

PTP 450i – BHS display of BHM Evaluation Data parameter



Web, Telnet, FTP Session Timeout	Enter the expiry in seconds for remote management sessions via HTTP , telnet , or ftp access to the AP/BHM.
IP Access Control	You can permit access to the AP/BHM 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 to 3	<p>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.</p> <p>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.</p>
Web Access	<p>The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • HTTP Only – provides non-secured web access. The radio to be accessed via <code>http://<IP of Radio></code>. • HTTPs Only – provides a secured web access. The radio to be accessed via <code>https://<IP of Radio></code>. • HTTP and HTTPs – If enabled, the radio can be accessed via both <code>http</code> and <code>https</code>.
SNMP	<p>This option allows to configure SNMP agent communication version. It can be selected from drop down list :</p> <ul style="list-style-type: none"> • SNMPv2c Only – Enables SNMP v2 community protocol. • SNMPv3 Only – Enables SNMP v3 protocol. It is a 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.

Security page of SM

The security page of SM/BHS is explained in [Table 90](#).

Table 91 Security attributes for SM

Authentication Key Settings

Authentication Key :	<input type="text"/> (Using All 0xFF's Key)
Select Key :	<input type="radio"/> Use Key above <input checked="" type="radio"/> Use Default Key

AAA Authentication Settings

Enforce Authentication :	Disable	
Phase 1 :	eaptls	
Phase 2 :	MSCHAPv2	
Identity/Realm :	<input type="radio"/> Enable Realm <input checked="" type="radio"/> Disable Realm Identity <input type="text"/> anonymous @ Realm <input type="text"/> canopy.net	
Username :	<input type="text"/> 0a-00-3e-a0-00-79	<input type="button"/> Use Default Username
Password :	<input type="password"/>	
Confirm Password :	<input type="password"/>	

RADIUS Certificate Settings

Upload Certificate File
File: <input type="button"/> Choose File No file chosen
<input type="button"/> Import Certificate
<input type="button"/> Use Default Certificates
<i>This will delete all current certificates</i>

Certificate 1

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

Certificate 2

C =US S =Illinois O = Canopy Solutions, Inc. OU =Canopy Wireless Broadband CN =PMP320 Demo CA Valid From: 07/01/2009 06:00:00 Valid To: 12/31/2049 23:59:59
<input type="button"/> Delete

The screenshot shows the 'Airlink Security' configuration interface with the following sections:

- Encryption Setting:** DES
- Session Timeout:** Web, Telnet, FTP Session Timeout: 800000 Seconds
- SM Management Interface Access via Ethernet Port:**
 - Ethernet Access: Enabled (radio button selected)
- IP Access Filtering:**
 - IP Access Control:
 - IP Access Filtering Enabled - Only allow access from IP addresses specified below
 - IP Access Filtering Disabled - Allow access from all IP addresses
 - Allowed Source IP 1: 0.0.0.0 / 32 Network Mask (set to 32 to disable)
 - Allowed Source IP 2: 0.0.0.0 / 32 Network Mask (set to 32 to disable)
 - Allowed Source IP 3: 0.0.0.0 / 32 Network Mask (set to 32 to disable)
- Security Mode:**
 - Web Access: HTTP Only
 - SNMP: SNMPv2c Only
 - Telnet: Enabled (radio button selected)
 - FTP: Enabled (radio button selected)
 - TFTP: Enabled (radio button selected)

Attribute	Meaning
Authentication Key	Only if the AP to which this SM will register requires authentication, specify the key that the SM will use when authenticating. For alpha characters in this hex key, use only upper case.
Select Key	<p>The Use Default Key selection specifies the predetermined key for authentication in Wireless Manager</p> <p>The Use Key above selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the WM</p>
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).
Phase 1	The protocols supported for the Phase 1 (Outside Identity) phase of authentication are EAPTLS (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	<p>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.</p> <p>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.</p>
Username	Enter a Username for the SM. This must match the username configured for the SM on the RADIUS server. The default Username is the SM's MAC address. The Username can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password	Enter the desired password for the SM in the Password and Confirm Password fields. The Password must match the password configured for the SM on the RADIUS server. The default Password is "password". The Password can be up to 128 non-special (no diacritical markings) alphanumeric characters
Upload Certificate File	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Encryption Setting	Specify the type of airlink security to apply to this SM. The encryption

setting must match the encryption setting of the AP.

None provides no encryption on the air link.

DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system.

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 than DES. 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 SM.
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.
	<p> Note</p> <p>This setting does not prevent a device connected to the Ethernet port from accessing the management interface of other SMs in the network. To prevent this, use the IP Access Filtering Enabled selection in the IP Access Control parameter of the SMs in the network. See IP Access Control below.</p>
	<p>If you want to allow management access through the Ethernet port, select Ethernet Access Enabled. This is the factory default setting for this parameter.</p>
IP Access Control	You can permit access to the SM 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 to 3	<p>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 SM from any IP address. You may populate as many as all three.</p> <p>If you selected IP Access Filtering Disabled for the IP Access Control</p>

	<p>parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.</p> <p>A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.</p>
Web Access	<p>The Radio supports secured and non-secured web access protocols.</p> <p>Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • HTTP Only – provides non-secured web access. The radio to be accessed via <code>http://<IP of Radio></code>. • HTTPs Only – provides a secured web access. The radio to be accessed via <code>https://<IP of Radio></code>. • HTTP and HTTPs – If enabled, the radio can be accessed via both http and https.
SNMP	<p>This option allows to configure SNMP agent communication version. It can be selected from drop down list :</p> <ul style="list-style-type: none"> • 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.

Security page of BHS

The Security page of BHS is explained in [Table 90](#).

Table 92 Security attributes for BHS

Authentication Key Settings												
Authentication Key : <input type="text"/> (Using All 0xFF's Key)												
Airlink Security												
Encryption Setting : <input type="text" value="DES"/>												
Session Timeout												
Web, Telnet, FTP Session Timeout : <input type="text" value="600"/> Seconds												
IP Access Filtering												
<p>IP Access Control : <input checked="" type="radio"/> IP Access Filtering Enabled - Only allow access from IP addresses specified below <input type="radio"/> IP Access Filtering Disabled - Allow access from all IP addresses</p> <table border="1"> <tr> <td>Allowed Source IP 1 :</td> <td><input type="text" value="0.0.0.0"/> / <input type="text" value="32"/></td> <td>Network Mask (set to 32 to disable)</td> </tr> <tr> <td>Allowed Source IP 2 :</td> <td><input type="text" value="0.0.0.0"/> / <input type="text" value="32"/></td> <td>Network Mask (set to 32 to disable)</td> </tr> <tr> <td>Allowed Source IP 3 :</td> <td><input type="text" value="0.0.0.0"/> / <input type="text" value="32"/></td> <td>Network Mask (set to 32 to disable)</td> </tr> </table>			Allowed Source IP 1 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/>	Network Mask (set to 32 to disable)	Allowed Source IP 2 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/>	Network Mask (set to 32 to disable)	Allowed Source IP 3 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/>	Network Mask (set to 32 to disable)	
Allowed Source IP 1 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/>	Network Mask (set to 32 to disable)										
Allowed Source IP 2 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/>	Network Mask (set to 32 to disable)										
Allowed Source IP 3 :	<input type="text" value="0.0.0.0"/> / <input type="text" value="32"/>	Network Mask (set to 32 to disable)										
Security Mode												
<table border="1"> <tr> <td>Web Access :</td> <td><input type="text" value="HTTP Only"/></td> </tr> <tr> <td>SNMP :</td> <td><input type="text" value="SNMPv2c Only"/></td> </tr> <tr> <td>Telnet :</td> <td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td> </tr> <tr> <td>FTP :</td> <td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td> </tr> <tr> <td>TFTP :</td> <td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td> </tr> </table>			Web Access :	<input type="text" value="HTTP Only"/>	SNMP :	<input type="text" value="SNMPv2c Only"/>	Telnet :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	FTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	TFTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Web Access :	<input type="text" value="HTTP Only"/>											
SNMP :	<input type="text" value="SNMPv2c Only"/>											
Telnet :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled											
FTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled											
TFTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled											

Attribute	Meaning
Authentication Key	Only if the BHM to which this BHS registers requires an authentication, specify the key that the BHS will use when authenticating. For alpha characters in this hex key, use only upper case.
Encryption Setting	<p>Specify the type of airlink security to apply to this BHS. The encryption setting must match the encryption setting of the BHM.</p> <p>None provides no encryption on the air link.</p> <p>DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system.</p> <p>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 than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.</p>
Web, Telnet, FTP	Enter the expiry in seconds for remote management sessions via HTTP,

Session Timeout	telnet, or FTP access to the BHS.
IP Access Control	You can permit access to the BHS 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 to 3	<p>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 BHS from any IP address. You may populate as many as all three.</p> <p>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.</p> <p>A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.</p>
Web Access	<p>The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • HTTP Only – provides non-secured web access. The radio to be accessed via <code>http://<IP of Radio></code>. • HTTPs Only – provides a secured web access. The radio to be accessed via <code>https://<IP of Radio></code>. • HTTP and HTTPs – If enabled, the radio can be accessed via both <code>http</code> and <code>https</code>.
SNMP	<p>This option allows to configure SNMP agent communication version. It can be selected from drop down list :</p> <ul style="list-style-type: none"> • 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.

Configuring radio parameters

- [Radio configuration page on page 7-116](#)
- [MIMO-A mode of operation for PMP 450i on page 7-134](#)
- [Improved PPS performance of PMP 450i SMs on page 7-135](#)

Radio configuration page

Radio page of AP

The **Radio** tab of the AP contains some of the configurable parameters that define how an AP operates.



Note

Only the frequencies available for your region and the selected Channel bandwidth (5/10/20) are displayed.

Table 93 AP Radio attributes

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5490.0 ▾
Channel Bandwidth :	10 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 2.5 ms
Color Code :	254 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	4 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	-10 dBm (Range: -30 — +27 dBm) (-13 dBm V / -13 dBm H)
External Gain :	0 dB (Range: 0 — +40 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power

Multicast Data Control	
Multicast VC Data Rate :	Disable ▾
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 0 kbps)

Advanced	
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Attribute	Meaning
Frequency Band	Select the desired operating frequency band.
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is None . For a list of channels in the band, see the drop-down list on the radio GUI.
Alternate Frequency Carrier 1 and 2	These parameters are displayed based on Regional Settings. Refer Country on page 7-72
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. The supported Channel Bandwidths are 5, 10 and 20 MHz.
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 multipathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Frame Period	Select the Frame Period in of the radio. The support Frame Periods are 5 ms and 2.5 ms.
Color Code	<p>Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP <i>must</i> match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.</p> <p>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 (<i>not</i> all 255 color codes).</p>
Subscriber Color Code Rescan (When not on a Primary Color Code)	<p>This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code.</p> <p>The time (in minutes) for a subscriber to rescan (if this AP is not configured with the SM's primary color code). This timer will only fire once – if the Subscriber Color Code Wait Period for Idle timer is configured with a nonzero value and the Subscriber Color Code Rescan expires, the Subscriber Color Code Wait Period for Idle is started. If the Subscriber Color Code Wait Period for Idle timer is configured with a zero value and the Subscriber Color Code Rescan timer expires, the SM will immediately go into rescan mode</p>
Subscriber Color Code Wait Period for Idle	The time (in minutes) for a subscriber to rescan while idle (if this AP is not configured with the SM's primary color code). This timer will fire periodic events. The fired event determines if any RF unicast traffic (either inbound or outbound) has occurred since the last event. If the results of the event determine that no RF unicast traffic has occurred (SM is idle), then the subscriber will rescan.

Installation Color Code	<p>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 a 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 Rescan APs functionality on the AP Eval page).</p>
Max Range	<p>Enter a number of miles (or kilometers divided by 1.61, then rounded to an integer) for the furthest distance from which a SM is allowed to register to this AP. Do not set the distance to any greater number of miles. A greater distance</p> <ul style="list-style-type: none"> • does not increase the power of transmission from the AP. • can reduce aggregate throughput. <p>Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. If the AP is in cluster, then you <i>must</i> set this parameter on all other APs in the cluster exactly the same, except as described in the NOTE admonition below. The default value of this parameter is 2 miles (3.2 km).</p>
Downlink Data	<p>Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the AP to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the AP is 90 Mb, then 75% specified for this parameter allocates 67.5 Mb for the downlink and 22.5 Mb for the uplink. The default for this parameter is 75%. This parameter must be set in the range of 15% - 85%, otherwise the invalid input will not be accepted and the previously-entered valid setting is used.</p>
	<p>Note</p> <p>This setting does not prevent a device connected to the Ethernet port from accessing the management interface of other SMs in the network. To prevent this, use the IP Access Filtering Enabled selection in the IP Access Control parameter of the SMs in the network. See IP Access Control below.</p>
Contention Slots	This field indicates the number of (reserved) Contention slots configured

(a.k.a. Control Slots)	by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page 7-129 .
Broadcast Repeat Count	<p>The default is 2 repeats (in addition to the original broadcast packet, for a total of 3 packets sent for every one needed), and is settable to 1 or 0 repeats (2 or 1 packets for every broadcast).</p> <p>ARQ (Automatic Repeat reQuest) is not present in downlink broadcast packets, since it can cause unnecessary uplink traffic from every SM for each broadcast packet. For successful transport without ARQ, the AP repeats downlink broadcast packets. The SMs filter out all repeated broadcast packets and, thus, do not transport further.</p> <p>The default of 2 repeats is optimum for typical uses of the network as an internet access system. In applications with heavy download broadcast such as video distribution, overall throughput is significantly improved by setting the repeat count to 1 or 0. This avoids flooding the downlink with repeat broadcast packets.</p>
Transmitter Output Power	<p>This value represents the combined power of the AP's two transmitters. Nations and regions may regulate transmitter output power. For example</p> <ul style="list-style-type: none"> 5.4 GHz and 5.8 GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. <p>The professional installer of the equipment has the responsibility to</p> <ul style="list-style-type: none"> maintain awareness of applicable regulations. calculate the permissible transmitter output power for the module. confirm that the initial power setting is compliant with national or regional regulations. confirm that the power setting is compliant following any reset of the module to factory defaults.
External Gain	This value needs to correspond to the published gain of the antenna used to ensure the radio will meet regulatory requirements.
SM Receive Target Level	Each SM's Transmitter Output Power is automatically set by the AP. The AP monitors the received power from each SM, and adjusts each SM's Transmitter Output Power so that the received power at the AP from that SM is not greater than what is set in this field. This value represents the transmitted and received power (combined power) perceived on the SM.
Multicast VC Data Rate	This pull down menu of the Multicast Data Control screen helps in configuring multicast packets to be transmitted over a dedicated channel at a configurable rate of 1X, 2X, 4X or 6X. The default value is "Disable". If set to the default value, all multicast packets are transmitted over the Broadcast VC data path. This feature is available only for the PMP 450 and is not backward compatible with PMP 430 series of radios.

Multicast Repeat Count	<p>This value is the number of packets that are repeated for every multicast VC packet received on the AP (located under Radio tab of Configuration). Multicast (like Broadcast) packets go over a VC that is shared by all SMs, so there is no guaranteed delivery. The repeat count is an attempt to improve the odds of the packets getting over the link. If the user has issues with packets getting dropped, they can use this parameter to improve the performance at the cost of the overall throughput possible on that channel. The default value is <i>0</i>.</p>
Multicast Downlink CIR	<p>This value is the committed information rate for the multicast downlink VC (located under the Radio tab of Configuration). The default value is <i>0</i> kbps. The range of this parameter is based on the number of repeat counts. The higher the repeat count, the lower the range for the multicast downlink CIR.</p>
Receive Quality Debug	<p>To aid in link performance monitoring, the AP and SM now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM) and per channel (polarization).</p>

**Note**

Due to CPU load, this will slightly degrade packet per second processing.

Radio page of BHM

The Radio page of BHM is explained in [Table 93](#).

Table 94 Radio page attributes - BHM

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5490.0 ▾
Channel Bandwidth :	10 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 2.5 ms
Color Code :	254 (0—254)
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

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

Power Control	
Transmit Power :	-10 dBm (Range: -30 — +27 dBm) (-13 dBm V / -13 dBm H)
External Gain :	0 dB (Range: 0 — +40 dB)

Advanced	
Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Attribute	Meaning
Frequency Band	Select the operating frequency band of the radio. The supported bands are 4.9 GHz, 5.4 GHz and 5.7 GHz.
Frequency Carrier	Specify the frequency for the module to transmit. The default for this parameter is None . For a list of channels in the band, see the drop-down list on the radio GUI.
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 prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Frame Period	Select the Frame Period of the radio. The support Frame Periods are : 5 ms and 2.5 ms.
Color Code	<p>Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS must match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each link a different color code.</p> <p>Color code allows you to force a BHS to register to only a specific BHM. The default setting for the color code value is 0. This value matches only the color code of 0 (not all 255 color codes).</p>
Large VC data Q	<p>Enable Large VC Q for applications that burst data high rates. Large Qs may decrease effective throughput for TCP application.</p> <p>Disable Large VC Q if application need not handle bursts of data. Large Qs may decrease effective throughput for TCP application.</p>
Downlink Data	Specify the percentage of the aggregate throughput for the downlink (frames transmitted from the BHM to the subscriber). For example, if the aggregate (uplink and downlink total) throughput on the BHM is 132 Mbps, then 75% specified for this parameter allocates 99 Mbps for the downlink and 33 Mbps for the uplink. The default for this parameter is 50%. This parameter must be set in the range of 15% - 85%, otherwise the invalid input will not be accepted and the previously-entered valid setting is used.
<div style="display: flex; align-items: center;"> <div style="text-align: center; margin-right: 10px;">  </div> <div> <p>Note</p> <p>In order to prevent self-interference, the frame configuration needs to align. This includes Downlink Data, Max Range and Contention slots.</p> </div> </div>	
Transmit Power	This value represents the combined power of the BHM's two transmitters.

Nations and regions may regulate transmit power. For example

- PTP 450i modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance.

The professional installer of the equipment has the responsibility to:

- Maintain awareness of applicable regulations.
- Calculate the permissible transmitter output power for the module.
- Confirm that the initial power setting is compliant with national or regional regulations.

Confirm that the power setting is compliant following any reset of the module to factory defaults.

External Gain	This value needs to correspond to the published gain of the antenna used to ensure the radio will meet regulatory requirements.
Frame Alignment Legacy Mode	<p>Enabled (Leacy Mode, no alignment): This is to enable Frame alignment Legacy mode.</p> <p>Disabled: This is to disable Frame Alignment Legacy Mode.</p> <p>By default this is recommended to be left enabled. However, if GPS sync problems are found, please contact support for use of this option.</p>
Receive Quality Debug	To aid in link performance monitoring, the BHM and BHS now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM, 256-QAM) and per channel (polarization).



Note

Due to CPU load, this slightly degrades the packet during per second processing.

Radio page of SM

The Radio page of SM is explained in [Table 94](#).

Table 95 Radio attributes - SM

Radio Configuration

The unit is configured for None, but the network has overridden it to Other

4.9 GHz	<input type="checkbox"/> 4980.000
5.4 GHz	<input checked="" type="checkbox"/> 5472.5 <input type="checkbox"/> 5475.0 <input type="checkbox"/> 5477.5 <input type="checkbox"/> 5480.0 <input type="checkbox"/> 5482.5 <input type="checkbox"/> 5485.0 <input type="checkbox"/> 5487.5 <input checked="" type="checkbox"/> 5490.0 <input type="checkbox"/> 5492.5 <input type="checkbox"/> 5495.0 <input type="checkbox"/> 5497.5 <input type="checkbox"/> 5500.0 <input type="checkbox"/> 5502.5 <input type="checkbox"/> 5505.0 <input type="checkbox"/> 5507.5 <input type="checkbox"/> 5510.0 <input type="checkbox"/> 5512.5 <input type="checkbox"/> 5515.0 <input type="checkbox"/> 5517.5 <input type="checkbox"/> 5520.0 <input type="checkbox"/> 5522.5 <input type="checkbox"/> 5525.0 <input type="checkbox"/> 5527.5 <input type="checkbox"/> 5530.0 <input type="checkbox"/> 5532.5 <input type="checkbox"/> 5535.0 <input type="checkbox"/> 5537.5 <input type="checkbox"/> 5540.0 <input type="checkbox"/> 5542.5 <input type="checkbox"/> 5545.0 <input type="checkbox"/> 5547.5 <input type="checkbox"/> 5550.0 <input type="checkbox"/> 5552.5 <input type="checkbox"/> 5555.0 <input type="checkbox"/> 5557.5 <input type="checkbox"/> 5560.0 <input type="checkbox"/> 5562.5 <input type="checkbox"/> 5565.0 <input type="checkbox"/> 5567.5 <input type="checkbox"/> 5570.0 <input type="checkbox"/> 5572.5 <input type="checkbox"/> 5575.0 <input type="checkbox"/> 5577.5 <input type="checkbox"/> 5580.0 <input type="checkbox"/> 5582.5 <input type="checkbox"/> 5585.0 <input type="checkbox"/> 5587.5 <input type="checkbox"/> 5590.0 <input type="checkbox"/> 5592.5 <input type="checkbox"/> 5595.0 <input type="checkbox"/> 5597.5 <input type="checkbox"/> 5600.0 <input type="checkbox"/> 5602.5 <input type="checkbox"/> 5605.0 <input type="checkbox"/> 5607.5 <input type="checkbox"/> 5610.0 <input type="checkbox"/> 5612.5 <input type="checkbox"/> 5615.0 <input type="checkbox"/> 5617.5 <input type="checkbox"/> 5620.0 <input type="checkbox"/> 5622.5 <input type="checkbox"/> 5625.0 <input type="checkbox"/> 5627.5 <input type="checkbox"/> 5630.0 <input type="checkbox"/> 5632.5 <input type="checkbox"/> 5635.0 <input type="checkbox"/> 5637.5 <input type="checkbox"/> 5640.0 <input type="checkbox"/> 5642.5 <input type="checkbox"/> 5645.0 <input type="checkbox"/> 5647.5 <input type="checkbox"/> 5650.0 <input type="checkbox"/> 5652.5 <input type="checkbox"/> 5655.0 <input type="checkbox"/> 5657.5 <input type="checkbox"/> 5660.0 <input type="checkbox"/> 5662.5 <input type="checkbox"/> 5665.0 <input type="checkbox"/> 5667.5 <input type="checkbox"/> 5670.0 <input type="checkbox"/> 5672.5 <input type="checkbox"/> 5675.0 <input type="checkbox"/> 5677.5 <input type="checkbox"/> 5680.0 <input type="checkbox"/> 5682.5 <input type="checkbox"/> 5685.0 <input type="checkbox"/> 5687.5 <input type="checkbox"/> 5690.0 <input type="checkbox"/> 5692.5 <input type="checkbox"/> 5695.0 <input type="checkbox"/> 5697.5 <input type="checkbox"/> 5700.0 <input type="checkbox"/> 5702.5 <input type="checkbox"/> 5705.0 <input type="checkbox"/> 5707.5 <input type="checkbox"/> 5710.0 <input type="checkbox"/> 5712.5 <input type="checkbox"/> 5715.0 <input type="checkbox"/> 5717.5 <input type="checkbox"/> 5720.0 <input checked="" type="checkbox"/> 5722.5
Custom Radio Frequency Scan Selection List :	<input type="checkbox"/> 5727.5 <input type="checkbox"/> 5730.0 <input type="checkbox"/> 5732.5 <input type="checkbox"/> 5735.0 <input type="checkbox"/> 5737.5 <input type="checkbox"/> 5740.0 <input type="checkbox"/> 5742.5 <input type="checkbox"/> 5745.0 <input type="checkbox"/> 5747.5 <input type="checkbox"/> 5750.0 <input type="checkbox"/> 5752.5 <input type="checkbox"/> 5755.0 <input type="checkbox"/> 5757.5 <input type="checkbox"/> 5760.0 <input type="checkbox"/> 5762.5 <input type="checkbox"/> 5765.0 <input type="checkbox"/> 5767.5 <input type="checkbox"/> 5770.0 <input type="checkbox"/> 5772.5 <input type="checkbox"/> 5775.0 <input type="checkbox"/> 5777.5 <input type="checkbox"/> 5780.0 <input type="checkbox"/> 5782.5 <input type="checkbox"/> 5785.0 <input type="checkbox"/> 5787.5 <input type="checkbox"/> 5790.0 <input type="checkbox"/> 5792.5 <input type="checkbox"/> 5795.0 <input type="checkbox"/> 5797.5 <input type="checkbox"/> 5800.0 <input type="checkbox"/> 5802.5 <input type="checkbox"/> 5805.0 <input type="checkbox"/> 5807.5 <input type="checkbox"/> 5810.0 <input type="checkbox"/> 5812.5 <input type="checkbox"/> 5815.0 <input type="checkbox"/> 5817.5 <input type="checkbox"/> 5820.0 <input type="checkbox"/> 5822.5 <input type="checkbox"/> 5825.0 <input type="checkbox"/> 5827.5 <input type="checkbox"/> 5830.0 <input type="checkbox"/> 5832.5 <input type="checkbox"/> 5835.0 <input type="checkbox"/> 5837.5 <input type="checkbox"/> 5840.0 <input type="checkbox"/> 5842.5 <input type="checkbox"/> 5845.0 <input type="checkbox"/> 5847.5 <input type="checkbox"/> 5850.0 <input type="checkbox"/> 5852.5 <input type="checkbox"/> 5855.0 <input type="checkbox"/> 5857.5 <input type="checkbox"/> 5860.0 <input type="checkbox"/> 5862.5 <input type="checkbox"/> 5865.0 <input type="checkbox"/> 5867.5 <input type="checkbox"/> 5870.0 <input type="checkbox"/> 5872.5 <input type="checkbox"/> 5875.0 <input type="checkbox"/> 5877.5 <input type="checkbox"/> 5880.0 <input type="checkbox"/> 5882.5 <input type="checkbox"/> 5885.0 <input type="checkbox"/> 5887.5 <input type="checkbox"/> 5890.0 <input type="checkbox"/> 5892.5 <input type="checkbox"/> 5895.0 <input checked="" type="checkbox"/> 5897.5

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

Channel Bandwidth Scan :	<input type="checkbox"/> 5 MHz <input checked="" type="checkbox"/> 10 MHz <input type="checkbox"/> 20 MHz
Cyclic Prefix Scan :	<input checked="" type="checkbox"/> One Sixteenth
Color Code :	<input type="text" value="254"/> (0—254)
Large VC data Q :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Power Control

Transmit Power :	<input type="text" value="16"/> dBm (Range: -30 — +27 dBm) (13 dBm V / 13 dBm H)
External Gain Fixed :	23 dB (Range: 0 — +40 dB)

Advanced

Receive Quality Debug :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
-------------------------	--

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-129.
Channel Bandwidth Scan	<p>The channel size used by the radio for RF transmission.</p> <p> Note</p> <p>Selecting multiple channel bandwidths will increase registration and re-registration times.</p>
Cyclic Prefix Scan	The cyclic prefix for which AP scanning is executed.
AP Selection Method	<p>Operators may configure the method by which a scanning SM selects an AP. By default, AP Selection Method is set to “Optimize for Throughput”, which has been the mode of operation in releases prior to 12.0.3.1.</p> <p>Power Level: AP selection based solely on power level <i>or</i> Optimize for Throughput: AP selection based on throughput optimization – the selection decision is based on power level (which affects the modulation state), channel bandwidth (which affects throughput) and number of SM registrations to the AP (which affects system contention performance).</p>
Color Code 1	<p>Color code allows you to force the SM to register to only a specific AP, even where the SM can communicate with multiple APs. For registration to occur, the color code of the SM and the AP <i>must</i> match. Specify a value from 0 to 254.</p> <p>Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.</p> <p>The default setting for the color code value is 0. This value matches only the color code of 0 (<i>not</i> all 255 color codes).</p> <p>SMs may be configured with up to 20 color codes. These color codes can be tagged as Primary, Secondary, or Tertiary, or Disable. When the SM is scanning for APs, it will first attempt to register to an AP that matches one of the SM’s primary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM’s secondary color codes. Failing that, the SM will continue scanning and attempt to register to an AP that matches one of the SM’s tertiary color codes. This is all done in the scanning mode of the SM and will repeat until a registration has occurred.</p> <p>Color codes in the same priority group are treated equally. For example, all APs matching one of the SM’s primary color codes are analyzed equally. Likewise, this evaluation is done for the secondary and tertiary groups in order. The analysis for selecting an AP within a priority group is based on various inputs, including signal strength and number of SMs</p>

already registered to each AP.

The first color code in the configuration is the pre-Release 9.5 color code. Thus, it is always a primary color code for legacy reasons.

The color codes can be disabled, with the exception of the first color code.

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. 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.
External Gain	<p>This value represents the antenna gain.</p> <p>For ODUs with integrated antenna, this is set at the correct value in the factory.</p> <p>For Connectorized ODUs with external antenna, the user must set this value to the overall antenna gain, including any RF cable loss between the ODU and the antenna.</p>
Large VC data Queue	AP and BH have a configurable option used to prevent packet loss in the uplink due to bursting IP traffic. This is designed for IP burst traffic particular to video surveillance applications.
Receive Quality Debug	To aid in link performance monitoring, the AP and SM now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM) and per channel (polarization).



Note

Due to CPU load, this will slightly degrade packet per second processing.



Note

The frequencies that a user can select are controlled by the country or a region and the Channel Bandwidth selected. There can be a case where a user adds a custom frequency (from the [Custom Frequencies page](#) on page 7-133) and cannot see it in the pull down menu.

Radio page of BHS

The **Radio** page of BHS is explained in [Table 95](#).

Table 96 Radio attributes - BHS

Radio Configuration

5.4 GHz

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

Custom Radio Frequency Scan Selection List :

5.7 GHz

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

5 MHz only
10 MHz only
Not available in this region

Channel Bandwidth Scan : 5 MHz, 10 MHz, 20 MHz

Cyclic Prefix Scan : One Sixteenth

Color Code : (0—254)

Large VC data Q : Enabled, Disabled

Power Control

Transmit Power :	16	dBm (Range: -30 — +22 dBm) (13 dBm H / 13 dBm V)
External Gain :	0	dB (Range: 0 — +35 dB)

Advanced

Receive Quality Debug :	<input type="radio"/> Enabled, <input checked="" type="radio"/> Disabled
-------------------------	--

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check any frequency that you want the BHS to scan for BHM transmissions. See Radio Frequency Scan Selection List on page 7-129.
Channel Bandwidth Scan	The channel size used by the radio for RF transmission.



Note

Selecting multiple channel bandwidths will increase registration and re-registration times.

Cyclic Prefix Scan	The cyclic prefix for which BHM scanning is executed.
Color Code	<p>Color code allows to force the BHS to register to only a specific BHM, even where the BHS can communicate with multiple BHMs. For registration to occur, the color code of the BHS and the BHM <i>must</i> match. Specify a value from 0 to 254.</p> <p>The color codes can be disabled, with the exception of the first color code.</p>
Large VC data Q	BHM and BHS have a configurable option used to prevent packet loss in the uplink due to bursting IP traffic. This is designed for IP burst traffic particular to video surveillance applications.
Transmit Power	This field lists the current combined transmit power level, in dBm.
External Gain	<p>This value represents the antenna gain.</p> <p>For ODUs with integrated antenna, this is set at the correct value in the factory.</p> <p>For Connectorized ODUs with external antenna, the user must set this value to the overall antenna gain, including any RF cable loss between the ODU and the antenna.</p>
Receive Quality Debug	To aid in link performance monitoring, the BHM and BHS now report the number of fragments received per modulation (i.e. QPSK, 16-QAM, 64-QAM) and per channel (polarization).


Note

Due to CPU load, this will slightly degrade packet per second processing.

Contention slots

The SM uses reserved Contention slots and unused data slots for bandwidth requests.

Uplink Data Slots are used first for data. If they are not needed for data in a given frame, the remaining data slots can be used by the SMs for bandwidth requests. This allows SMs in sectors with a small number of Contention slots configured to still successfully transmit bandwidth requests using unused data slots.

A higher number of Contention slots give higher probability that a SM's bandwidth request is correctly received when the system is heavily loaded, but with the tradeoff that sector capacity is reduced, so there is less capacity to handle the request. The sector capacity reduction is about 200 kbps for each Contention slot configured in a 20 MHz channel at QPSK MIMO-A modulation. The reduction in sector capacity is proportionally higher at MIMO-B modulations (2 times at QPSK MIMO-B, 4 times at 16 QAM MIMO-B, 6 times at 64 QAM MIMO-B and 8 times at 256 QAM MIMO-B). If very few reserved Contention slots are specified, then latency increases in high traffic periods. If too many are specified, then the maximum capacity is unnecessarily reduced.

The suggested Contention slot settings as a function of the number of active VCs in the sector are shown in the table below.

Table 97 Contention slots and number of VCs

Number of VCs	Recommended Number of Contention slots
1 to 10	3
11 to 50	4
51 to 150	6
151 and above	8

Note that each SM uses one or two VCs. All SMs have a Low Priority Channel that uses one VC; if the High Priority Channel is enabled for the SM, then the SM uses a second VC. Therefore the number of active VCs in a sector is greater than or equal to the number of SMs registered to the AP in the sector. For example, a network including 20 SMs with High Priority Channel disabled and 20 SMs with High Priority Channel enabled has 60 active VCs and may be configured with 6 Contention slots.

In a typical cluster, each AP must be set to the same number of Contention slots to assure proper timing in the send and receive cycles. However, where high incidence of small packets exists, as in a sector that serves several VoIP streams, additional Contention slots may provide better results. For APs in a cluster of mismatched Contention slots setting, or where PMP 450 is collocated with radios using different technologies, like PMP 430 or FSK, in the same frequency band, use the frame calculator. To download the PMP 450 Contention Slots Paper, see

<http://www.cambiumnetworks.com/solution-papers/pmp-450-contention-slots>.

Radio Frequency Scan Selection List

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

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

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

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

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

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

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

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

Dedicated Multicast Virtual Circuit (VC)

A Multicast VC allows to configure multicast packets to be transmitted over a dedicated channel at a configurable rate of 1X, 2X, 4X or 8X. This feature is available only for the PMP 450 and PMP 450i and is not backward compatible with PMP 430 series of radios.

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

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



Note

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

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



Note

- Actual Multicast CIR honored by the AP = Configured Multicast CINR/ (Multicast Repeat Count + 1).
- Increasing the Multicast data rate has no impact on the Unicast data rate.
- For multicast and unicast traffic mix scenario examples, see [Table 97](#).

Table 98 Example for mix of multicast and unicast traffic scenarios

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

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

Figure 70 Multicast VC statistics

Data VC Statistics (CoS: 00 = Lowest Priority, 07 = Highest Priority)																		
Subscriber	VC	CoS	Inbound Statistics							Outbound Statistics					Queue Overflow	High Priority Queue		
			octets	ucast pkts	nucast pkts	discards	errors	QPSK frgmts	16-QAM frgmts	64-QAM frgmts	256-QAM frgmts	octets	ucast pkts	nucast pkts	discards	errors		
Site Name - LUID: 002	018	00	2144887	6558	1121	0	0	5649 2098	3378 1656	2019 1607	1950 1199	2060928	7088	63	0	0	0	3972
Multicast	016	00	NA	NA	NA	NA	NA	NA	NA	NA	NA	0	0	0	0	NA	NA	
Broadcast	012	00	NA	NA	NA	NA	NA	NA	NA	NA	NA	592059	16	8523	0	0	NA	NA

The AP and SM display Transmit and Receive Multicast Data Count (under the **Statistics > Scheduler** page), as shown in [Figure 71](#).

Figure 71 Multicast scheduler statistics

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

Custom Frequencies page

In addition to the **Radio** tab, AP/SM/BH has another tab called **Custom Frequencies** as shown in Table 98.

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



Note

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

Table 99 Custom Frequencies – AP/SM/BH

Custom Frequencies Configuration	
Custom Frequency Configuration :	4950.000 MHz (Range: 4902.500 — 4997.500 MHz)
<input type="button" value="Add Frequency"/> <input type="button" value="Remove Frequency"/> <input type="button" value="Add Default Frequencies"/> <input type="button" value="Remove All Custom Frequencies"/>	
Custom Frequencies	
Number of Custom Frequencies :	12
4905.000 MHz 4910.000 MHz 4915.000 MHz 4920.000 MHz 4925.000 MHz 4930.000 MHz 4935.000 MHz 4940.000 MHz 4945.000 MHz 4950.000 MHz 4980.000 MHz 4990.001 MHz	

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

MIMO-A mode of operation for PMP 450i

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

In addition to introducing MIMO-A modes, improvements have been made to the existing rate adapt algorithm to switch between MIMO-A and MIMO-B seamlessly without any intervention or added configuration by the operator. The various modulation levels used by the PMP 450 are shown in [Table 99](#).

Table 100 PMP/PTP 450i Modulation levels

Rate	MIMO-B	MIMO-A
QPSK	2X MIMO-B	1X MIMO-A
16-QAM	4X MIMO-B	2X MIMO-A
64-QAM	6X MIMO-B	3X MIMO-A
256-QAM	8X MIMO-B	4X MIMO-A

System Performance

For System Performance details of all the PMP/PTP 450i products please refer the Link Capacity Planner at:

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

Table 101 Co-channel Interference per (CCI) MCS, PMP/PTP 450i

MCS of Victim	MCS of Interferer	Channel BW	CCI
1X (QPSK SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	10 dB
2X (16-QAM SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	17 dB
3X (64-QAM SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	25 dB
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	7 dB
2X (16-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	14 dB
3X (64-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	22 dB
4X (256-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	30 dB

2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	10 dB
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	17 dB
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	25 dB
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	33 dB

Table 102 Adjacent Channel Interference (ACI) per MCS, PMP/PTP 450i

MCS of Victim	MCS of Interferer	Channel BW	ACI	Guard Band
1X (QPSK SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
2X (16-QAM SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
3X (64-QAM SISO)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-13 dB	None
2X (16-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-13 dB	None
3X (64-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-13 dB	None
4X (256-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-10 dB	None
2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-16 dB	None
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 10 or 20 MHz	-10 dB	None

Guard Band

No Guard Bands are needed for the 5.4 GHz and 5.8 GHz bands.

Improved PPS performance of PMP 450i SMs

The PMP 450i provides improved packets per second (PPS) performance with regards to the PMP 450. Through hardware and software enhancements, the PPS performance of the PMP 450i AP has been improved to 40000 packets/second, measured through a standard RFC2544 test using 64 bytes packets. With this enhancement, operators are able to provide higher bandwidth including better VoIP and video services to end customers using existing SM deployments.

Setting up SNMP agent

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

- SNMPv2c
- SNMPv3

Configuring SNMP

The SNMP page configuration is explained below.



Note

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

SNMP page – AP/SM/BHM/BHS

The SNMP page is explained in [Table 102](#).

Table 103 SNMP page attributes

SNMPv2c Settings	
SNMP Community String 1 :	Canopy
SNMP Community String 1 Permissions :	<input type="radio"/> Read Only <input checked="" type="radio"/> Read / Write
SNMP Community String 2 (Read Only) :	Canopyro
SNMPv3 Settings	
Engine ID :	800000a1030a003ea004be
SNMPv3 Security Level :	noAuth,noPriv
SNMPv3 Authentication Protocol :	md5
SNMPv3 Privacy Protocol :	cbc-des
SNMPv3 Read-Only User :	Username: Canopyro Authorization Key: Privacy Key:
SNMPv3 Read/Write User :	<input type="radio"/> Enable R/W User Note: Also enable SNMPv2c Permission to be R/W <input checked="" type="radio"/> Disable R/W User Username: Canopy Authorization Key: Privacy Key:
SNMPv3 Trap Configuration :	Disabled
SNMP Accessing Addresses	
Accessing IP / Subnet Mask 1 :	0.0.0.0 /0
Accessing IP / Subnet Mask 2 :	0.0.0.0 /0
Accessing IP / Subnet Mask 3 :	0.0.0.0 /0
Accessing IP / Subnet Mask 4 :	0.0.0.0 /0
Accessing IP / Subnet Mask 5 :	0.0.0.0 /0
Accessing IP / Subnet Mask 6 :	0.0.0.0 /0
Accessing IP / Subnet Mask 7 :	0.0.0.0 /0
Accessing IP / Subnet Mask 8 :	0.0.0.0 /0
Accessing IP / Subnet Mask 9 :	0.0.0.0 /0
Accessing IP / Subnet Mask 10 :	0.0.0.0 /0
Trap Addresses	
SNMP Trap Server DNS Usage :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name
Trap Address 1 :	0.0.0.0
Trap Address 2 :	0.0.0.0
Trap Address 3 :	0.0.0.0
Trap Address 4 :	0.0.0.0
Trap Address 5 :	0.0.0.0
Trap Address 6 :	0.0.0.0
Trap Address 7 :	0.0.0.0
Trap Address 8 :	0.0.0.0
Trap Address 9 :	0.0.0.0
Trap Address 10 :	0.0.0.0

Trap Enable	
Sync Status :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Session Status :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Site Information	
Site Information Viewable to Guest Users :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Site Name :	No Site Name
Site Contact :	No Site Contact
Site Location :	No Site Location

Attribute	Meaning
SNMP Community String 1	Specify a control string that can allow a Network Management Station (NMS) to access SNMP information. No spaces are allowed in this string. The default string is Canopy .
SNMP Community String 1 Permissions	You can designate the SNMP Community String 1 to be the password for WM, for example, to have Read / Write access to the module via SNMP or for all SNMP access to the module to be Read Only .
SNMP Community String 2 (Read Only)	Specify an additional control string that can allow a Network Management Station (NMS) to read SNMP information. No spaces are allowed in this string. The default string is Canopyro . This password will never authenticate a user or an NMS to read/write access. The Community String value is clear text and is readable by a packet monitor. Additional security derives from the configuration of the Accessing Subnet, Trap Address, and Permission parameters.
Engine ID	The Engine ID may be between 5 and 32 hex characters. The hex character input is driven by RFC 3411 recommendations on the Engine ID. The default Engine ID is the MAC address of the device
SNMPv3 Security Level	Specify security model where users are defined and authenticated before granting access to any SNMP service. Each device can configure the security level of SNMPv3 to No authentication/No privacy, Authentication/No privacy, or Authentication/Privacy.
SNMPv3 Authentication Protocol	Currently, the SNMPv3 authentication protocol MD5 is supported.
SNMPv3 Privacy Protocol	Currently, the SNMPv3 privacy protocol CBC-DES is supported.
SNMPv3 Read-Only User	This field allows for a read-only user per device. The default values for the Read-Only users are: <ul style="list-style-type: none">• Username = Canopyro• Authentication Password = authCanopyro• Privacy Password = privacyCanopyro
SNMPv3 Read/Write	Read-write user by default is disabled. The default values for the

User	<p>Read/Write users is :</p> <ul style="list-style-type: none"> • Username = Canopy • Authentication Password = authCanopy • Privacy Password = privacyCanopy
SNMPv3 Trap Configuration	<p>When enabling transmission of SNMPv3 traps the read-only or read-write user credentials must be used and selected properly in order for the SNMP manager to correctly interpret the traps. By default transmission of SNMPv3 traps is disabled and all traps sent from the radios are in SNMPv2c format.</p>
Accessing IP / Subnet Mask 1 to 10	<p>Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both</p> <ul style="list-style-type: none"> • The network IP address in the form xxx.xxx.xxx.xxx • The CIDR (Classless Interdomain Routing) prefix length in the form /xx <p>For example:</p> <ul style="list-style-type: none"> • the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet). • 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct Community String value. <p>The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on "Classless Interdomain Routing." You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations.</p> <p>RECOMMENDATION:</p> <p>The subscriber can access the SM/BHS by changing the subscriber device to the accessing subnet. This hazard exists because the Community String and Accessing Subnet are both visible parameters. To avoid this hazard, configure the SM/BHS to filter (block) SNMP requests.</p>
SNMP Trap Server DNS Usage	<p>The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.</p>
Trap Address 1 to 10	<p>Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) or DNS names to which SNMP traps must be sent. Traps inform Wireless Manager or an NMS that something has occurred. For example, trap information is sent</p>

	<ul style="list-style-type: none">• after a reboot of the module.• when an NMS attempts to access agent information but either• supplied an inappropriate community string or SNMP version number.• is associated with a subnet to which access is disallowed.
Trap Enable, Sync Status	If the sync status traps (sync lost and sync regained) have to be sent to Wireless Manager or an NMS, select Enabled . If these traps have to be suppressed, select Disabled .
Trap Enable, Session Status	If you want session status traps sent to Wireless Manager or an NMS, select Enabled .
Site Information Viewable to Guest Users	Operators can enable or disable site information from appearing when a user is in GUEST account mode.
Site Name	Specify a string to associate with the physical module. This parameter is written into the <i>sysName</i> SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Contact	Enter contact information for the module administrator. This parameter is written into the <i>sysContact</i> SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Location	Enter information about the physical location of the module. This parameter is written into the <i>sysLocation</i> SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.

Configuring syslog

PMP/PTP 450i includes enhancements to the existing Syslog functionality.

- [Syslog event logging](#)
- [Configuring system logging](#)

Syslog event logging

Following events are logged in syslog as explained in [Table 103](#).

Table 104 Syslog parameters

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

Configuring system logging

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

Syslog page of AP/BHM

The Syslog Configuration page for AP/BHM is shown in [Table 104](#).

Table 105 Syslog Configuration attributes - AP

Syslog Server Configuration	
Syslog DNS Server Usage :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name
Syslog Server :	0.0.0.0
Syslog Server Port :	514 <small>Default port number is 514</small>
Syslog Transmission	
AP Syslog Transmit :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SM Syslog Transmit :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Syslog Level	
Syslog Minimum Level :	info
Attribute	Meaning
Syslog DNS Server Usage	To configure the AP/BHM to append or not append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
AP Syslog Transmit Or BHM Syslog Transmit	When enabled, syslog messages are sent from the AP/BHM.
SM Syslog Transmit Or BHS Syslog Transmit	When enabled, syslog messages are sent from all the registered SMs/BHS, unless they are individually set to override this.
Syslog Minimum Level	<p>This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity).</p> <p>For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.</p>

Syslog page of SM

To configure system logging, select the menu option **Configuration > Syslog**. The Syslog Configuration page is shown in [Table 105](#).

Table 106 Syslog Configuration attributes -SM

Syslog Server Configuration	
Syslog Configuration Source :	<input checked="" type="radio"/> AP preferred, use local when AP configuration unavailable <input type="radio"/> Local only
Syslog DNS Server Usage :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name
Syslog Server :	0.0.0.0
Syslog Server Port :	514 Default port number is 514
Syslog Transmission	
Syslog Transmission :	Obtain from AP, default disabled ▾
Syslog Level	
Syslog Minimum Level Source :	<input checked="" type="radio"/> AP preferred, use local when AP configuration unavailable <input type="radio"/> Local only
Syslog Minimum Level :	info ▾
Attribute	Meaning
Syslog Configuration Source	<p>This control determines whether the SM will attempt to use the syslog server definition from the AP, or whether it will use a local server definition.</p> <p>When set to AP preferred, use local when AP configuration unavailable, and if the SM can register with an AP, then it uses the syslog server defined on that AP. If the SM cannot register then it will syslog to its locally defined syslog server through its wired connection, if any.</p> <p>When set to Local only the SM ignores the AP's definition of the syslog server and allows the syslog server to be configured individually for each SM.</p>
Syslog DNS Server Usage	To configure the SM to append or not the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
Syslog Transmission	Controls the SMs ability to transmit syslog messages. When set to "Learn from AP" the AP will control whether this SM transmits syslog messages. When set to "enable" or "disable" the SM will control whether it sends syslog messages. This allows an operator to override the AP settings for individual SMs in a sector.
Syslog Minimum Level Source	<p>This control determines whether the SM attempts to use the minimum syslog level defined by the AP, or whether it uses a local defined value using the "Syslog Minimum Level" parameter.</p> <p>When set to "AP preferred, use local when AP configuration unavailable", and if the SM can register with an AP, then it uses the Syslog Minimum Level defined on that AP. If the SM cannot register then it uses its own Syslog Minimum Level setting.</p> <p>When set to "Local only" the SM will always use its own Syslog Minimum Level setting and ignores the AP's setting.</p>

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

Syslog page of BHS

The Syslog Configuration page is shown in [Table 106](#).

Table 107 Syslog Configuration attributes -BHS

Attribute	Meaning
Syslog Configuration Source	<p>This control determines whether the BHS will attempt to use the syslog server definition from the BHM, or whether it will use a local server definition.</p> <ul style="list-style-type: none"> When set to BHM preferred, use local when BHM configuration unavailable, and if the BHS can register with a BHM, then it uses the syslog server defined on that BHM. If the BHS cannot register then it will syslog to its locally defined syslog server through its wired connection, if any. When set to Local only the BHS ignores the BHM's definition of the syslog server and allows the syslog server to be configured individually for each BHS.
Syslog DNS Server Usage	To configure the BHS to append or not to append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.
Syslog Transmission	Controls the BHSs ability to transmit syslog messages. When set to Learn from BHM the BHM will control whether this BHS transmits syslog messages. When set to enable or disable the BHS will control whether it sends syslog messages. This allows an operator to override

the BHM settings for individual BHSs in a sector.

This control determines whether the BHS attempts to use the minimum syslog level defined by the BHM, or whether it uses a local defined value using the **Syslog Minimum Level** parameter.

Syslog Minimum Level Source

- When set to **BHM preferred, use local when BHM configuration unavailable**, and if the BHS can register with a BHM, then it uses the Syslog Minimum Level defined on that BHM. If the BHS cannot register then it uses its own Syslog Minimum Level setting.

When set to **Local only** the BHS will always use its own Syslog Minimum Level setting and ignores the BHM's setting.

Syslog Minimum Level

This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity).

For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

Configuring remote access

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

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

Table 108 LAN1 Network Interface Configuration tab of IP page attributes

LAN1 Network Interface Configuration	
IP Address :	<input type="text" value="169.254.1.1"/>
Network Accessibility :	<input type="radio"/> Public <input checked="" type="radio"/> Local
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway IP Address :	<input type="text" value="169.254.0.0"/>
DHCP state :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DHCP DNS IP Address :	<input type="radio"/> Obtain Automatically <input type="radio"/> Set Manually
Preferred DNS Server :	<input type="text" value="10.120.10.12"/>
Alternate DNS Server :	<input type="text" value="10.120.10.13"/>
Domain Name :	<input type="text" value="example.com"/>

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

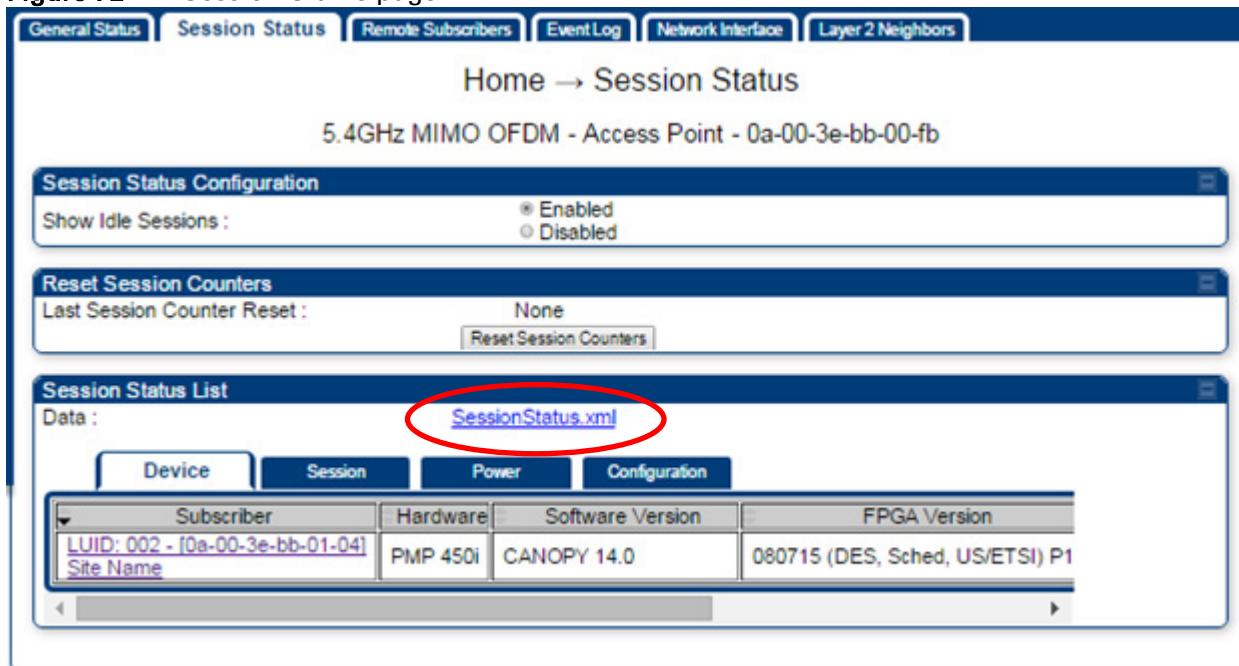
Preferred DNS Server	The first address used for DNS resolution.
Alternate DNS Server	If the Preferred DNS server cannot be reached, the Alternate DNS Server is used.
Domain Name	The operator's management domain name may be configured for DNS. The domain name configuration can be used for configuration of the servers in the operator's network. The default domain name is example.com, and is only used if configured as such.

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

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

For example, to access one of the SMs, click **LUID: 002 – [0a-00-3e-37-b9-fd]**, as shown in [Figure 72](#).

Figure 72 AP Session Status page



The screenshot shows the AP Session Status page with the following sections:

- Session Status Configuration:** Shows 'Show Idle Sessions' with radio buttons for 'Enabled' (selected) and 'Disabled'.
- Reset Session Counters:** Shows 'Last Session Counter Reset' as 'None' and a 'Reset Session Counters' button.
- Session Status List:** A table with columns: Device, Session, Power, Configuration. The 'Session' column contains a link to 'SessionStatus.xml' (which is circled in red).

Device	Session	Power	Configuration
Subscriber	Hardware	Software Version	FPGA Version
LUID: 002 - [0a-00-3e-bb-01-04]	PMP 450i	CANOPY 14.0	080715 (DES, Sched, US/ETSI) P1
<input style="float: left; margin-right: 10px;" type="button" value="Previous"/> <input style="float: right;" type="button" value="Next"/>			

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

To access any one of the SMs, click PMP450i SM hyperlink, as shown in [Figure 73](#).

Figure 73 AP Remote Subscribers page

Home → Remote Subscribers

5.4GHz MIMO OFDM - Access Point - 0a-00-3e-bb-00-fb



Monitoring the Link

Link monitoring procedure

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

To monitor the link for performance, follow these instructions:

Procedure 21 Monitoring the AP-SM link

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

Figure 74 Session Status page

Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-bb-01-04] No Site Name	PMP 450i	CANOPY 14.0	080715 (DES, Sched, US/ETSI) P13	IN SESSION (Encrypt Disabled)

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

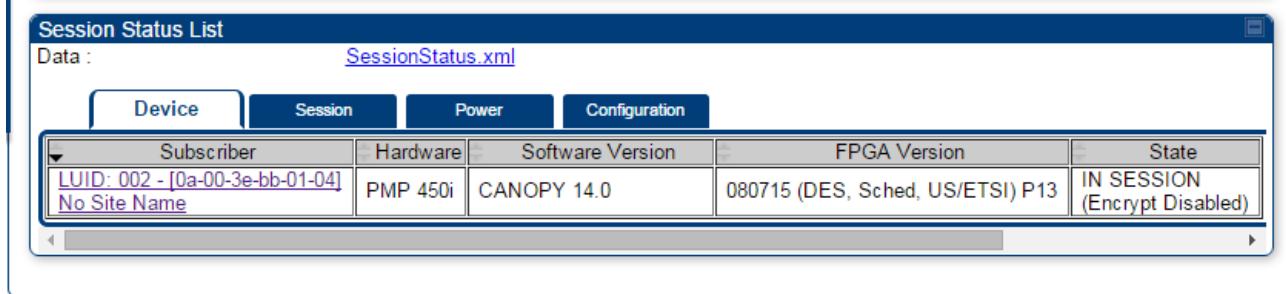
- **Session Count:** This field displays how many sessions the SM/BHS has had with the AP/BHM. Typically, this is the sum of Reg Count and Re-Reg Count. However, the result of internal calculation may display here as a value that slightly differs from the sum.
 - **Reg Count:** When a SM/BHS makes a registration request, the AP/BHM checks its local data to see whether it considers the SM/BHS to be already registered. If the AP/BHM concludes that the SM/BHS is not, then the request increments the value of this field.
 - Typically, a Re-Reg is the case where both
 - SM/BHS attempts to reregister for having lost communication with the AP/BHM.
 - AP/BHM has not yet observed the link to the SM/BHS as being down.
- 6 Click **Power** tab of Session Status list to display Downlink Rate, AP Tx Power (dBm), Signal Strength Radio (dB) and Signal to Noise Radio (dB).
- 7 Click **Configuration** tab of Session Status list to get QoS configuration details:
- Sustained Data Rate (kbps)
 - Burst Allocation (kbit)
 - Max Burst Rate (kbit)
 - Low Priority CIR (kbps)
- 8 Briefly monitor these values, occasionally refreshing this page by clicking another tab and then the Session Status tab again.
- 9 If these values are low (for example, 1, 1, and 0, respectively, meaning that the SM/BHS registered and started a stable session once) and are not changing:
 - Consider the installation successful.
 - Monitor these values from the network office over the next several hours and days.If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, Use **Receive Power Level** for aiming and then use Link Tests to confirm alignment).

Refer [Viewing Session Status](#) on page 9-14 for more details.

Exporting Session Status page of AP/BHM

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

Figure 75 Exporting Session Status page of the AP



Subscriber	Hardware	Software Version	FPGA Version	State
LUID: 002 - [0a-00-3e-bb-01-04] No Site Name	PMP 450i	CANOPY 14.0	080715 (DES, Sched, US/ETSI) P13	IN SESSION (Encrypt Disabled)

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

Export from command line

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

Wget

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

Configuring quality of service

Maximum Information Rate (MIR) Parameters

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

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

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

Token Bucket Algorithm

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

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

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

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

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

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

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in [Figure 76](#).



Note

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

Figure 76 Uplink and downlink rate caps adjusted to apply aggregate cap

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

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

For example, in the SM, if you set the **Sustained Uplink Data Rate** parameter to 2,000 kbps and the **Sustained Downlink Data Rate** parameter to 10,000 kbps, then the uplink and downlink MIR that is enforced for the SM can be calculated as shown in [Figure 77](#).

Figure 77 Uplink and downlink rate cap adjustment example

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

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

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

Committed Information Rate (CIR)

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

CIR parameters may be configured in the following ways:

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

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

Bandwidth from the SM Perspective

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

Interaction of Burst Allocation and Sustained Data Rate Settings

If the Burst Allocation is set to 1200 kb and the Sustained Data Rate is set to 128 kbps, a data burst of 1000 kb is transmitted at full speed because the Burst Allocation is set high enough. After the burst, the bucket experiences a significant refill at the Sustained Data Rate. This configuration uses the advantage of the settable Burst Allocation.

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

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

High-priority Bandwidth

To support low-latency traffic such as VoIP (Voice over IP) or video, the system implements a high-priority channel. This channel does not affect the inherent latencies in the system but allows high-priority traffic to be immediately served. The high-priority pipe separates low-latency traffic from traffic that is latency tolerant, such as standard web traffic and file downloads.

The number of channels available on the AP is reduced by the number of SMs configured for the high-priority channel (each SM operating with high-priority enabled uses two channels (virtual circuits) instead of one).

A module prioritizes traffic by

- reading the Low Latency bit (Bit 3) in the IPv4 Type of Service (ToS) byte in a received packet. Bit 3 is set by a device outside the system.
- reading the 802.1p field of the 802.1Q header in a received packet, where VLAN is enabled on the module.
- comparing the 6-bit Differentiated Services Code Point (DSCP) field in the ToS byte of a received packet to a corresponding value in the **Diffserv** tab of the Configuration page of the module. A packet contains no flag that indicates whether the encoding is for the Low Latency bit or the DSCP field. For this reason, you must ensure that all elements in your trusted domain, including routers and endpoints, set and read the ToS byte with the same scheme.

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

- The 6-bit length of the field allows it to specify one of 64 service differentiations.

- These correlate to 64 individual (**CodePoint**) parameters in the **Diffserv** tab of the Configuration page.
- Per RFC 2474, 3 of these 64 are preset and cannot be changed. (See <http://www.faqs.org/rfcs/rfc1902.html>.)
- For any or all of the remaining 61 CodePoint parameters, you can specify a value of
 - 0 through 3 for low-priority handling.
 - 4 through 7 for high-priority handling.

**Note**

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

An example of the **Diffserv** page in the Configuration menu and parameter descriptions are provided under [DiffServ attributes – AP/BHM](#) on page 7-61. This tab and its rules are identical from module type to module type. However, any of the 61 configurable Code Points can be set to a different value from module to module, thus defining unique per-hop behavior for some traffic.

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

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

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

Traffic Scheduling

The characteristics of traffic scheduling in a sector are summarized in [Table 108](#).

Table 109 Characteristics of traffic scheduling

Category	Factor	Treatment
Throughput	Aggregate throughput, less additional overhead	132 Mbps
Latency	Number of frames required for the scheduling process	1
	Round-trip latency	≈ 6 ms
	AP broadcast the download schedule	No
High-priority Channel	Allocation for <i>uplink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for <i>downlink</i> high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Order of transmission	CIR high-priority CIR low-priority Other high-priority Other low-priority



Caution

Power requirements affect the recommended maximums for power cord length feeding the CMM4. See the dedicated user guide that supports the CMM that you are deploying.

Packets that have a priority of 4 to 7 in either the DSCP or a VLAN 802.1p tag are automatically sent on the high-priority channel, but only where the high-priority channel is enabled.

Setting the Configuration Source

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

- all MIR settings:
 - Sustained Uplink Data Rate
 - Uplink Burst Allocation
 - Max Burst Uplink Data Rate
 - Sustained Downlink Data Rate
 - Downlink Burst Allocation
 - Max Burst Downlink Data Rate
- all CIR settings:
 - Low Priority Uplink CIR
 - Low Priority Downlink CIR
 - Hi Priority Uplink CIR
 - Hi Priority Downlink CIR
- all SM VLAN settings
 - Dynamic Learning
 - Allow Only Tagged Frames
 - VLAN Aging Timeout
 - Untagged Ingress VID
 - Management VID
 - VLAN Membership
- the Hi Priority Channel setting

Table 110 Recommended combined settings for typical operations

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

Table 111 Where feature values are obtained for a SM with authentication required

Configuration Source Setting in the AP	Values are obtained from		
	MIR Values	VLAN Values	High Priority Channel State
Authentication Server	Authentication Server	Authentication Server	Authentication Server
SM	SM	SM	SM
Authentication Server+SM	Authentication Server	Authentication Server, then SM	Authentication Server, then SM

**Note**

HPC represents the Hi Priority Channel (enable or disable).

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

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

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

For any SM whose **Authentication Mode** parameter is not set to 'Authentication Required', the listed settings are derived as shown in [Table 111](#).

Table 112 MIR, VLAN, HPC, and CIR Configuration Sources, Authentication Disabled

Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	VLAN Values	High Priority Channel State	CIR Values
Authentication Server	AP	AP	AP	AP
SM	SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM	SM

Configuring Quality of Service (QoS)

Quality of Service (QoS) page of AP

The QoS page of AP is explained in [Table 112](#).

Table 113 QoS page attributes - AP

AP Bandwidth Settings	
(Uplink + Downlink) Sustained Data Rate <= 100000 kbps	
Max Burst Uplink Data Rate :	0 (kbps) (Range: 0— 100000 kbps)
Sustained Uplink Data Rate :	50000 (kbps) (Range: 0— 100000 kbps)
Uplink Burst Allocation :	2500000 (kbits) (Range: 0— 2500000 kbits)
Max Burst Downlink Data Rate :	0 (kbps) (Range: 0— 100000 kbps)
Sustained Downlink Data Rate :	50000 (kbps) (Range: 0— 100000 kbps)
Downlink Burst Allocation :	2500000 (kbits) (Range: 0— 2500000 kbits)
Broadcast Downlink CIR :	200 (kbps) (Range: 0— 2333 kbps)
Priority Settings	
Priority Precedence :	802.1p Then DiffServ ▾
PPPoE Control Message Priority :	<input type="radio"/> High <input checked="" type="radio"/> Normal
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Attribute	Meaning
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 transmit more. When set to 0 (default), the burst rate is unlimited.
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 <ul style="list-style-type: none"> Maximum Information Rate (MIR) Parameters on page 7-153 Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 Configuration Source on page 7-71
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 7-153 <ul style="list-style-type: none"> Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 Configuration Source on page 7-71
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.
Sustained Downlink Data Rate	<p>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 7-153</p> <ul style="list-style-type: none"> • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 • Configuration Source on page 7-71
Downlink Burst Allocation	<p>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</p> <ul style="list-style-type: none"> • Maximum Information Rate (MIR) Parameters on page 7-153 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 • Configuration Source on page 7-71
Broadcast Downlink CIR	<p>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.</p> <p>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.</p>
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.

Quality of Service (QoS) page of SM

The QoS page of SM is explained in [Table 113](#).

Table 114 QoS page attributes - SM

MIR Bandwidth Settings	
(Uplink + Downlink) Sustained Data Rate <= 130000 kbps	
Sustained Uplink Data Rate :	50000 (kbps) (Range: 0— 130000 kbps)
Sustained Downlink Data Rate :	50000 (kbps) (Range: 0— 130000 kbps)
Uplink Burst Allocation :	2500000 (kbytes) (Range: 0 — 2500000 kbytes)
Downlink Burst Allocation :	2500000 (kbytes) (Range: 0 — 2500000 kbytes)
Max Burst Uplink Data Rate :	0 (kbps) (Range: 0— 130000 kbps)
Max Burst Downlink Data Rate :	0 (kbps) (Range: 0— 130000 kbps)
Enable Broadcast/ Multicast Data Rate :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Broadcast/ Multicast Uplink Data Rate :	Kbps ▼ 130000 (Range: 1— 130000 kbps/65535 pps)
Priority Settings	
(Uplink + Downlink)(Low Priority + High Priority) CIR Data Rate <= 65534 kbps	
Low Priority Uplink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Low Priority Downlink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Hi Priority Channel :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Hi Priority Uplink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Hi Priority Downlink CIR :	0 (kbps) (Range: 0— 65534 kbps)
Priority Precedence :	802.1p Then DiffServ ▼
PPPoE Control Message Priority :	<input type="radio"/> High <input checked="" type="radio"/> Normal
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Attribute	Meaning
Sustained Uplink Data Rate	<p>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 7-153</p> <ul style="list-style-type: none"> • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 • Configuration Source on page 7-71
Sustained Downlink Data Rate	<p>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 7-153</p> <ul style="list-style-type: none"> • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 • Configuration Source on page 7-71
Uplink Burst Allocation	<p>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 7-153</p> <ul style="list-style-type: none"> • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-155 • Configuration Source on page 7-71
Downlink Burst Allocation	<p>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</p>

with transmission credits. See [Maximum Information Rate \(MIR\) Parameters](#) on page 7-153

- [Interaction of Burst Allocation and Sustained Data Rate Settings](#) on page 7-155
- [Configuration Source](#) on page 7-71

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.
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.
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.
Low Priority Uplink CIR	<p>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).</p> <ul style="list-style-type: none"> • Committed Information Rate (CIR) on page 7-154 • Setting the Configuration Source on page 7-158
Low Priority Downlink CIR	<p>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).</p> <ul style="list-style-type: none"> • Committed Information Rate (CIR) on page 7-154 • Setting the Configuration Source on page 7-158
Hi Priority Channel	<p>See</p> <ul style="list-style-type: none"> • High-priority Bandwidth on page 7-155 • Configuration Source on page 7-71
Hi Priority Uplink CIR	<p>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).</p> <ul style="list-style-type: none"> • Committed Information Rate (CIR) on page 7-154 • Setting the Configuration Source on page 7-158
Hi Priority Downlink CIR	<p>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).</p> <ul style="list-style-type: none"> • Committed Information Rate (CIR) on page 7-154 • Setting the Configuration Source on page 7-158

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.

Quality of Service (QoS) page of BHM

The QoS page of BHM is explained in [Table 114](#).

Table 115 QoS page attributes - BHM

Priority Settings	
Priority Precedence :	<input type="button" value="802.1p Then DiffServ ▾"/>
PPPoE Control Message Priority :	<input checked="" type="radio"/> High <input checked="" type="radio"/> Normal
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
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 115](#).

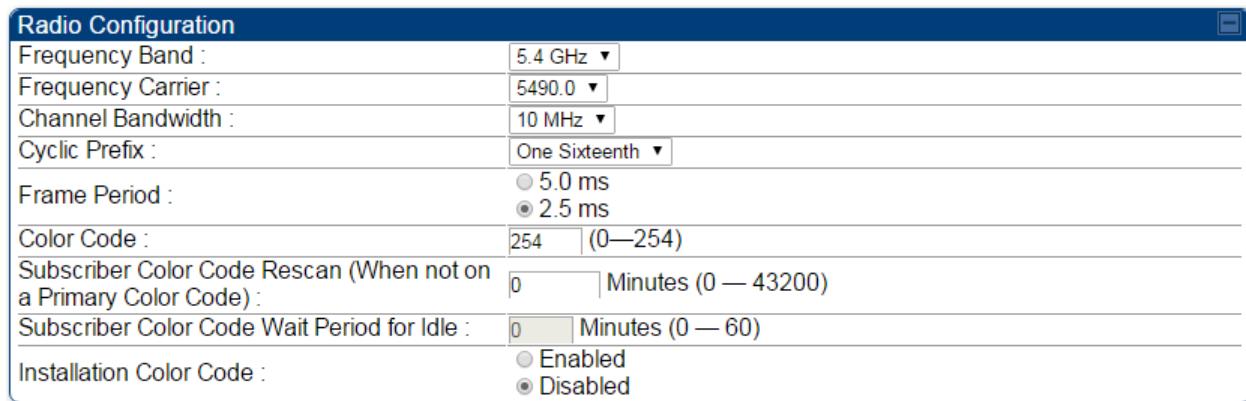
Table 116 QoS page attributes - BHS

Priority Settings	
Attribute	Meaning
Priority Precedence :	802.1p Then DiffServ ▾
PPPoE Control Message Priority :	<input type="radio"/> High <input checked="" type="radio"/> Normal
Prioritize TCP ACK :	<input checked="" type="radio"/> Enabled <input type="radio"/> 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 78 Installation Color Code - AP



The screenshot shows the 'Radio Configuration' window with the following settings:

Frequency Band :	5.4 GHz
Frequency Carrier :	5490.0
Channel Bandwidth :	10 MHz
Cyclic Prefix :	One Sixteenth
Frame Period :	<input checked="" type="radio"/> 5.0 ms <input type="radio"/> 2.5 ms
Color Code :	254 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

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 7-168.

Configuration Steps

Procedure 22 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 one 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 13.3 (Build 15) 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.

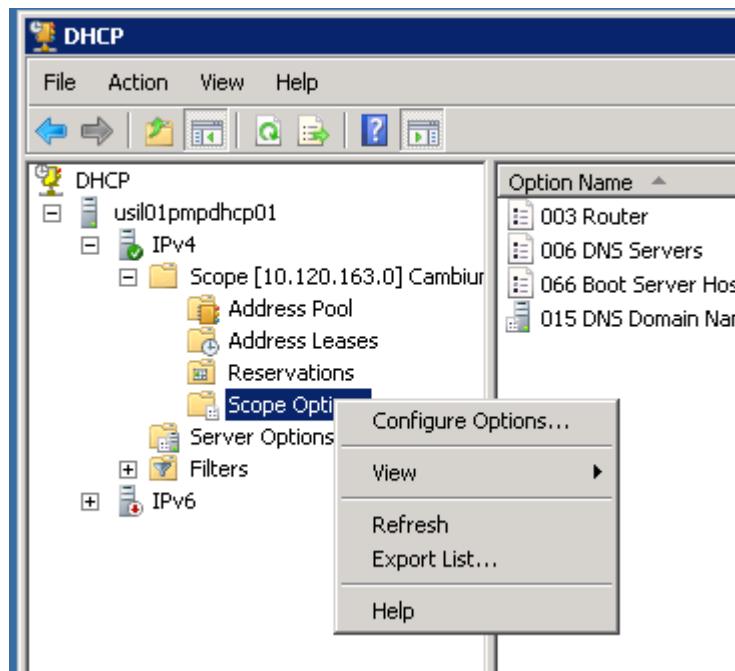
DHCP server configuration

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

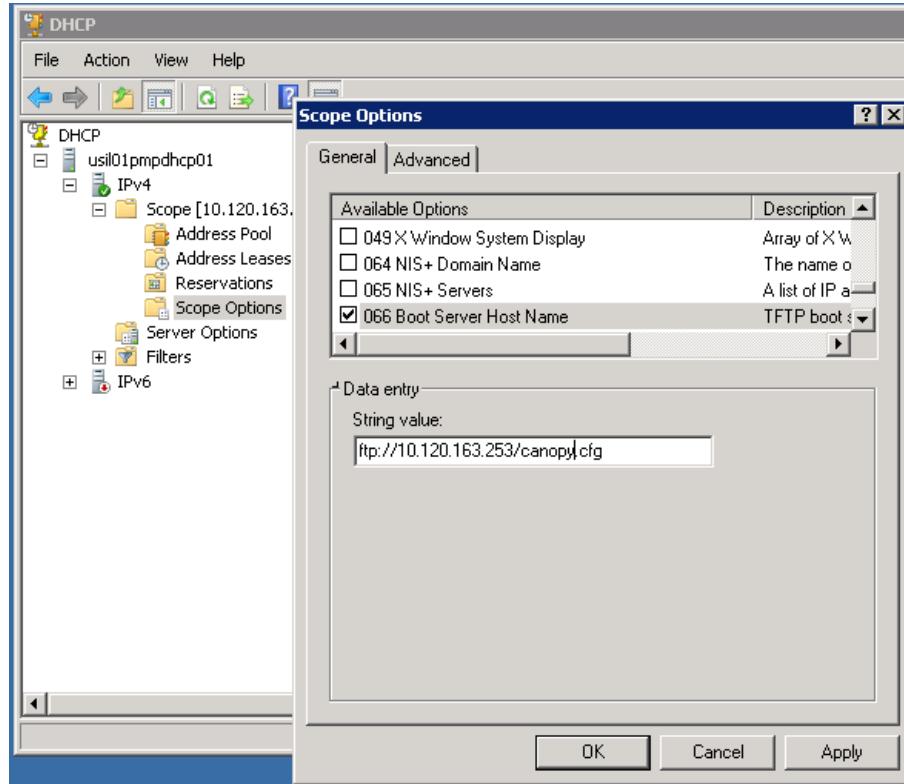
The following example explains how to make the change for Windows Server 2008. Adapt it to your specific DHCP server.

Procedure 23 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.

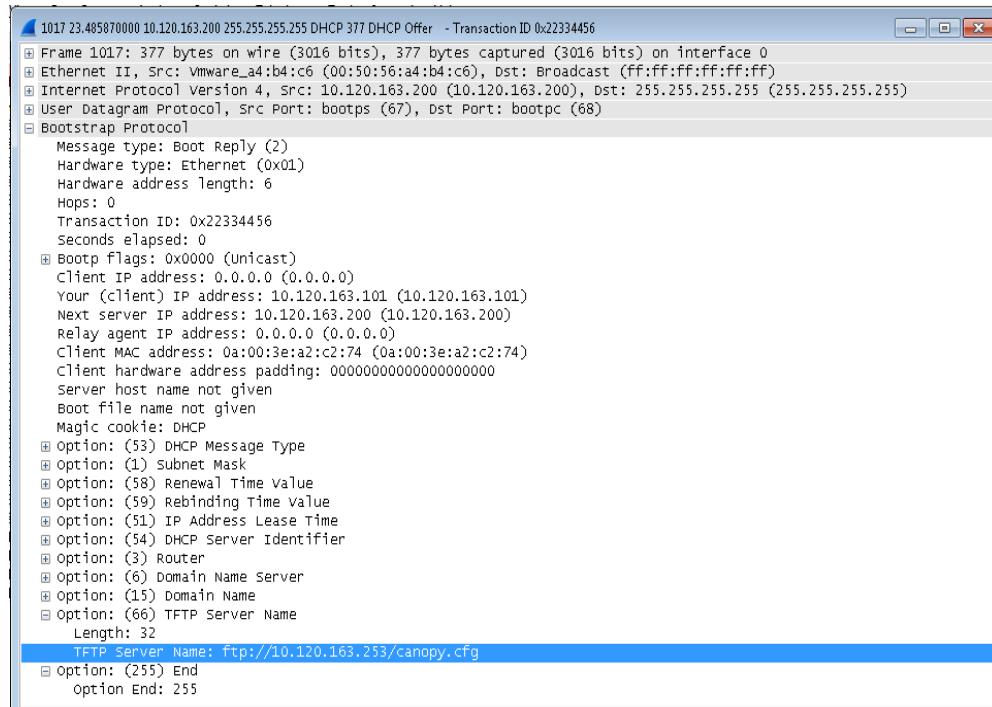
For example:

<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 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 PMP/PTP 450i 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.

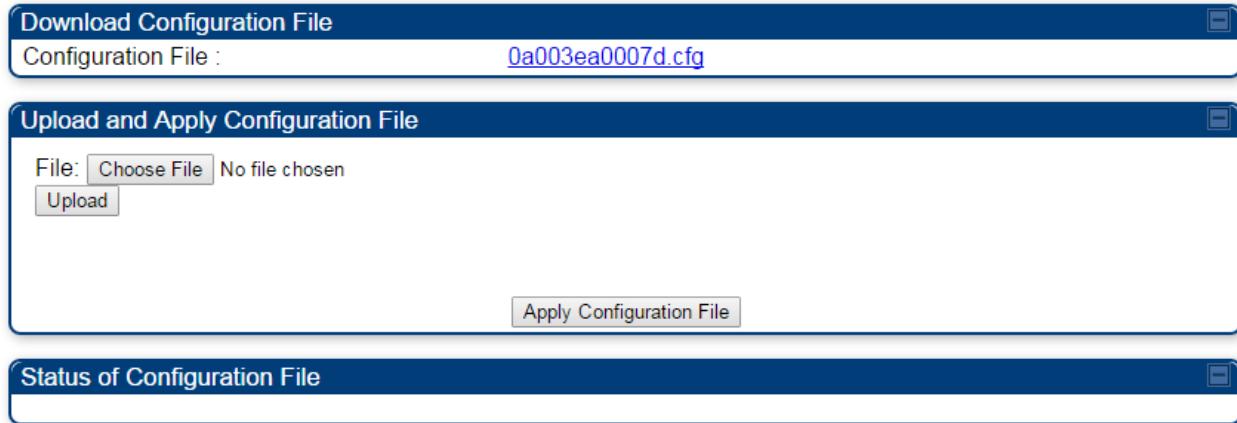
The exported configuration file contains the complete configuration including all the default values. To keep a backup of the current configuration, the file can be saved as-is and imported later.

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 7-174).

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 79 Configuration File upload and download page



The DHCP server configuration procedure is as follows:

Procedure 24 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 25 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 26 Special Headers for configuration file

- 1 A "configFileParameters" section can be added to the header to control the behaviour of the device when importing configuration.
- 2 The "**setToDefaults**" when set to "true" tell the device to reset to factory default configuration and apply the configuration in the file on top of that. So any attribute not in the configuration file will be set to its factory default value. By default, the configuration in the file is merged with the existing configuration on the device.
The "**rebootIfRequired**" flag when set to "true" tell the device to reboot automatically if needed to apply the configuration change. By default, the device will not reboot automatically.

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

Configuring a RADIUS server

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

Understanding RADIUS for PMP 450i

PMP 450i 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), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when a SM registers to an AP.
- **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



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 117 Security tab attributes

Authentication Server Settings	
Authentication Mode :	<input type="button" value="Disabled"/>
Authentication Server DNS Usage :	<input type="radio"/> Append DNS Domain Name <input checked="" type="radio"/> Disable DNS Domain Name
Authentication Server 1 : Shared Secret 10.120.226.6
Authentication Server 2 : Shared Secret 0.0.0.0
Authentication Server 3 : Shared Secret 0.0.0.0
Authentication Server 4 (BAM ONLY) :	0.0.0.0
Authentication Server 5 (BAM ONLY) :	0.0.0.0
Radius Port :	1812 <i>Default port number is 1812</i>
Authentication Key :	(Using All 0xFF's Key)
Select Key :	<input type="radio"/> Use Key above <input checked="" type="radio"/> Use Default Key
Airlink Security	
Encryption Setting :	<input type="button" value="None"/>
AP Evaluation Configuration	
SM Display of AP Evaluation Data :	<input type="radio"/> Disable Display <input checked="" type="radio"/> Enable Display
Session Timeout	
Web, Telnet, FTP Session Timeout :	3600 Seconds
IP Access Filtering	
IP Access Control :	<input type="radio"/> IP Access Filtering Enabled - Only allow access from IP addresses specified below <input checked="" type="radio"/> IP Access Filtering Disabled - Allow access from all IP addresses
Allowed Source IP 1 :	0.0.0.0 /32 Network Mask (set to 32 to disable)
Allowed Source IP 2 :	0.0.0.0 /32 Network Mask (set to 32 to disable)
Allowed Source IP 3 :	0.0.0.0 /32 Network Mask (set to 32 to disable)
Security Mode	
Web Access :	<input type="button" value="HTTP Only"/>
SNMP :	<input type="button" value="SNMPv3 Only"/>
Telnet :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
FTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TFTP :	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Attribute	Meaning

Authentication Mode	<p>Operators may use this field to select the following authentication modes:</p> <p>Disabled—the AP requires no SMs to authenticate.</p> <p>Authentication Server —the AP requires any SM that attempts registration to be authenticated in Wireless Manager before registration.</p> <p>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.</p> <p>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.</p>
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	
Authentication Server 2	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 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 0xFFFFFFFFFFFFFFFFFFFFFFF.
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	<p>Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs.</p> <p>None provides no encryption on the air link.</p> <p>DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect the performance or throughput of the system.</p> <p>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 than DES. AES products are certified as compliant with the Federal Information Processing Standards (FIPS 197) in the U.S.A.</p>
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	<p>The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list:</p> <ul style="list-style-type: none"> • HTTP Only – provides non-secured web access. The radio to be accessed via <code>http://<IP of Radio></code>. • HTTPs Only – provides a secured web access. The radio to be accessed via <code>https1://<IP of Radio></code>. • 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 : <ul style="list-style-type: none">• 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 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.

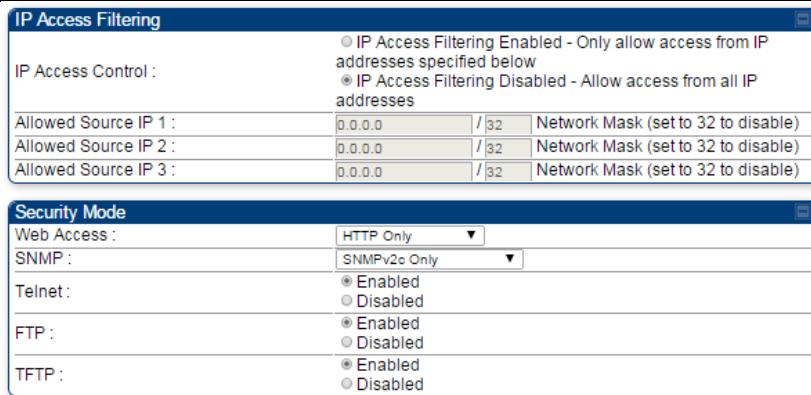


Note

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 118 SM Security tab attributes

Authentication Key Settings	
Authentication Key : <input type="text" value=""/> (Using All 0xFF's Key) Select Key : <input type="radio"/> Use Key above <input checked="" type="radio"/> Use Default Key	
AAA Authentication Settings	
Enforce Authentication : <input type="button" value="Disable"/> <input type="button" value="Enable"/> Phase 1 : <input type="button" value="eapTLS"/> <input type="button" value="WPA2PSK"/> Phase 2 : <input type="button" value="MSCHAPv2"/> <input type="button" value="PEAP"/> Identity/Realm : <input type="radio"/> Enable Realm <input checked="" type="radio"/> Disable Realm Identity [anonymous] @ Realm <input type="text" value="canopy.net"/> Username : <input type="text" value="0a-00-3e-a0-00-6c"/> <input type="button" value="Use Default Username"/> Password : <input type="password" value="*****"/> Confirm Password : <input type="password"/>	
RADIUS Certificate Settings	
Upload Certificate File File: <input type="button" value="Choose File"/> No file chosen <input type="button" value="Import Certificate"/> <input type="button" value="Use Default Certificates"/> <i>This will delete all current certificates</i>	
Certificate 1	
C =US S =Illinois O = Canopy Solutions, Inc. OU =Canopy Wireless Broadband CN =Canopy AAA Server Demo CA E =technical-support@canopywireless.com Valid From: 01/01/2001 00:00:00 Valid To: 12/31/2049 23:59:59 <input <=""]="" td="" type="button" value="Delete"/>	
Certificate 2	
<i>Certificate 2 deleted.</i>	
Airlink Security	
Encryption Setting : <input type="button" value="DES"/> <input type="button" value="AES"/>	
Session Timeout	
Web, Telnet, FTP Session Timeout : <input type="text" value="600000"/> Seconds	
SM Management Interface Access via Ethernet Port	
Ethernet Access : <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	



Attribute	Meaning
Authentication Key	The authentication key is a 32-character hexadecimal string used when Authentication Mode is set to AP PreShared Key . By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFF.
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 EAPTLS (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.
Username	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.
Password	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.
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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Encryption Setting	<p>Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs.</p> <p>None provides no encryption on the air link.</p> <p>DES (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of</p>

data. DES encryption does not affect the performance or throughput of the system.

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 than DES. 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	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	
Allowed Source IP 3	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: <ul style="list-style-type: none"> • HTTP Only – provides non-secured web access. The radio to be accessed via <code>http://<IP of Radio></code>. • HTTPs Only – provides a secured web access. The radio to be accessed via <code>https://<IP of Radio></code>. • HTTP and HTTPs – If enabled, the radio can be accessed via both <code>http</code> and <code>https</code>.
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 **eapTLS** (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 (**eapTLS** 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 **eapTLS** 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 80 SM Certificate Management

Configuring RADIUS servers for SM authentication

Your RADIUS server must be configured to use the following:

- EAPTLS 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 are 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 is *not* 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 are 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 118](#). 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 118](#)).

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 118](#)). 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 119 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Required	Value
MS-MPPE-Send-Key ¹	26.311.16	-	Y	-
-	-	-	-	-
MS-MPPE-Recv-Key ²	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 > Hi Priority Uplink CIR				0 kbps 32 bits
Cambium-Canopy-HPDLCIR	26.161.4	integer	N	0-65535 kbps
Configuration > Quality of Service > Hi Priority Uplink CIR				0 kbps 32 bits
Cambium-Canopy-HPENABLE	26.161.5	integer	N	0-disable, 1-enable

¹ Contains key for encrypting packets sent by the NAS to the remote host (for Microsoft Point-to-Point Encryption Protocol)

² Contains key for encrypting packets received by the NAS from the remote host (for Microsoft Point-to-Point Encryption Protocol)

Configuration > Quality of Service > Hi 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
Configuration > Quality of Service > Uplink Burst Allocation	dependent on radio feature set	32 bits
Cambium-Canopy-DLBR	26.161.8	integer N
Configuration > Quality of Service > Sustained Downlink Data Rate	dependent on radio feature set	32 bits
Cambium-Canopy-DLBL	26.161.9	integer N
Configuration > Quality of Service > Downlink Burst Allocation	dependent on radio feature set	32 bits
Cambium-Canopy- VLLEARNEN	26.161.14	integer N
Configuration > VLAN > Dynamic Learning	1	32 bits
Cambium-Canopy- VLFRAMES	26.161.15	integer N
Configuration > VLAN > Allow Frame Types	0	32 bits
Cambium-Canopy-VLIDSET	26.161.16	integer N
Configuration > VLAN Membership	0	32 bits
Cambium-Canopy-VLAGETO	26.161.20	integer N
Configuration > VLAN > VLAN Aging Timeout	25 mins	32 bits
Cambium-Canopy-VLIGVID	26.161.21	integer N
Configuration > VLAN > Default Port VID	1	32 bits
Cambium-Canopy-VLMGVID	26.161.22	integer N
Configuration > VLAN > Management VID	1	32 bits
Cambium-Canopy- VLSMMGPASS	26.161.23	integer N
Configuration > VLAN > SM Management VID Pass-through	1	32 bits
Cambium-Canopy-BCASTMIR	26.161.24	integer N
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



Note

VSA numbering:

26 connotes Vendor Specific Attribute, per RFC 2865

26.311 is Microsoft Vendor Code, per IANA

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 27 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.

Figure 81 User Authentication and Access Tracking tab of the AP

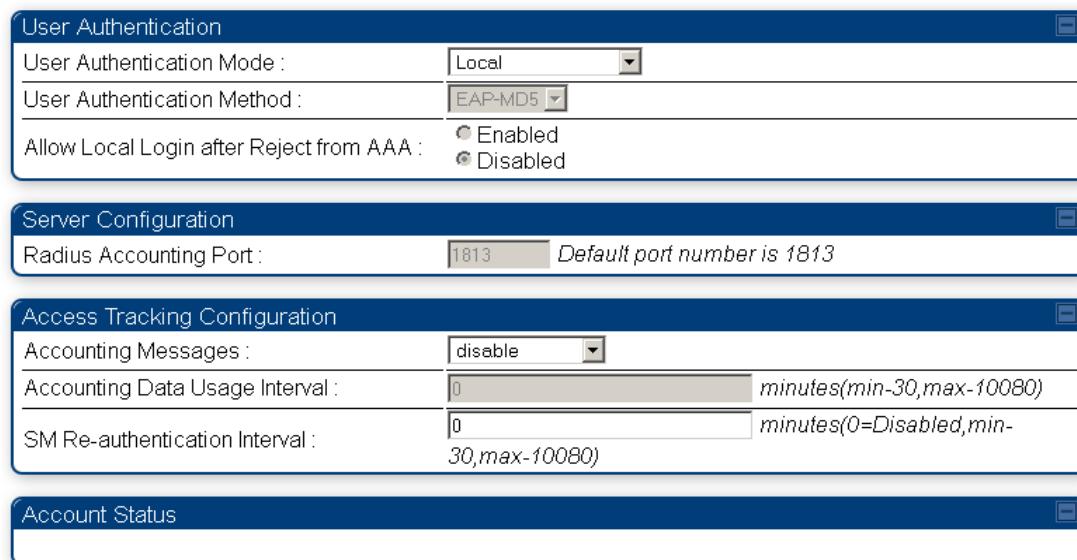


Table 120 AP User Authentication and Access Tracking attributes

The screenshot shows a configuration interface for a RADIUS server. It consists of four panels:

- User Authentication:** Set to Local and EAP-MD5.
- Server Configuration:** Radius Accounting Port is set to 1813 (Default port number is 1813).
- Access Tracking Configuration:** Accounting Messages are set to disable, Accounting Data Usage Interval is 0 minutes, and SM Re-authentication Interval is 0 minutes (0=Disabled, min-30, max-10080).
- Account Status:** This panel is currently empty.

Attribute	Meaning
User Authentication Mode	<ul style="list-style-type: none"> 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 is EAP-MD5.
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.
Radius Accounting Port	The destination port on the AAA server used for Radius accounting communication.
Accounting Messages	<p>disable – no accounting messages are sent to the RADIUS server</p> <p>deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 121).</p> <p>dataUsage – accounting messages are sent to the RADIUS server regarding data usage (see Table 121).</p>
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.
-------------------------------	--

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 [7-193](#) 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 82 User Authentication and Access Tracking tab of the SM

The screenshot shows the User Authentication and Access Tracking tab of the SM configuration interface. It is divided into three main sections: User Authentication, Access Tracking Configuration, and Account Status.

User Authentication: A note states: "Remote Login is enabled only when SM is Registered with an AP and the system is operating with a back-end AAA server. The SM will only do Local Login until these preconditions are met regardless of configuration settings on this page." The "Current State: OOSERVICE" is shown. Under "User Authentication Mode:", a dropdown menu is set to "Local". Under "Allow Local Login after Reject from AAA:", the "Disabled" radio button is selected.

Access Tracking Configuration: The "Accounting Messages:" dropdown is set to "disable".

Account Status: This section is currently empty.

Table 121 SM User Authentication and Access Tracking attributes

User Authentication	
<p><i>Remote Login is enabled only when SM is Registered with an AP and the system is operating with a back-end AAA server. The SM will only do Local Login until these preconditions are met regardless of configuration settings on this page.</i></p> <p>Current State: OOSERVICE</p>	
User Authentication Mode :	Local
Allow Local Login after Reject from AAA :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Access Tracking Configuration	
Accounting Messages :	disable
Account Status	
Attribute	Meaning
User Authentication Mode	<ul style="list-style-type: none"> 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 ".
Accounting Messages	<p> Note</p> <p>When the radio User Authentication Mode is set to "Local" or "Remote", the Allow Local Login after Reject from AAA does not any effect.</p> <ul style="list-style-type: none"> disable – no accounting messages are sent to the RADIUS server deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 121).

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 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 122 Device data accounting RADIUS attributes

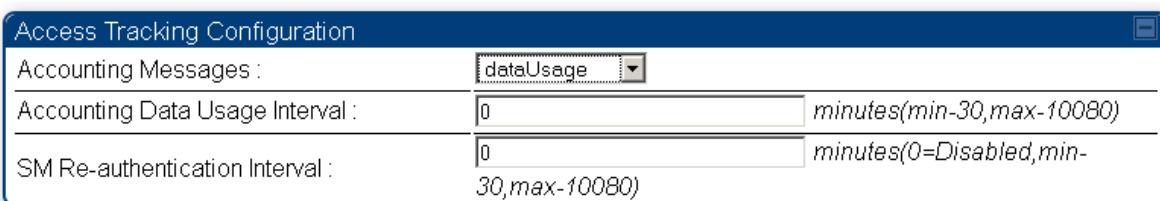
Sender	Message	Attribute	Value	Description
AP	Accounting-Request	Acct-Status-Type	1 - Start	This message is sent every time a SM registers with an AP, and after the SM stats are cleared.
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
	Event-Timestamp	Event-Timestamp	UTC time the event occurred on the AP	This message is sent every time a SM becomes unregistered with an AP, and when the SM stats are cleared.
		Acct-Status-Type	2 - Stop	
AP	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.	Sum of the input octets received at the SM over regular data VC and the high priority data VC (if enabled). Will not include broadcast.
		Acct-Input-Octets	Sum of the output octets sent from the SM over regular data VC and the high priority data VC (if enabled).	
	Acct-Output-Octets	Acct-Output-Octets	Sum of the output octets sent from the SM over regular data VC and the high priority data VC (if enabled).	This message is sent every time a SM becomes unregistered with an AP, and when the SM stats are cleared.
		Acct-Output-Octets	Sum of the output octets sent from the SM over regular data VC and the high priority data VC (if enabled).	

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-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).	
		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.
		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 regular data VC and the high priority data VC (if enabled). Will not include broadcast.	Interim update counts are cumulative over the course of the session
		Acct-Output-Octets	Sum of the output octets sent from the SM over regular data VC and the high priority data VC (if enabled).	

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 83 RADIUS accounting messages configuration



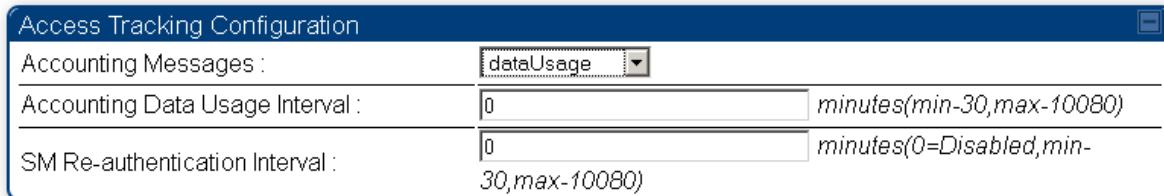
The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify 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 450i 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 84 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.

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 on page 8-2](#)
- [Using the Alignment Tool on page 8-13](#)
- [Using the Link Capacity Test tool on page 8-19](#)
- [Using AP Evaluation tool on page 8-22](#)
- [Using BHM Evaluation tool on page 8-26](#)
- [Using the OFDM Frame Calculator tool on page 8-30](#)
- [Using the Subscriber Configuration tool on page 8-34](#)
- [Using the Link Status tool on page 8-35](#)
- [Using BER Results tool on page 8-38](#)
- [Using the Sessions tool on page 8-39](#)

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 the amount of 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

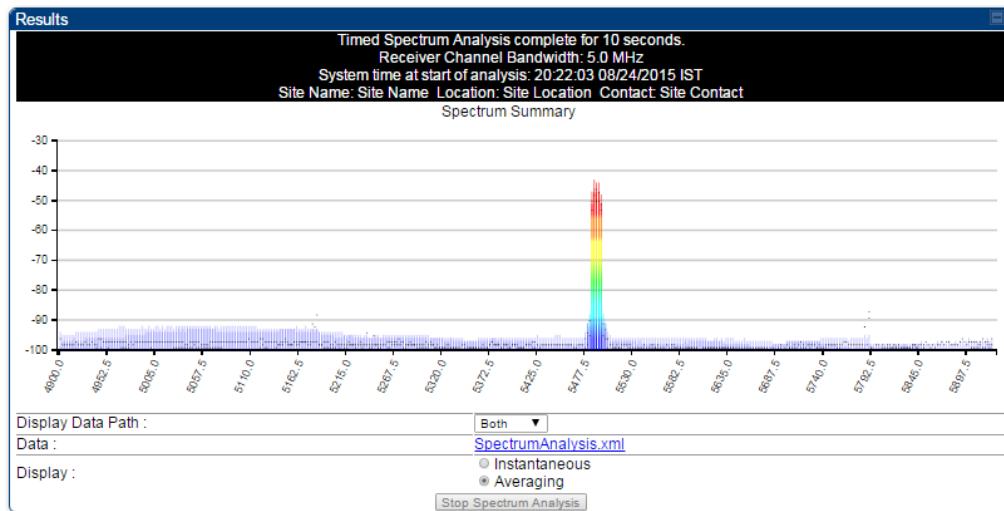
Analyzing the spectrum

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

Procedure 28 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** 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 85 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 find 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 85](#).

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 122](#).

Table 123 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	<p>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.</p> <p>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.</p>
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.
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.

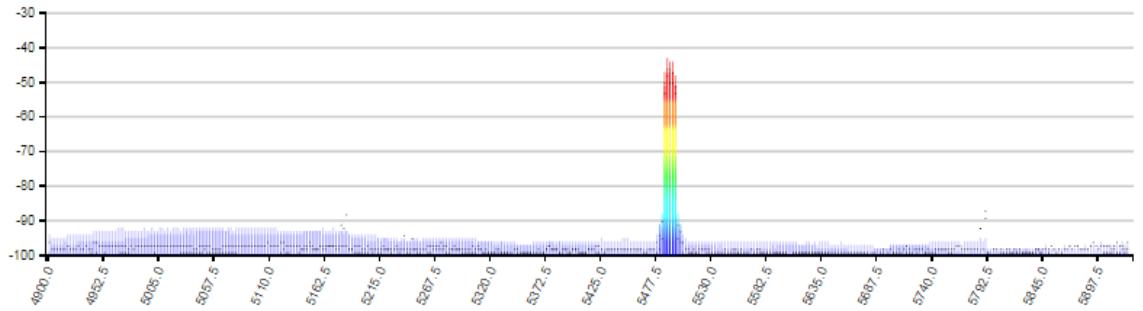
Continuous Spectrum Analyzer

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 123](#).

Table 124 Spectrum Analyzer page attributes - SM

Attribute	Meaning
Results	<p>Timed Spectrum Analysis complete for 10 seconds. Receiver Channel Bandwidth: 5.0 MHz System time at start of analysis: 20:22:03 08/24/2015 IST Site Name: Site Name Location: Site Location Contact Site Contact</p> <p>Spectrum Summary</p>  <p>Display Data Path : Both Data : SpectrumAnalysis.xml Display : <input type="radio"/> Instantaneous <input checked="" type="radio"/> Averaging Stop Spectrum Analysis</p>
Min And Max Frequencies	<p>Min and Max Frequencies in KHz : <input type="text" value="4900000"/> <input type="text" value="5925000"/> (Valid Range in KHz: 4900000 - 5925000) Set Min And Max To Full Scan</p>
Subscriber Module Stats	<p>Session Status : REGISTERED VC 18 Rate 8X/8X MIMO-B Registered AP : 0a-00-3e-bb-00-fb Site Name</p>
Spectrum Analyzer Options	<p>Scanning Bandwidth : 5.0 MHz</p>
Timed Spectrum Analyzer	<p>Duration : <input type="text" value="10"/> Seconds (10—1000) <input type="radio"/> Enable <input checked="" type="radio"/> Disable Start Timed Spectrum Analysis</p>
Continuous Spectrum Analyzer	<p>Start Continuous Spectrum Analysis</p> <p>Note: Continuous Spectrum Analysis has a max of 24 hours and afterwards will automatically resume scanning for APs.</p>

Display Data Path	Refer Table 122 on page 8-5
Data	Refer Table 122 on page 8-5
Display	Refer Table 122 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.
Registered SM Count	Refer Table 122 on page 8-5
Maximum Count to Registered SMs	Refer Table 122 on page 8-5
Duration	Refer Table 122 on page 8-5

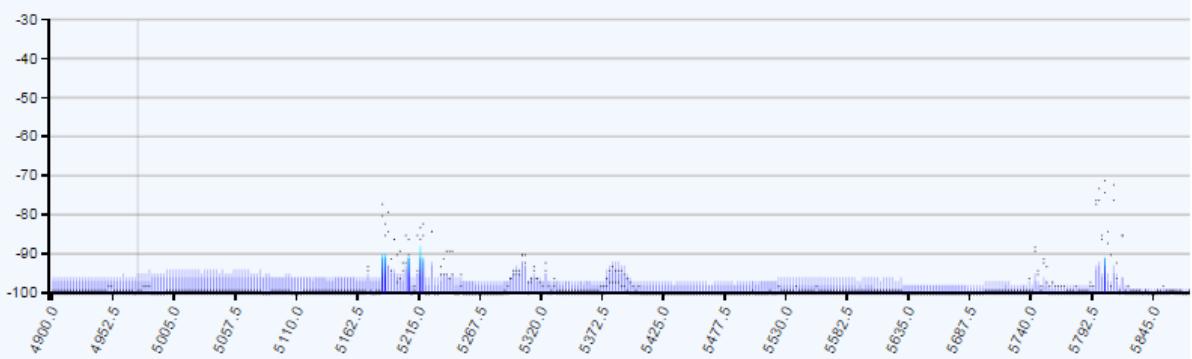
Spectrum Analyzer page of BHM

The Spectrum Analyzer page of BHM is explained in [Table 124](#).

Table 125 Spectrum Analyzer page attributes - BHM

Results

Sector Spectrum Analysis complete for 50 seconds.
 Receiver Channel Bandwidth: 10.0 MHz
 System time at start of analysis: 18:24:51 08/25/2015 IST
 Site Name: No Site Name Location: No Site Location Contact: No Site Contact
 Spectrum Summary -97dBm @ 4972.5MHz V [max: -100, mean: -97]



Display Data Path : Both
 Data : [SpectrumAnalysis.xml](#)
 Display : Instantaneous Averaging
[Stop Spectrum Analysis](#)

Min And Max Frequencies
 Min and Max Frequencies in KHz : 4900000 | 5925000 | (Valid Range in KHz: 4900000 - 5925000)
[Set Min And Max To Full Scan](#) [Set Min And Max To Center Scan +/-40MHz](#)

Backhaul Stats
 Timing Slave Status : Disconnected

Spectrum Analyzer Options
 BHS Scanning Bandwidth : 5.0 MHz
 Note: Only BHS changing channel bandwidth is currently supported. BHM will scan at current channel bandwidth

Timed Spectrum Analyzer
 Duration : 10 Seconds (10—1000)
[Start Timed Sector Spectrum Analysis](#)
 Note: BHM scans for extra 40 seconds

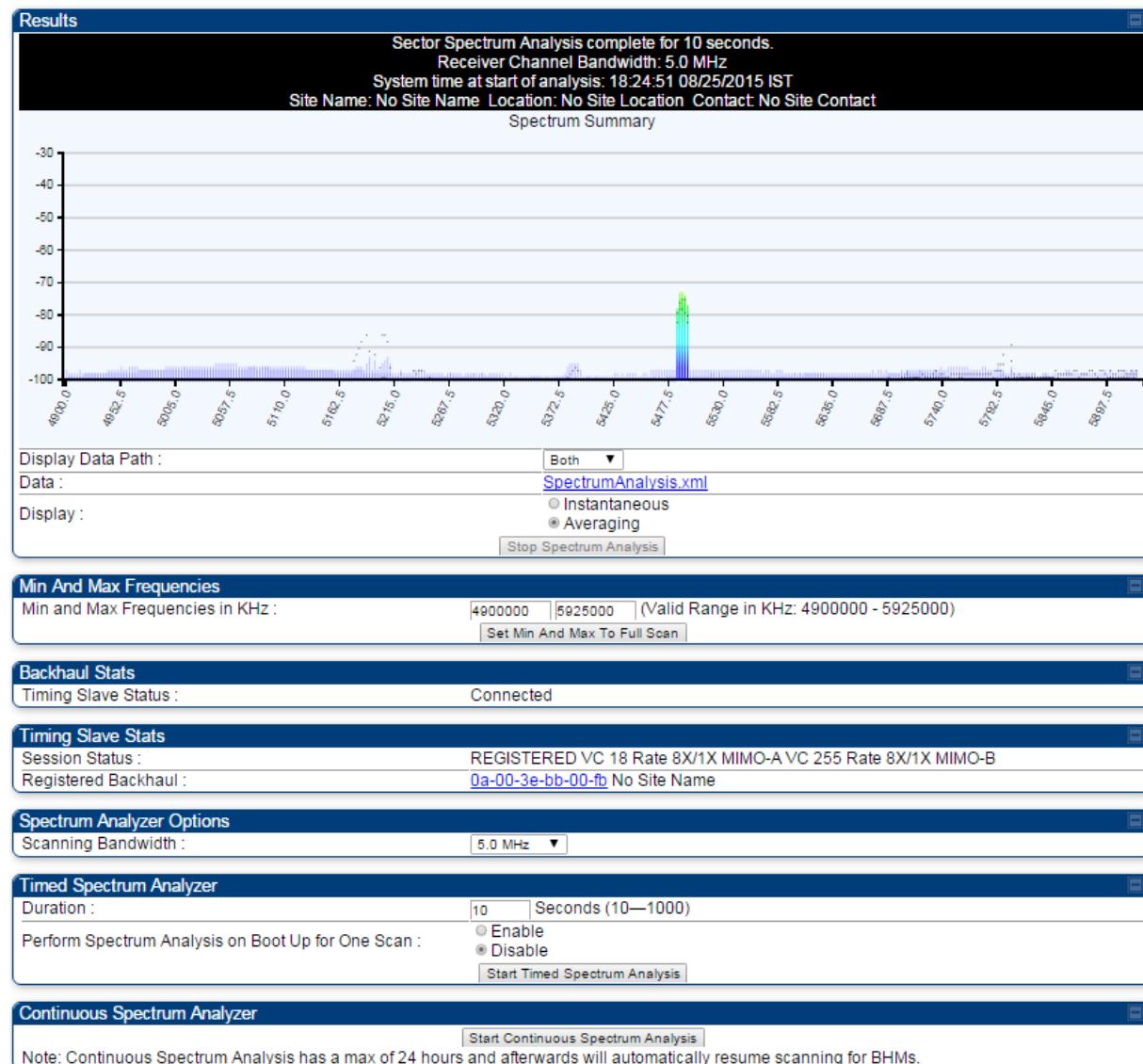
Continuous Spectrum Analyzer
[Start Continuous Spectrum Analysis](#)
 Note: Continuous Spectrum Analysis has a max of 24 hours and afterwards will automatically resume transmitting.

Attribute	Meaning
Data	Refer Table 122 on page 8-5
Display	Refer Table 122 on page 8-5
Duration	Refer Table 122 on page 8-5
Continuous Spectrum Analyzer	Refer Table 122 on page 8-5

Spectrum Analyzer page of BHS

The Spectrum Analyzer page of BHS is explained in [Table 125](#).

Table 126 Spectrum Analyzer page attributes - BHS



Attribute	Meaning
Data	Refer Table 122 on page 8-5
Display	Refer Table 122 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 122 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 122 on page 8-5

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 has to be selected from the drop-down list before launching **Start Remote Spectrum Analysis**.

Analyzing the spectrum remortly

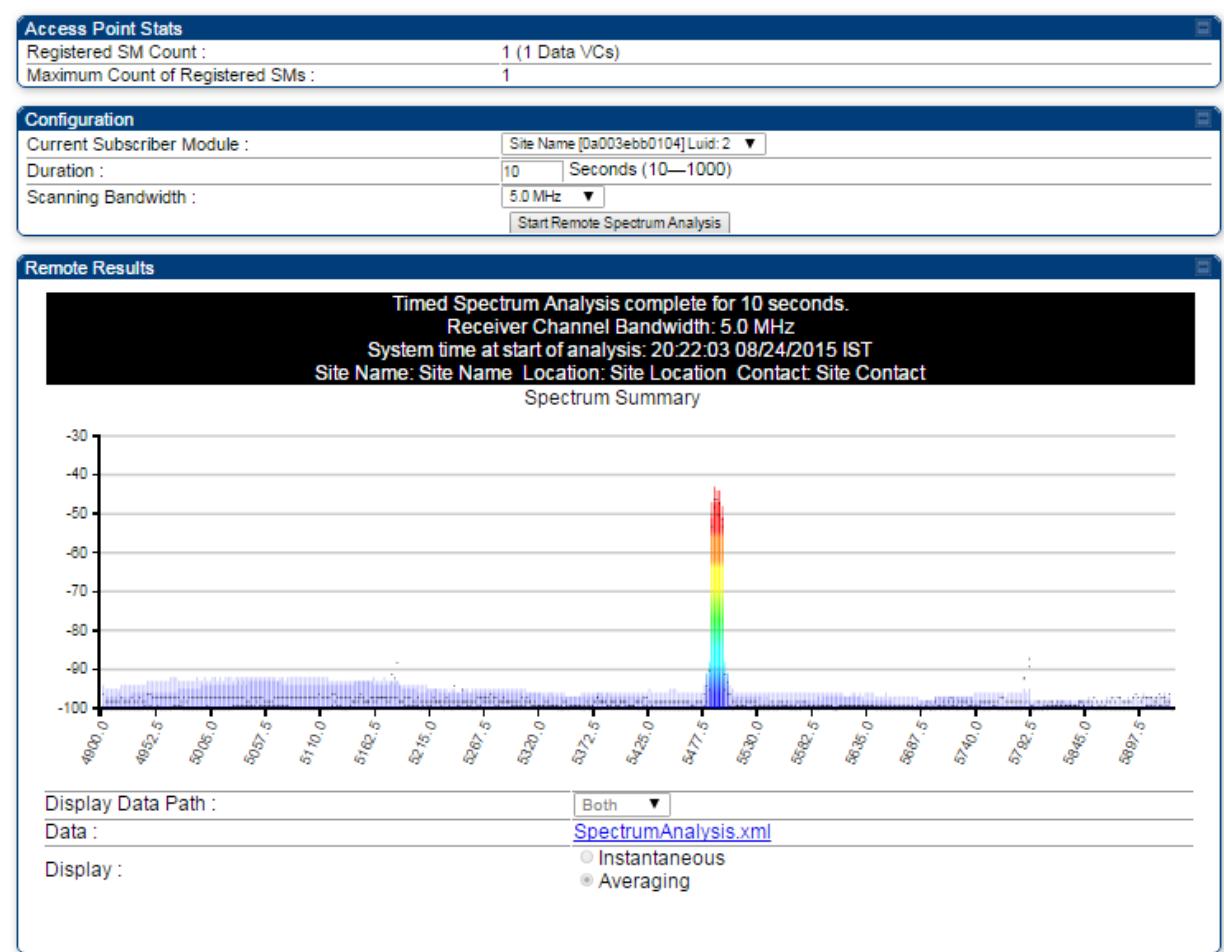
Procedure 29 Remote Spectrum Analyzer procedure

- 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 through the use of 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 `SpectrumAnalysis.xml` file.

Remote Spectrum Analyzer page of AP

The Remote Spectrum Analyzer page of AP is explained in [Table 126](#).

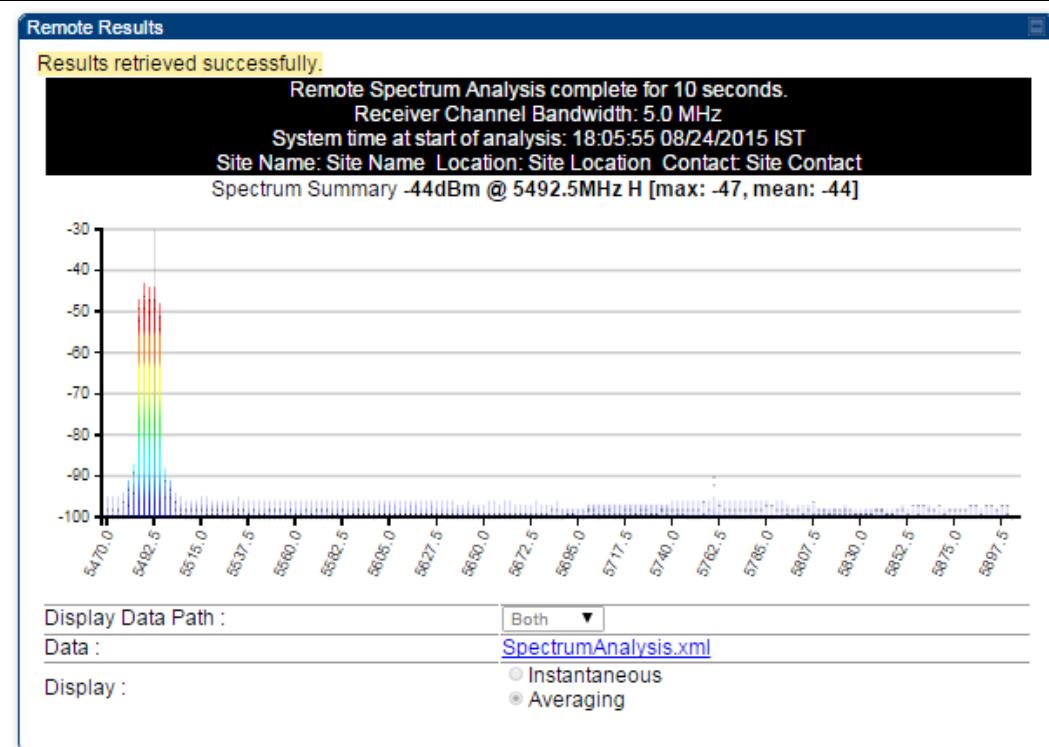
Table 127 Remote Spectrum Analyzer attributes - AP

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 127](#).

Table 128 Remote Spectrum Analyzer attributes - BHM



Attribute	Meaning
Duration	Refer Table 122 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 86 Alignment Tool tab of SM – Receive Power Level > -70 dBm

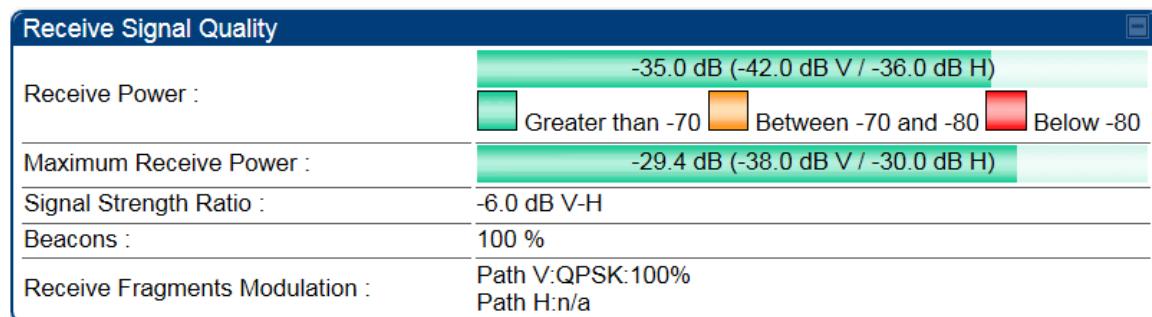


Figure 87 Alignment Tool tab of SM – Receive Power Level between -70 to -80 dBm

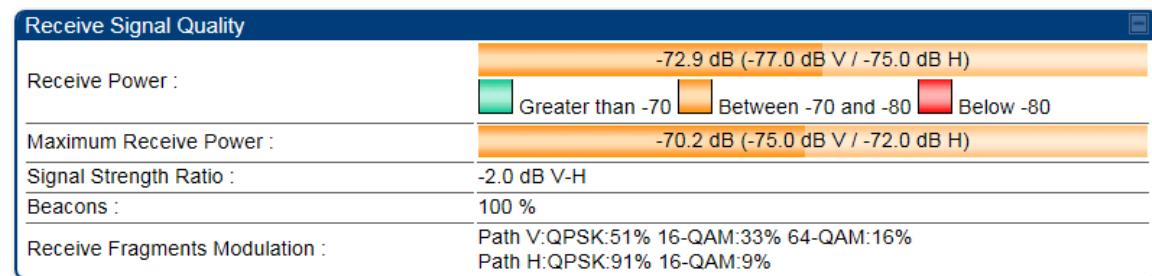
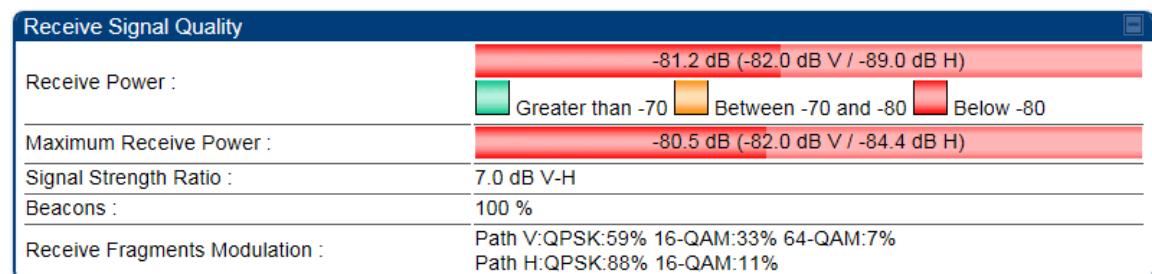


Figure 88 Alignment Tool tab of SM – Receive Power Level < -80 dBm



Alignment Tool and Diagnostic LED – SM/BHS

The SM's/BHS's Alignment Tool (located in **GUI Tools > Alignment**) 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 > Alignment**). To enter "aiming" mode, configure parameter **Scan Radio Frequency Only Mode** to "Enabled". See [SM/BHS LEDs](#) on page [2-7](#).



Note

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

Refer [Table 7 SM/BHS LED descriptions](#) on page [2-8](#) for SM/BHS LED details.

Alignment page of SM

The Alignment page of SM is explained in [Table 128](#).

Table 129 Alignment page attributes - SM

Aiming Configuration	
Scan Radio Frequency Only Mode :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <small>NOTE: No beacon information can be decoded when enabled</small>
Radio Frequency :	<input type="button" value="None"/> <input type="button" value="▼"/> <small>NOTE: This only applies if 'Scan Radio Frequency Only Mode' is enabled</small>
<input type="button" value="Enable"/> <input type="button" value="Disable"/> <small>(Push Enable button to manually refresh display)</small>	

Aiming Results	
Current Status :	SM is in Alignment Mode
Power Level :	-46 dBm V / -47 dBm H
Number Registered Users :	0 Range : (0 — 252)

Detailed Beacon Information	
Peak Power :	-43.5 (-46.0 V / -47.0 H) dBm
Users:	0
Frequency :	549.0 MHz
ESN :	0a-00-3e-bb-00-fb
Color Code :	254
Backhaul :	0

Attribute	Meaning
Scan Radio Frequency Only	Enabled: the radio is configured to "aiming" or "alignment" mode, wherein the LED panel displays an indication of receive power level. See SM/BHS LEDs on page 2-7 .

Mode	Table 7 SM/BHS LED descriptions on page 2-8 . Disabled: the radio is configured to “operating” mode, wherein the SM registers and passes traffic normally.
Radio Frequency	This field indicates the center frequency for which results are displayed.
Current Status	This field indicates the current mode of the radio, “alignment” or “operating”.
Power Level	This field indicates the current receive power level (vertical channel) for the frequency configured in parameter Radio Frequency .
Number Registered Users	When the radio is in “operating” mode, this field reports the number of registered SMs for the AP operating at the frequency defined in parameter Radio Frequency .
Peak Power	This field indicates the highest power level seen by the SMs receiver.
Users	This field indicates the number of SMs currently registered to the AP which is transmitting the beacon information.
Frequency	This field indicates the frequency of the AP which is transmitting the beacon information.
ESN	This field indicates the MAC, or hardware address of the AP 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 <i>must</i> 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 (<i>not</i> all 255 color codes).
Backhaul	0 indicates that the beacon transmitter is an AP.

Alignment page of BHS

The Alignment page of BHS is explained in [Table 129](#).

Table 130 Alignment page attributes - BHS

Aiming Configuration	
Scan Radio Frequency Only Mode :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled NOTE: No beacon information can be decoded when enabled
Radio Frequency :	None ▾ NOTE: This only applies if 'Scan Radio Frequency Only Mode' is enabled <input type="button" value="Enable"/> <input type="button" value="Disable"/> (Push Enable button to manually refresh display)
Aiming Results	
Current Status :	BHS is in Operating Mode
Power Level :	Not supported in this configuration. Radio needs to be in alignment mode.
Number Registered Users :	Not supported in this configuration Range : (0 — 252)
Detailed Beacon Information	
Aiming mode is currently disabled.	
Attribute	Meaning
Scan Radio Frequency Only Mode	Enabled: the radio is configured to "aiming" or "alignment" mode, wherein the SM's LED panel displays an indication of receive power level. See Table 139 on page 9-7 . Disabled: the radio is configured to "operating" mode, wherein the SM registers and passes traffic normally.
Radio Frequency	This field indicates the center frequency for which results are displayed.
Current Status	This field indicates the current mode of the radio, "alignment" or "operating".
Power Level	This field indicates the current receive power level (vertical channel) for the frequency configured in parameter Radio Frequency .
Number Registered Users	When the radio is in "operating" mode, this field reports the number of registered BHS for the BHM operating at the frequency defined in parameter Radio Frequency .
Peak Power	This field indicates the highest power level seen by the SMs receiver.
Users	This field indicates the number of BHS currently registered to the BHM which is transmitting the beacon information.
Frequency	This field indicates the frequency of the AP which is transmitting the beacon information.
ESN	This field indicates the MAC, or hardware address of the BHM which is transmitting the beacon information.
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 <i>must</i> 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 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).

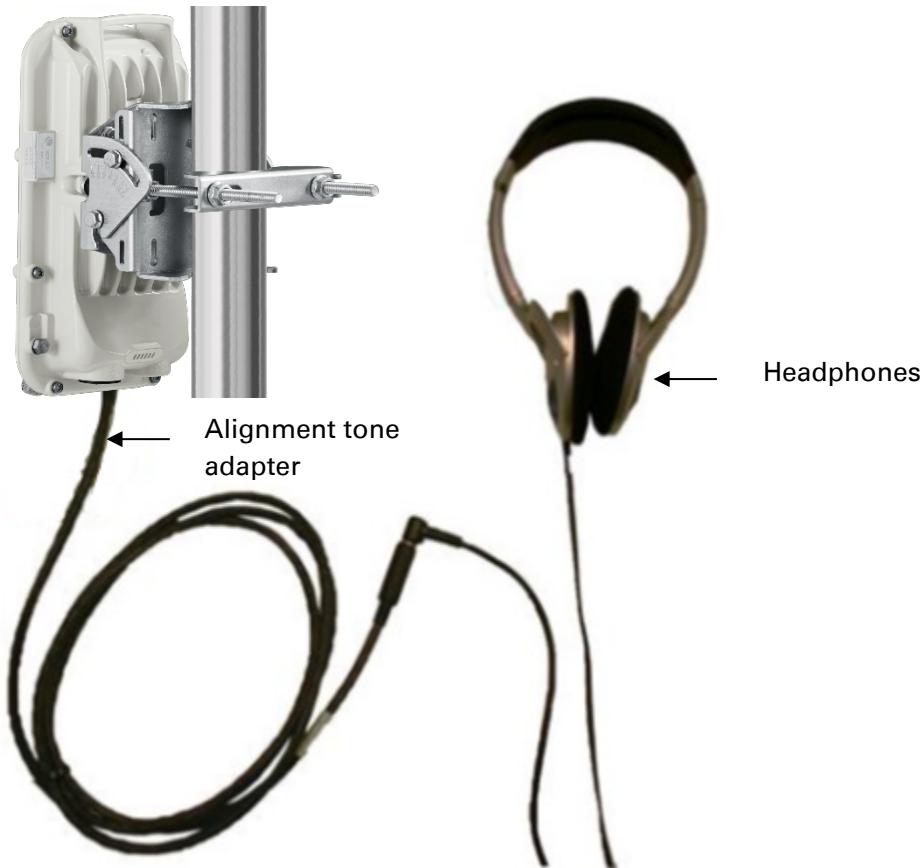
Backhaul

0 indicates that the beacon transmitter is a BHM.

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 [Alignment Tool and Diagnostic LED – SM/BHS on page 8-14](#), [Using the Link Capacity Test tool on page 8-19](#) and [Using AP Evaluation tool on page 8-22](#).

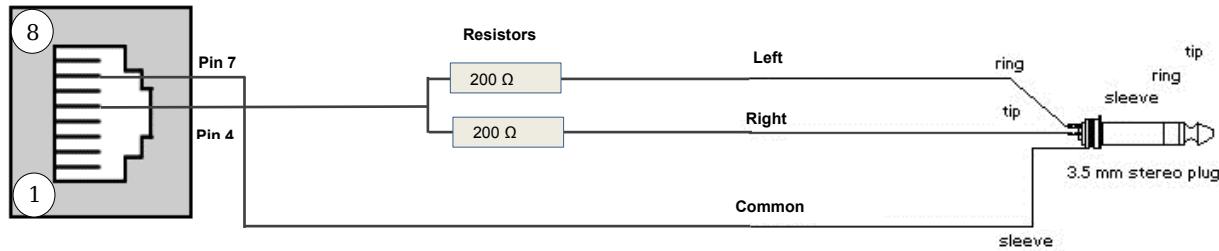
Figure 89 Link alignment tone



Alignment Tone Cable

A standard 32 ohms stereo headset can be connected to the AUX port to use the audio alignment tool. The diagram of the adapter is provided in [Figure 90](#). The recommended values for both resistors are 220 ohm, 0.25W.

Figure 90 Alignment Tone Cable



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** 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.

Performing link capacity test

To run a simple link capacity test that floods the link with 1714 byte packets for 10 seconds, perform the following procedure:

Procedure 30 Performing a simple Link Capacity Test

- 1 Access the Link Capacity Test tab in the Tools web page of the module.
- 2 Select Link Test Mode **Link Test with Bridging**
- 3 Select the subscriber module to test using the Current Subscriber Module parameter.
- 4 Type into the **Duration** field how long (in seconds) the RF link must be tested.
- 5 Type into the **Number of Packets** field a value of **0** to flood the link for the duration of the test.
- 6 Type into the **Packet Length** field a value of **1714** to send 1714-byte packets during the test.
- 7 Click the **Start Test** button.
- 8 In the Current Results Status block of this tab, view the results of the test. See [Figure 91](#) on page [8-19](#).

Figure 91 Link Capacity Test tab with 1714-byte packet length

Current Results Status
Stats for LUID: 2 Test Duration: 10 Pkt Length: 1714 Test Direction Bi-Directional

RF Link Test					
VC	Downlink	Uplink	Aggregate	Packet Transmit	Packet Receive
				Actual	Actual
18	40.95 Mbps	13.09 Mbps	54.05 Mbps, 3907 pps	9476 (947 pps)	29605(2960 pps)

Efficiency

Downlink		Uplink			
Efficiency	Fragments count	Efficiency	Fragments count		
				Actual	Expected
100%	799840	799840	100%	255856	255856

Link Test ran on 21:06:00 08/20/2015 IST

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

Link Capacity Test page of AP/SM

The Link Capacity Test page of AP is explained in [Table 130](#).

Table 131 Link Capacity Test page attributes - AP

Link Test Configurations	
Link Test Mode :	RF Link Test
Signal to Noise Ratio Calculation during Link Test :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Link Test VC Priority :	<input type="radio"/> High and Low Priority VCs <input checked="" type="radio"/> Low Priority VC only <small>Note: High and Low Priority VCs option requires that the SM already has high priority channel enabled.</small>
Link Test Settings	
Current Subscriber Module :	No Site Name [0a003ebb0104] Luid: 2
Duration :	10 Seconds (2 — 10)
Direction :	Bi-directional
Number of Packets :	0 (0 — 64) Zero will flood the link for duration of test
Packet Length :	1714 Bytes (64 — 1714 bytes)
Start Test	
Attribute	Meaning
Link Test Mode	<ul style="list-style-type: none"> RF Link Test: Fully 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.
	<p>Note</p>  <p>This mode setting must be equal on both the AP and the SM when running the link test for proper bridging and MIR handling..</p>
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.
Link Test VC Priority	This attribute may be used to enable/disable usage of the high priority virtual channel during the link test.
Current Subscriber Module	The SM with which the Link Capacity Test is run. This field is only applicable for AP (not SM page).
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 send during the Link Capacity Test. When Link Test Mode is set to RF Link Test 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

The Link Capacity Test page of BHM/BHS is explained in [Table 131](#).

Table 132 Link Capacity Test page attributes – BHM/BHS

Link Test Configurations	
Link Test Mode :	<input type="button" value="Link Test with Bridging"/>
Signal to Noise Ratio Calculation during Link Test :	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Link Test VC Priority :	<input type="radio"/> High and Low Priority VCs <input checked="" type="radio"/> Low Priority VC only
Link Test Settings	
Duration :	10 Seconds (2 — 10)
Direction :	<input type="button" value="Bi-directional"/>
Number of Packets :	0 (0 — 64) Zero will flood the link for duration of test
Packet Length :	1714 Bytes (64 — 1714 bytes)
<input type="button" value="Start Test"/>	
Current Results Status	
No test results available.	
Attribute	Meaning
Link Test Mode	See Table 130 on page 8-20
Signal to Noise Ratio Calculation during Link Test	See Table 130 on page 8-20
Link Test VC Priority	See Table 130 on page 8-20
Duration	See Table 130 on page 8-20
Direction	See Table 130 on page 8-20
Number of Packets	See Table 130 on page 8-20
Packet Length	See Table 130 on page 8-20

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.

AP Evaluation page of AP

The AP Evaluation page of AP is explained in [Table 132](#).

Table 133 AP Evaluation tab attributes - AP

AP List

AP Selection Method used: Optimize for Throughput
 Current entry index: 0 Session Status: REGISTERED (via Primary Color Code 254)

Index: 0 Frequency: 5490.000 MHz Channel Bandwidth: 10.0 MHz Cyclic Prefix: 1/16
 ESN: 0a-00-3e-bb-00-fb Region: Other
 Beacon Receive Power: -46.0 (-49.0 V / -49.0 H) dBm Beacon Count: 18 FECEn: 1
 Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail: 0 Range: 0 feet MaxRange: 2 miles TxBER: 1 EBcast: 0
 Session Count: 6 NoLUIDS: 0 OutOfRange: 0 AuthFail: 0 EncryptFail: 0 Rescan Req: 0 SMLimitReached: 0
 NoVC's: 0 VCRsv/430smFail: 0 VCActFail: 0
 AP Gain: -10 dBm AP RcvT: -55 dBm SectorID: 0 Color Code: 254 BeaconVersion: 1 SectorUserCount: 0
 SyncSrc: 0
 NumULSlots: 9 NumDLSlots: 26 NumULContSlots: 4
 WhiteSched: 0 ICC: 0 Authentication: Disabled
 SM PPPoE: Supported
 Frame Period: 2.5 ms

[Rescan APs](#)

Beacon Statistics

Unsupported Feature Beacon Received :	0
Unknown Feature Beacon Received :	0
Old Version Beacon Received :	0
Wrong Frequency Beacon Received :	0
Non Lite Beacon Received :	0

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	<p>This field contains the SNMP value from the AP that indicates whether the Forward Error Correction feature is enabled.</p> <p>0: FEC is disabled 1: FEC is enabled</p>
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 VC or a high priority data VC.
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 <i>must</i> 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 field 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 BHM

The BHM Evaluation page of BHM is explained in [Table 133](#).

Table 134 BHM Evaluation tab attributes - BHM



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 multipathing 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	<p>This field contains the SNMP value from the BHM that indicates whether the Forward Error Correction feature is enabled.</p> <p>0: FEC is disabled</p> <p>1: FEC is enabled</p>
Type	Multipoint indicates that the listing is for an 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	<p>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.</p> <p>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.</p>
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 an BHM which determines that no VC resources are available for allocation. This could be a primary data VC or a high priority data VC.
VCRsvFail	This counter is incremented when the BHS is registering to an 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 an 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	<p>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 <i>must</i> match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.</p> <p>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 (<i>not</i> all 255 color codes).</p>
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 field 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
- 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 APs/BHMs are within 300 bit times; if possible, within 150 bit times. In Cambium Point-to-Multipoint systems, 10 bit times = 1 μ s.

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.



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 134](#).

Table 135 OFDM Frame Calculator page attributes

OFDM Frame Calculator Parameters

Link Mode :	<input checked="" type="radio"/> Point-To-Point Link <input type="radio"/> Multipoint Link
Platform Type AP/BHM :	PMP/PTP 450/450i ▾
Platform Type SM/BHS :	PMP/PTP 450/450i ▾
Channel Bandwidth :	10.0 MHz ▾
Cyclic Prefix :	One Sixteenth ▾
Frame Period :	<input type="radio"/> 5.0 ms <input checked="" type="radio"/> 2.5 ms
Max Range :	2 Miles (Range: 1 - 40 miles)
Downlink Data :	75 %
Contention Slots :	1 (Range: 0 — 15)
SM/BHS One Way Air Delay :	0 ns

Calculated Frame Results

Modulation:OFDM
 Total Frame Bits : 25000
BHM Details :
 Data Slots (Down/Up) : 29 /10
 BHM Antenna Transmit End : 16218, 1.621854 ms
 BHM Antenna Receive Data Start : 16856, 1.685650 ms
 BHM Receive End : 26401
BHS Details :
 BHS Receive End : 16781
 BHS Transmit Start : 16856
 BHS One Way Air Delay : 0 ns
 BHS Approximate distance : 0.000 miles (0 feet)

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 8-33, 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 450i Series 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 450i) 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 <i>ns</i> (nano seconds), that a SM/BHS is away from the AP/BHM.

The Calculated Frame Results display several items of interest:

Table 136 OFDM Calculated Frame Results attributes

Attribute	Meaning
Modulation	The type of radio modulation used in the calculation (OFDM for PMP/PTP 450i)
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 field displays the time in <i>ns</i> , 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 31 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 92 SM Configuration page - AP

Select Subscriber

Current Subscriber Module : No Site Name [0a003ebb0104] Luid: 2

Subscriber Configuration Information

LUID: 002 - [0a-00-3e-bb-01-04] State: IN SESSION (Encrypt Disabled)

Site Name : No Site Name

Software Version : .SVM;14.SVm;0.SVB;25.SVW;F.IT;SOC110.SVT;01:58.SVD;08/20/2015.

Software Boot Version : CANOPYBOOT 1.0

FPGA Version : 080715 (DES, Sched, US/ETSI) P13

Sustained Uplink Data Rate(SM): 65000 Uplink Burst Allocation(SM): 2500000 Sustained Downlink Data Rate (SM): 65000 Downlink Burst Allocation (SM): 2500000 (kbit)

Sustained Broadcast Data Rate (SM): 0, units: (SM): kbps

Max Burst Uplink Rate (SM): 0 (kbit)

Max Burst Downlink Rate (SM): 0 (kbit)

HiPriChan(SM): 0 VCChannel: 2

Low Priority Uplink CIR (SM): 0 Low Priority Downlink CIR (SM): 0 High Priority Uplink CIR (SM): 0 High Priority Downlink CIR (SM): 0 (kbps)

Low Priority Uplink (SM): 3 Low Downlink Priority (SM): 3 High Uplink Priority (SM): 5 High Downlink Priority (SM): 5

APBerLevel(AP): 2 Level HiPriTCPAck(AP): 1

AllowVLANLearning(SM): 1 AllowVLANFrameType(SM): 0 VLANAgeTmout(SM): 25

SMMManageVIDDis(SM): 0

IngressVID(SM): 1 ManageVID(SM): 1

MemberSet(SM):

Empty Set

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 137 Color code vers 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

The current Uplink Rate (both low and high VC) for each SM or BHS in Session is now available on AP or BHM Link Status Page.

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

Table 138 Link Status page attributes - AP

Link Status												
<p><i>Due to current system load, Downlink Statistics will only be updated at most every 5 seconds.</i></p> <p>Note: To measure the receive modulation of every fragment, Receive Quality Debug must be enabled.</p> <p> ■ 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 </p>												
Subscriber	Uplink Statistics					Downlink Statistics				BER Results	Reg	ReReg
	Power Level dBm: Signal Strength Ratio (dB V - H)	Fragments Modulation	Signal to Noise Ratio (dB)	Link Test Efficiency	Rate	Power Level dBm: Signal Strength Ratio (dB V - H)	Signal to Noise Ratio (dB)	Link Test Efficiency	Rate			
Site Name - LUID: 002	-52.5 (-55.3 V/-55.7 H):0.4	Path V:QPSK:37% 16-QAM:21% 64-QAM:20% 256-QAM:20% Path H:QPSK:39% 16-QAM:23% 64-QAM:23% 256-QAM:14%	44 V / 42 H	NA	8X/8X MIMO-B	-42.2 (-44.0 V/-47.0 H):4.0	43 V / 43 H	NA	8X/8X MIMO-B	2.065307e-07	3	0

Attribute	Meaning
Subscriber	This field displays the LUID (logical unit ID), MAC address and Site Name of the SM. As each SM registers to the AP, the system assigns an LUID of 2 or a higher unique number to the SM. If a SM loses registration with the AP and then regains registration, the SM will retain the same LUID.

**Note**

The LUID associated is lost when a power cycle of the AP occurs.

Both the LUID and the MAC are hot links 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.

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.
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.
BER Results	<p>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%.</p> <p>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.</p>

Reg Requests	<p>A Reg Requests count is the number of times the SM/BHS registered after the AP/BHM determined that the link had been down.</p> <p>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).</p>
ReReg Requests	<p>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).</p> <p>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).</p>

Using BER Results tool

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

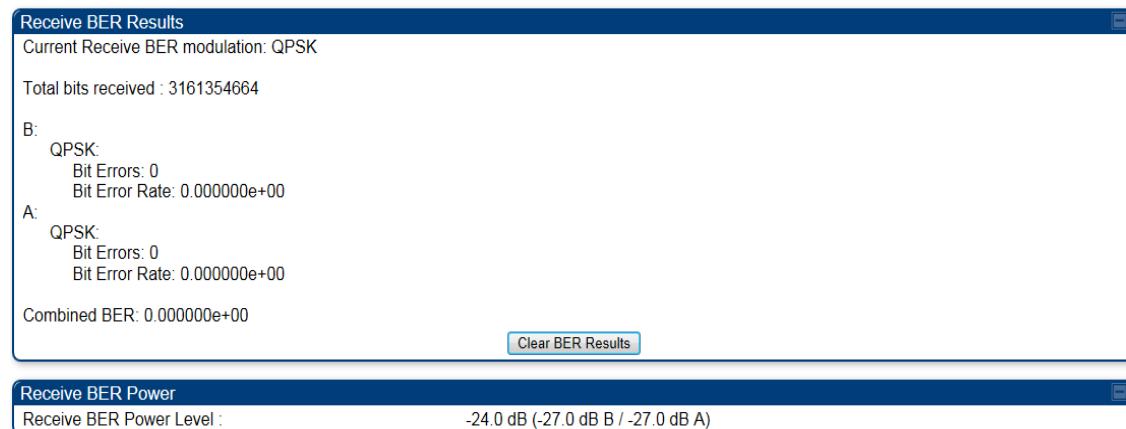
BER is only instrumented on the downlink and is displayed on the BER Results tab of the Tools page in any SM. Each time the tab is clicked, the current results are read and counters are reset to zero.

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

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

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

Figure 93 BER Results tab of the SM



Using the Sessions tool

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

Figure 94 Sessions tab of the AP



Chapter 9: Operation

This chapter provides instructions for operators of the PMP/PTP 450i wireless Ethernet Bridge.

The following topics are described in this chapter:

- [System](#) on page 9-2
 - [Viewing General Status](#) on page 9-2
 - [Viewing Session Status](#) on page 9-14
 - [Viewing Remote Subscribers](#) on page 9-19
 - [Interpreting messages in the Event Log](#) on page 9-19
 - [Viewing the Network Interface](#) on page 9-22
 - [Viewing the Layer 2 Neighbors](#) on page 9-23
- [System statistics](#) on page 9-24
 - [Viewing the Scheduler statistics](#) on page 9-24
 - [Viewing list of Registration Failures statistics](#) on page 9-26
 - [Interpreting Bridging Table statistics](#) on page 9-27
 - [Interpreting Translation Table statistics](#) on page 9-28
 - [Interpreting Ethernet statistics](#) on page 9-29
 - [Interpreting RF Control Block statistics](#) on page 9-32
 - [Interpreting VLAN statistics](#) on page 9-33
 - [Interpreting Data VC statistics](#) on page 9-35
 - [Interpreting Throughput statistics](#) on page 9-37
 - [Interpreting Overload statistics](#) on page 9-40
 - [Interpreting DHCP Relay statistics](#) on page 9-41
 - [Interpreting Filter statistics](#) on page 9-42
 - [Viewing ARP statistics](#) on page 9-43
 - [Viewing NAT statistics](#) on page 9-44
 - [Viewing NAT DHCP Statistics](#) on page 9-46
 - [Interpreting Sync Status statistics](#) on page 9-47
 - [Interpreting PPPoE Statistics for Customer Activities](#) on page 9-48
 - [Interpreting Bridge Control Block statistics](#) on page 9-49
 - [Interpreting Pass Through Statistics](#) on page 9-51
 - [Interpreting SNMPv3 Statistics](#) on page 9-52
 - [Interpreting syslog statistics](#) on page 9-54
 - [Interpreting Frame Utilization statistics](#) on page 9-54
- [Radio Recovery](#) on page 9-58

System information

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

- [Viewing General Status](#) on page 9-2
- [Viewing Session Status](#) on page 9-14
- [Viewing Remote Subscribers](#) on page 9-19
- [Interpreting messages in the Event Log](#) on page 9-19
- [Viewing the Network Interface](#) on page 9-22
- [Viewing the Layer 2 Neighbors](#) on page 9-23

Viewing General Status

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

General Status page of AP

The AP's **General Status** page is explained in [Table 138](#).

Table 139 General Status page attributes - AP

Device Information	
Device Type :	5.4GHz MIMO OFDM - Access Point - 0a-00-3e-bb-00-fb
Board Type :	P13 C110_SOC
Software Version :	CANOPY 14.0 AP-DES
Board MSN :	PMP450i
FPGA Version :	080715
Uptime :	1d, 00:41:44
System Time :	14:05:06 08/20/2015 IST
Ethernet Interface :	100Base-TX Full Duplex
Regional Code :	Other
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	5490.0 MHz
Channel Bandwidth :	10.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Color Code :	254
Max Range :	2 Miles
Transmit Power :	-10 dBm
Temperature :	32 °C / 90 °F
Access Point Stats	
Registered SM Count :	1 (1 Data VCs)
Sync Pulse Status :	Generating Sync
Sync Pulse Source :	Self Generate
Maximum Count of Registered SMs :	1
Frame Configuration Information	
Data Slots Down :	26
Data Slots Up :	9
Contention Slots :	4
Site Information	
Site Name :	Site Name
Site Contact :	Site Contact
Site Location :	Site Location
Key Features Information	
Time Updated and Location Code :	08/18/2015 06:41:40 - INTL
Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the SM, its module type and its MAC address.
Software Version	This field indicates the system release, the time and date of the release and whether communications involving the module are secured by DES

or AES encryption. If you request technical support, provide the information from this field.	
Board Type	This field indicates the series of hardware.
Combo Radio Mode	This field indicates the mode of operation, currently only 'MIMO OFDM Only' is supported.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. If you request technical support, provide the value of this field.
FPGA Type	Where the type of logic as a subset of the logic version in the module as manufactured distinguishes its circuit board, this field is present to indicate that type. If you request technical support, provide the value of this field.
PLD Version	This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. If the AP is connected to a CMM4, then this field provides GMT (Greenwich Mean Time). Any SM that registers to the AP inherits the system time.
Last NTP Time Update	This field displays when the AP last used time sent from an NTP server. If the AP has not been configured in the Time tab of the Configuration page to request time from an NTP server, then this field is populated by 00:00:00 00/00/00.
Ethernet Interface	This field indicates the speed and duplex state of the Ethernet interface to the AP.
Regulatory	This field indicates whether the configured Country Code and radio frequency are compliant with respect to their compatibility. PMP 450 equipment shipped to the United States is locked to a Country Code setting of "United States". Units shipped to regions other than the United States must be configured with the corresponding Country Code to comply with local regulatory requirements.
Channel Center Frequency	This field indicates the current operating center frequency, in MHz.
Channel Bandwidth	This field indicates the current size of the channel band used for radio transmission.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multi-pathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an

	additional bit is used.
Frame Period	This field indicates the current Frame Period setting of the radio in ms.
Color Code	<p>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 <i>must</i> match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code.</p> <p>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 (<i>not</i> all 255 color codes).</p>
Max Range	This field indicates the setting of the Max Range parameter, which contributes to the way the radio transmits. Verify that the Max Range parameter is set to a distance slightly greater than the distance between the AP and the furthest SM that must register to this AP.
Transmitter Output Power	This field indicates the combined power level at which the AP is set to transmit, based on the Country Code and Antenna Gain settings.
Temperature	This field indicates the current operating temperature of the device board.
Registered SM Count	This field indicates how many SMs are registered to the AP.
Sync Pulse Status	<p>This field indicates the status of synchronization as follows:</p> <p>Generating Sync indicates that the module is set to <i>generate</i> the sync pulse.</p> <p>Receiving Sync indicates that the module is set to <i>receive</i> a sync pulse from an outside source and is receiving the pulse.</p> <p>No Sync Since Boot up / ERROR: No Sync Pulse indicates that the module is set to <i>receive</i> a sync pulse from an outside source and is not receiving the pulse.</p>
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  </div> <div> <p>Note</p> <p>When this message is displayed, the AP transmitter is turned off to avoid self-interference within the system.</p> </div> </div>	
Sync Pulse Source	<p>This field indicates the status of the synchronization source:</p> <p>Searching indicates that the unit is searching for a GPS fix</p> <p>Timing Port/UGPS indicates that the module is receiving sync via the timing AUX/SYNC timing port</p> <p>Power Port indicates that the module is receiving sync via the power port (Ethernet port).</p> <p>On-board GPS indicates that the module is receiving sync via the unit's internal GPS module</p>

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.
Data Slots Down	This field indicates the number of frame slots that are designated for use by data traffic in the downlink (sent from the AP to the SM). The AP calculates the number of data slots based on the Max Range, Downlink Data and (reserved) Contention Slots configured by the operator.
Data Slots Up	This field indicates the number of frame slots that are designated for use by data traffic in the uplink (sent from the SM to the AP). The AP calculates the number of data slots based on the Max Range, Downlink Data and (reserved) Contention Slots configured by the operator.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. See Contention slots on page 7-129.
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the AP Configuration page. This information is also set into the <i>sysName</i> SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page. This information is also set into the <i>sysName</i> SNMP MIB-II object and can be polled by an SNMP management server.
Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the AP Configuration page.
Time Updated and Location Code	This field displays information about the keying of the radio.

General Status page - SM

The SM's **General Status** page is explained in [Table 139](#).



Note

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

Table 140 General Status page attributes - SM

Device Information	
Device Type :	4.9/5.9GHz MIMO OFDM - Backhaul - Timing Slave - 0a-00-3e-bb-01-04
Board Type :	P13 C110_SOC
Software Version :	CANOPY 14.0 BHUL450-DES
Board MSN :	PMP450IMSN
FPGA Version :	080715
Uptime :	00:11:31
System Time :	22:19:50 08/24/2015 IST
Ethernet Interface :	100Base-TX Full Duplex
Regional Code :	Other
Antenna Type :	External
Frame Period :	2.5 ms
Temperature :	35 °C / 95 °F
Timing Slave Stats	
Session Status :	REGISTERED VC 18 Rate 8X/1X MIMO-A VC 255 Rate 8X/1X MIMO-B
Session Uptime :	00:08:04
Registered Backhaul :	0a-00-3e-bb-00-fb Site Name
Channel Frequency :	5490.0 MHz
Receive Power :	-42.2 dBm
Signal Strength Ratio :	5.0dB V - H
Transmit Power :	16 dBm
Signal to Noise Ratio :	43 V / 43 H dB
Beacons :	0 %
Air Delay :	0 ns, approximately 0.000 miles (0 feet)
Frame Configuration Information	
Data Slots Down :	29
Data Slots Up :	10
Region Specific Information	
Regional Code :	Other
Site Information	
Site Name :	Site Name
Site Contact :	Site Contact
Site Location :	Site Location
Key Features Information	
Time Updated and Location Code :	08/24/2015 16:36:49 - INTL
Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency band of the SM, its module type and its MAC address.
Board Type	This field indicates the series of hardware.
Software Version	This field indicates the system release, the time and date of the release. If you request technical support, provide the information from this field.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the

information from this field.	
PLD Version	This field indicates the version of the programmable logic device (PLD) on the module. If you request technical support, provide the value of this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. Any SM that registers to an AP inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).
Ethernet Interface	This field indicates the speed and duplex state of Ethernet interface to the SM.
Regional Code	A parameter that offers multiple fixed selections, each of which automatically implements frequency band range restrictions for the selected region. Units shipped to regions other than the United States must be configured with the corresponding Country Code to comply with local regulatory requirements.
DFS	This field indicates that DFS operation is enabled based on the configured region code, if applicable.
Antenna Type	The current antenna type that has been selected.
Frame Period	This field indicates the current Frame Period setting of the radio in ms.
Temperature	The current operating temperature of the board.
Session Status	This field displays the following information about the current session: Scanning indicates that this SM currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page. Syncing indicates that this SM currently attempts to receive sync. Registering indicates that this SM has sent a registration request message to the AP and has not yet received a response. Registered indicates that this SM is both: <ul style="list-style-type: none">• registered to an AP.• ready to transmit and receive data packets.
Session Uptime	This field displays the duration of the current link. The syntax of the displayed time is <i>hh:mm:ss</i> .
Registered AP	Displays the MAC address and site name of the AP to which the SM is registered to. This parameter provides click-through proxy access to the AP's management interface.
Color Code	This field displays a value from 0 to 254 indicating the SM's configured color code. For registration to occur, the color code of the SM and the AP <i>must</i> 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 (<i>not</i> all 255 color codes).	
Channel Frequency	This field lists the current operating frequency of the radio.
Channel Bandwidth	The size in MHz of the operating channel.
Cyclic Prefix	OFDM technology uses a cyclic prefix, where a portion of the end of a symbol (slot) is repeated at the beginning of the symbol to allow multipathing to settle before receiving the desired data. A 1/16 cyclic prefix means that for every 16 bits of throughput data transmitted, an additional bit is used.
Air Delay	This field displays the distance in feet between this SM and the AP. To derive the distance in meters, multiply the value of this parameter by 0.3048. Distances reported as less than 200 feet (61 meters) are unreliable.
Receive Power	This field lists the current combined receive power level, in dBm.
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power.
Signal to Noise Ratio	This field lists the current signal-to-noise level, an indication of the separation of the received power level vs. noise floor.
Beacons	Displays a count of beacons received by the SM in percentage. This value must be typically between 99-100%. If lower than 99%, it indicates a problematic link. This statistic is updated every 16 seconds.
Transmit Power	This field lists the current combined transmit power level, in dBm.
Data Slots Down	This field lists the number of slots used for downlink data transmission.
Data Slots Up	This field lists the number of slots used for uplink data transmission.
Contention Slots	This field indicates the number of (reserved) Contention Slots configured by the operator. See Contention slots on page 7-129 .
Site Name	This field indicates the name of the physical module. You can assign or change this name in the SNMP tab of the SM Configuration page. This information is also set into the <code>sysName</code> SNMP MIB-II object and can be polled by an SNMP management server.
Site Contact	This field indicates contact information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page. This information is also set into the <code>sysName</code> SNMP MIB-II object and can be polled by an SNMP management server.

Site Location	This field indicates site information for the physical module. You can provide or change this information in the SNMP tab of the SM Configuration page.
Maximum Throughput	This field indicates the limit of aggregate throughput for the SM and is based on the default (factory) limit of the SM and any floating license that is currently assigned to it.
Time Updated and Location Code	This field displays information about the keying of the radio.

G7eneral Status page of BHM

The BHM's **General Status** page is explained in [Table 140](#).

Table 141 General Status page attributes - BHM

Device Information	
Device Type :	5.4GHz MIMO OFDM - Backhaul - Timing Master - 0a-00-3e-bb-00-fb
Board Type :	P13 C110_SOC
Software Version :	CANOPY 14.0 BHUL450-DES
Board MSN :	PMP450iMSN
FPGA Version :	080715
Uptime :	00:12:14
System Time :	22:22:58 08/24/2015 IST
Ethernet Interface :	100Base-TX Full Duplex
Regional Code :	Other
Regulatory :	Passed
Antenna Type :	External
Channel Frequency :	5490.0 MHz
Channel Bandwidth :	10.0 MHz
Cyclic Prefix :	1/16
Frame Period :	2.5 ms
Color Code :	254
Transmit Power :	-10 dBm
Temperature :	32 °C / 90 °F

Backhaul Stats	
Timing Slave Status :	Connected
Sync Pulse Status :	Receiving Sync
Sync Pulse Source :	Power Port
UGPS Power Status :	Power Off

Frame Configuration Information	
Data Slots Down :	29
Data Slots Up :	10

Site Information	
Site Name :	Site Name
Site Contact :	Site Contact
Site Location :	Site Location

Key Features Information	
Time Updated and Location Code :	08/24/2015 16:39:29 - INTL

Attribute	Meaning
Device Type	This field indicates the type of the module. Values include the frequency

	band of the BHM, its module type and its MAC address.
Board Type	This field indicates the series of hardware.
Software Version	This field indicates the system release, the time and date of the release. If you request technical support, provide the information from this field.
Board MSN	This field indicates the Manufacturer's Serial number. A unique serial number assigned to each radio at the factory for inventory and quality control.
FPGA Version	This field indicates the version of the field-programmable gate array (FPGA) on the module. When you request technical support, provide the information from this field.
Uptime	This field indicates how long the module has operated since power was applied.
System Time	This field provides the current time. Any BHS that registers to a BHM inherits the system time, which is displayed in this field as GMT (Greenwich Mean Time).
Ethernet Interface	This field indicates the speed and duplex state of Ethernet interface to the BHM.
Antenna Type	The current antenna type that has been selected.
Temperature	The current operating temperature of the board.
Session Status	This field displays the following information about the current session: Scanning indicates that this BHS currently cycles through the radio frequencies that are selected in the Radio tab of the Configuration page. Syncing indicates that this BHM currently attempts to receive sync. Registering indicates that this BHM has sent a registration request message to the BHM and has not yet received a response. Registered indicates that this BHM is both: <ul style="list-style-type: none">• Registered to a BHM.• Ready to transmit and receive data packets.
Session Uptime	This field displays the duration of the current link. The syntax of the displayed time is <i>hh:mm:ss</i> .
Registered Backhaul	Displays the MAC address and site name of the BHM to which the BHS is registered to. This parameter provides click-through proxy access to the BHM's management interface.
Channel Frequency	This field lists the current operating frequency of the radio.
Receive Power	This field lists the current combined receive power level, in dBm.
Signal Strength Ratio	This field displays the difference of the Vertical path received signal power to the Horizontal path received signal power.