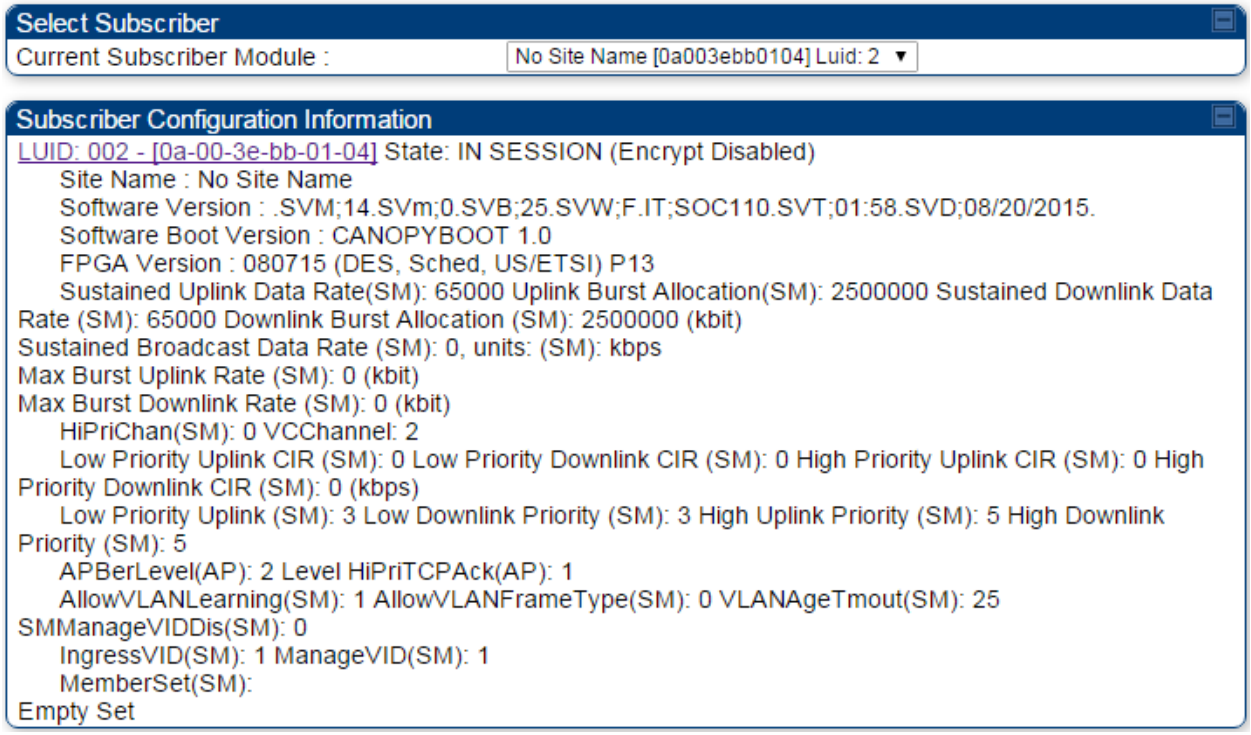
Using the Subscriber Configuration tool

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 201 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 218 Color code versus uplink/downlink rate column

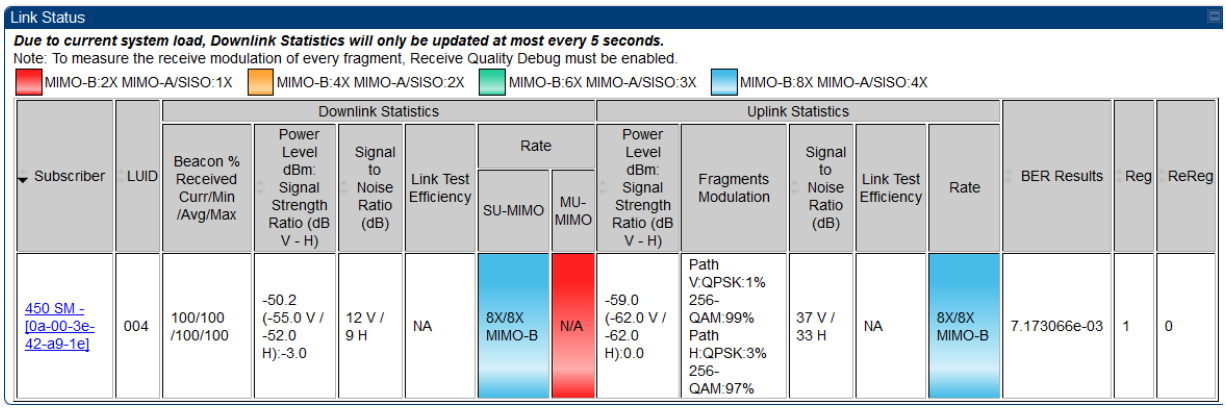
Actual Rate	1x	2x	3x	4x	6x	8x
SISO	RED	ORANGE	GREEN	BLUE	NA	NA
MIMO-A	RED	ORANGE	GREEN	BLUE	NA	NA
MIMO B	NA	RED	NA	ORANGE	GREEN	BLUE

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 219 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)	Link Test Efficiency	Rate		Power Level dBm: Signal Strength Ratio (dB V - H)	Fragments Modulation	Signal to Noise Ratio (dB)	Link Test Efficiency	Rate			
						SU-MIMO	MU-MIMO								
450 SM - [0a-00-3e-42-a9-1e]	004	100/100 /100/100	-50.2 (-55.0 V / -52.0 H):-3.0	12 V / 9 H	NA	8X/8X MIMO-B	N/A	-59.0 (-62.0 V / -62.0 H):0.0	Path V:QPSK:1% 256-QAM:99% Path H:QPSK:3% 256-QAM:97%	37 V / 33 H	NA	8X/8X MIMO-B	7.173066e-03	1	0

Attribute	Meaning
Subscriber	This field displays the MAC address and Site Name of the SM. **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 % Received Curr/Min/Max/Avg	This field displays a count of beacons received by the SM in percentage. This value must be between 99-100%. If it is lower than 99%, it indicates a problematic link. This statistic is updated every 16 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 – 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.
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	This field represents the percentage of fragments received at each modulation state, per path (polarization).
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.

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). 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).