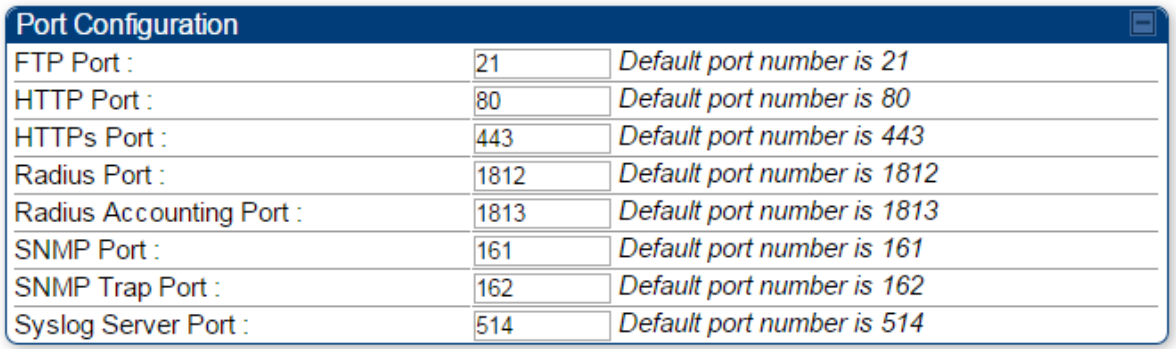
Port configuration

450 Platform Family ODUs support access to various communication protocols and only the ports required for these protocols are available for access by external entities. Operators may change the port numbers for these protocols via the radio GUI or SNMP.

The **Port Configuration** page of the AP/SM/BHM/BHS is explained in Table 137.

Table 137 Port Configuration attributes – AP/SM/BHM/BMS



Port Configuration		
FTP Port :	21	*Default port number is 21*
HTTP Port :	80	*Default port number is 80*
HTTPs Port :	443	*Default port number is 443*
Radius Port :	1812	*Default port number is 1812*
Radius Accounting Port :	1813	*Default port number is 1813*
SNMP Port :	161	*Default port number is 161*
SNMP Trap Port :	162	*Default port number is 162*
Syslog Server Port :	514	*Default port number is 514*

Attribute	Meaning
FTP Port	The listen port on the device used for FTP communication.
HTTP Port	The listen port on the device used for HTTP communication.
HTTPS Port	The listen port on the device used for HTTPS communication
Radius Port	The destination port used by the device for RADIUS communication.
Radius Accounting Port	The destination port used by the device for RADIUS accounting communication.
SNMP Port	The listen port on the device used for SNMP communication.
SNMP Trap Port	The destination port used by the device to which SNMP traps are sent.
Syslog Server Port	The destination port used by the device to which Syslog messaging is sent.

Encrypting downlink broadcasts

See Encrypting downlink broadcasts on page 3-48.

Isolating SMs

See Isolating SMs in PMP on page 3-48.

Filtering management through Ethernet

See Filtering management through Ethernet on page 3-48.

Allowing management only from specified IP addresses

See Allowing management from only specified IP addresses on page 3-49.

Restricting radio Telnet access over the RF interface

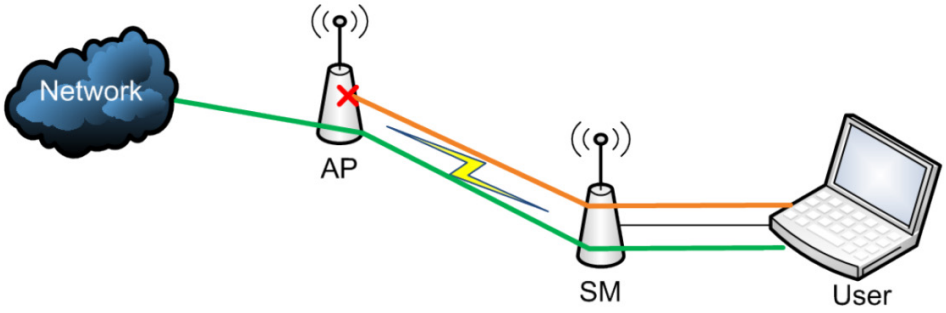
RF Telnet Access restricts Telnet access to the AP from a device situated below a network SM (downstream from the AP). This is a security enhancement to restrict RF-interface sourced AP access specifically to the LAN1 IP address and LAN2 IP address (Radio Private Address, typically 192.168.101. [LUID]). This restriction disallows unauthorized users from running Telnet commands on the AP that can change AP configuration or modifying network-critical components such as routing and ARP tables.

The RF Telnet Access may be configured via the AP GUI or via SNMP commands, and RF Telnet Access is set to “Enabled” by default. Once RF Telnet Access is set to “Disabled”, if there is a Telnet session attempt to the AP originating from a device situated below the SM (or any downstream device), the attempt is dropped. This also includes Telnet session attempts originated from the SM’s management interface (if a user has initiated a Telnet session to a SM and attempts to Telnet from the SM to the AP). In addition, if there are any active Telnet connections to the AP originating from a device situated below the SM (or any downstream device), the connection is dropped. This behavior must be considered if system administrators use Telnet downstream from an AP (from a registered SM) to modify system parameters.

Setting RF Telnet Access to “Disabled” does not affect devices situated above the AP from accessing the AP via Telnet, including servers running the CNUT (Canopy Network Updater tool) application. Also, setting RF Telnet Access to “Disabled” does not affect any Telnet access into upstream devices (situated above or adjacent to the AP) through the AP (see Figure 143).

The figure below depicts a user attempting two telnet sessions. One is targeted for the AP (orange) and one is targeted for the network upstream from the AP (green). If RF Telnet Access is set to “Disabled” (factory default setting), the Telnet attempt from the user to the AP is blocked, but the attempt from the user to Network is allowed to pass through the Cambium network.

Figure 143 RF Telnet Access Restrictions (orange) and Flow through (green)



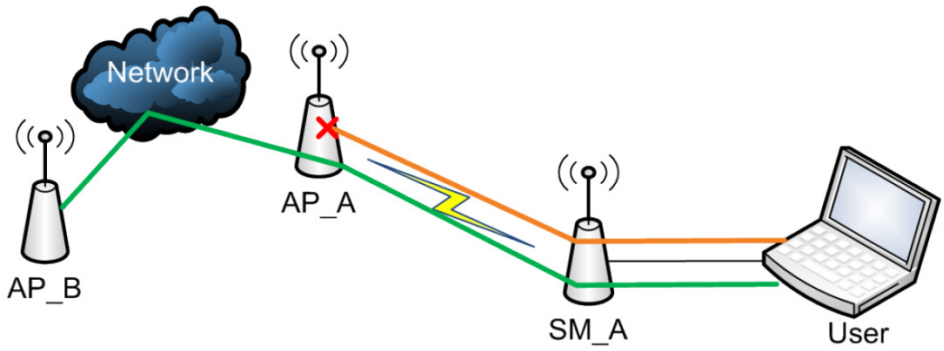
Key Security Considerations when using the RF Telnet Access Feature

To ensure that the network is fully protected from unauthorized AP Telnet sessions, the following topics must be considered:

Securing AP Clusters

When working with a cluster of AP units, to eliminate potential security holes allowing Telnet access, ensure that the RF Telnet Access parameter is set to “Disabled” for every AP in the cluster. In addition, since users situated below the AP are able to pass Telnet sessions up through the SM and AP to the upstream network (while AP RF Telnet Access is set to “Disabled”), ensure that all CMM4 or other networking equipment is secured with strong passwords. Otherwise, users may Telnet to the CMM4 or other networking equipment, and subsequently access network APs (see Figure 144) via their Ethernet interfaces (since RF Telnet Access only prevents Telnet sessions originating from the AP’s wireless interface).

Figure 144 RF Telnet Access Restriction (orange) and Potential Security Hole (green)



As a common practice, AP administrator usernames and passwords must be secured with strong, non-default passwords.

Restricting AP RF Telnet Access

AP Telnet access via the RF interface may be configured in two ways – the AP GUI and SNMP.

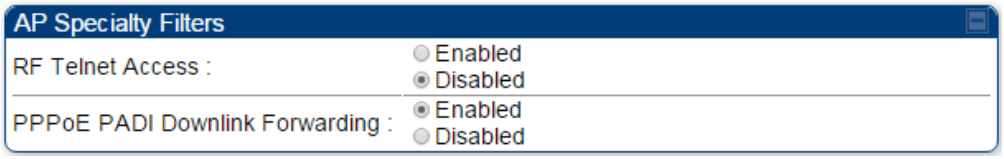
Controlling RF Telnet Access via the AP GUI

To restrict all Telnet access to the AP via the RF interface from downstream devices, follow these instructions using the AP GUI:

Procedure 20 Restricting RF Telnet access

1. Log into the AP GUI using administrator credentials
2. On the AP GUI, navigate to **Configuration > Protocol Filtering**

3 Under GUI heading “Telnet Access over RF Interface”, set **RF Telnet Access** to **Disabled**



4 Click the **Save** button

5 Once the **Save** button is clicked, all RF Telnet Access to the AP from devices situated below the AP is blocked.

Note

The factory default setting for RF Telnet Access is disabled and PPPoE PADI Downlink Forwarding is enabled.

Configuring SNMP Access

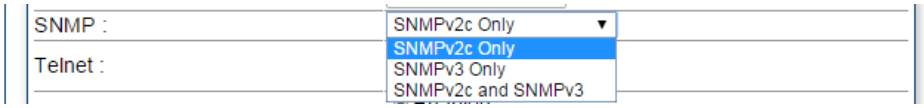
The SNMPv3 interface provides a more secure method to perform SNMP operations. This standard provides services for authentication, data integrity and message encryption over SNMP. Refer to Planning for SNMPv3 operation on page 3-42 for details.

Note

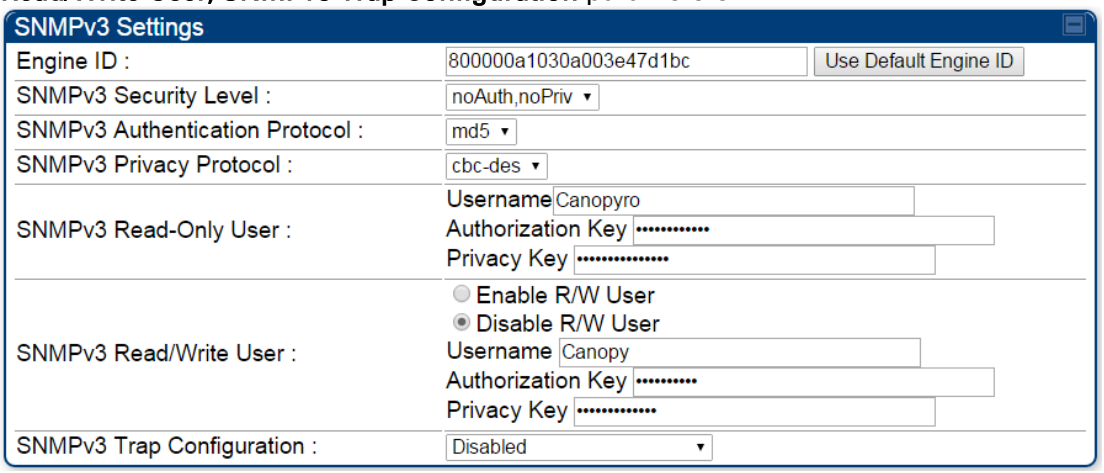
The factory default setting for SNMP is “SNMPv2c Only”.

Procedure 21 Configuring SNMPv3

1. Log into the AP GUI using administrator credentials
2. On the AP/SM GUI, navigate to **Configuration > Security Page**
3. Under GUI heading “Security Mode”, set **SNMP** to **SNMPv3 Only**



4. Click the **Save Changes** button
5. Go to **Configuration > SNMP Page**
6. Under GUI heading “SNMPv3 setting”, set **Engine ID, SNMPv3 Security Level, SNMPv3 Authentication Protocol, SNMPv3 Privacy Protocol, SNMPv3 Read-Only User, SNMPv3 Read/Write User, SNMPv3 Trap Configuration** parameters:



Engine ID :

Each radio (AP/SM/BHM/BHS) has a distinct SNMP authoritative engine identified by a unique Engine ID. While the Engine ID is configurable to the operator it is expected that the operator follow the guidelines of the SNMPEngineID defined in the SNMP-FRAMEWORK-MIB (RFC 3411). The default Engine ID is the MAC address of the device.

SNMPv3 security level, Authentication and Privacy Protocol

The authentication allows authentication of SNMPv3 user and privacy allows for encryption of SNMPv3 message. 450 Platform Family supports MD5 authentication and CBC-DES privacy protocols.

SNMPv3 Read-Only and Read/Write User

The user can defined by configurable attributes. The attributes and default values are:

- Read-only user
  - Username = Canopyro
  - Authentication Password = authCanopyro
  - Privacy Password = privacyCanopyro
- Read-write user (by default read-write user is disabled)
  - Username = Canopy
  - Authentication Password = authCanopy
  - Privacy Password = privacyCanopy

SNMPv3 Trap Configuration

The traps may be sent from radios in SNMPv3 format based on parameter settings. It can be configured for Disabled, Enabled for Read-Only User, Enable for Read/Write User.

Configuring Security

Applicable products	PMP : ☑ AP ☑ SM	PTP: ☑ BHM ☑ BMS

Security page – 450 Platform Family AP/BHM

The security page of AP/BHM is explained in Table 138.

Table 138 Security attributes –450 Platform Family AP

Authentication Server Settings	
Authentication Mode :	Disabled
Authentication Server DNS Usage :	○ Append DNS Domain Name ◉ Disable DNS Domain Name
Authentication Server 1 :	•••••••••••••••••• Shared Secret 0.0.0.0
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 *Default port number is 1812*
Authentication Key :	(Using All 0xFF's Key)
Select Key :	○ Use Key above ◉ Use Default Key
Dynamic Authorization Extensions for RADIUS :	○ Enable CoA and Disconnect Message ◉ Disable CoA and Disconnect Message
Bypass Authentication for ICC SMs :	○ Enabled ◉ Disabled

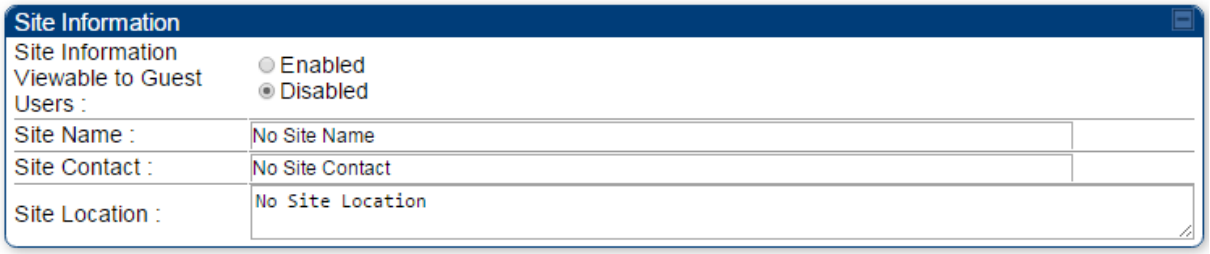
Airlink Security	
Encryption Setting :	None

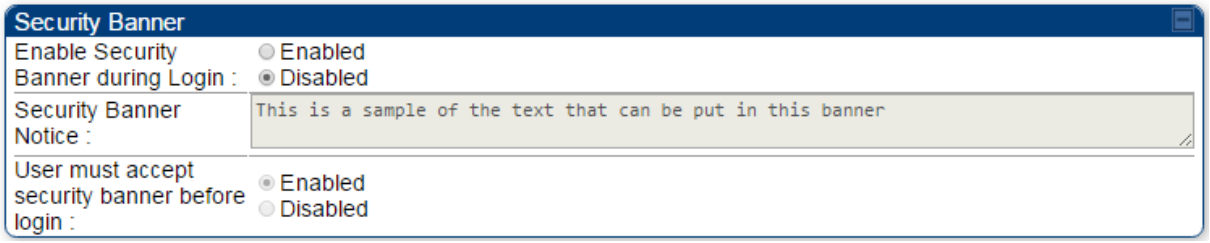
AP Evaluation Configuration	
SM Display of AP Evaluation Data :	○ Disable Display ◉ Enable Display

Session Timeout	
Web, Telnet, FTP Session Timeout :	600 Seconds

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

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





Attribute	Meaning
Authentication Mode	Operators may use this field to select from among the following authentication modes: **Disabled**—the AP/BHM requires no SMs/BHS to authenticate. (Factory default). **Authentication Server** —the AP/BHM requires any SM/BHS that attempts registration to be authenticated in Wireless Manager before registration. **AP PreShared Key** - The AP/BHM acts as the authentication server to its SMs/BHS and will make use of a user-configurable pre-shared authentication key. The operator enters this key on both the AP/BHM and all SMs/BHS desired to register to that AP/BHM. There is also an option of leaving the AP/BHM and SMs/BHS 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/BHS and reboot them BEFORE enabling the key and option on the AP/BHM. Otherwise, if you configure the AP/BHM first, none of the SMs/BHS is able to register. **RADIUS AAA** - When RADIUS AAA is selected, up to 3 Authentication Server (RADIUS Server) IP addresses and Shared Secrets can be configured. The IP address(s) configured here must match the IP address(s) of the RADIUS server(s). The shared secret(s) configured here must match the shared secret(s) configured in the RADIUS server(s). Servers 2 and 3 are meant for backup and reliability, not for splitting the database. If Server 1 doesn't respond, Server 2 is tried, and then server 3. If Server 1 rejects authentication, the SM is denied entry to the network, and does not progress trying the other servers. **Note** This parameter is applicable to BHM.

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. **Note** This parameter is applicable to BHM.
Authentication Server *1 to 5*	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. **Note** This parameter is applicable to BHM.
Radius Port	This field allows the operator to configure a custom port for RADIUS server communication. The default value is *1812*. **Note** This parameter is applicable to BHM.
Authentication Key	The authentication key is a 32-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF. **Note** This parameter is applicable to BHM.
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 **Note** This parameter is applicable to BHM.
Dynamic Authorization Extensions for RADIUS	**Enable CoA and Disconnect Message**: Allows to control configuration parameters of SM using RADIUS CoA and Disconnect Message feature. **Disable CoA and Disconnect Message**: Disables RADIUS CoA and Disconnect Message feature. To enable CoA and Disconnect feature, the Authentication Mode should be set to RADIUS AAA.
Bypass Authentication for ICC SMs	**Enabled**: SM authentication is disabled when SM connects via ICC (Installation Color Code). **Disabled**: SM authentication is enabled.
Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs.

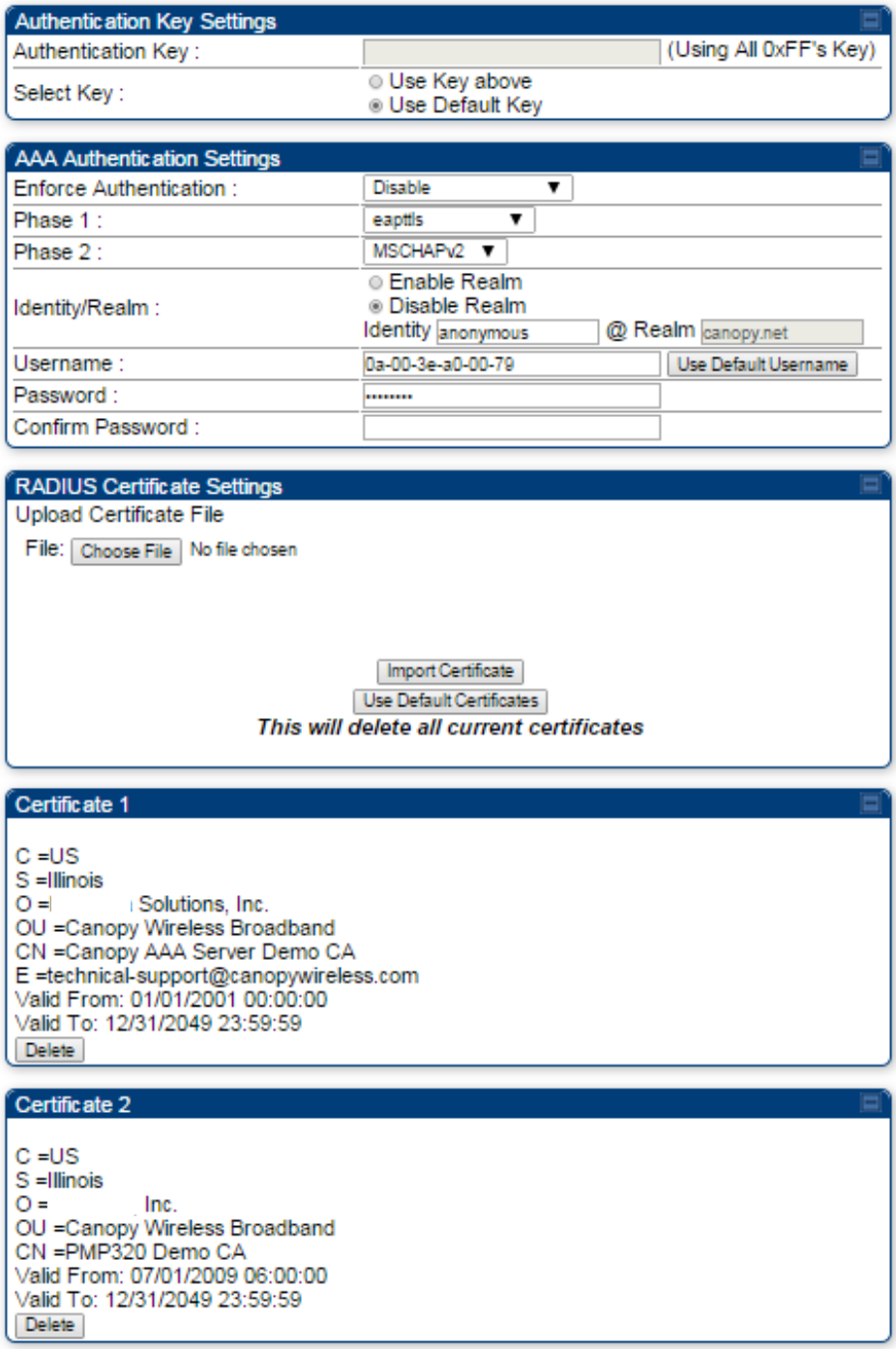
	None provides no encryption on the air link. **DES** (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data. DES encryption does not affect 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. **Note** This parameter is applicable to BHM.
SM Display of AP Evaluation Data Or BHS Display of BHM Evaluation Data	Allows operators to suppress the display of data about this AP/BHM on the AP/BHM Evaluation tab of the Tools page in all SMs/BHS that register. The factory default setting for SM Display of AP Evaluation Data or BHS Display of BHM Evaluation Data is enabled display. PMP 450/450i Series – SM display of AP Evaluation Data parameter AP Evaluation Configuration SM Display of AP Evaluation Data : Disable Display / Enable Display PTP 450/450i Series – BHS display of BHM Evaluation Data parameter BHM Evaluation Configuration BHS Display of BHM Evaluation Data : Disable Display / Enable Display
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*	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.

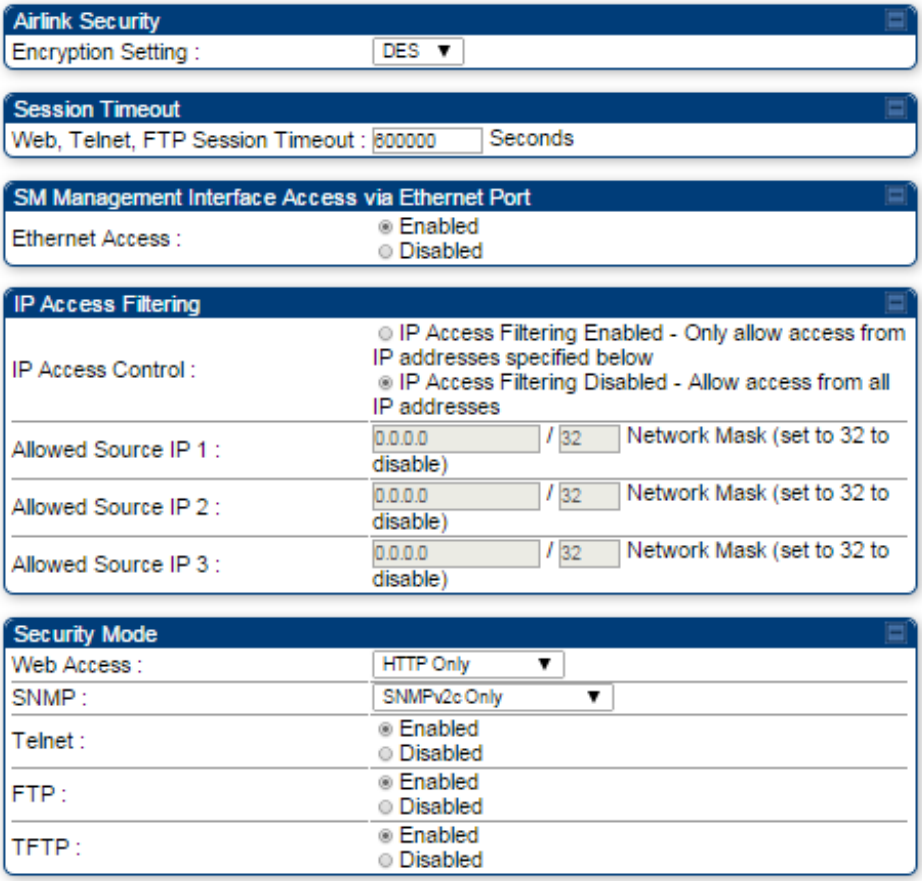
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent 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 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 - 450 Platform Family SM

The security page of 450 Platform Family SM is explained in Table 139.

Table 139 Security attributes –450 Platform Family SM





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	The **Use Default Key** selection specifies the predetermined key for authentication in Wireless Manager The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the SM and the WM
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 EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

Phase 2	Select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAP** (Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.
Identity/Realm	If Realms are being used, select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters. Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Username	Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password	Enter the desired password for the SM in the **Password** and **Confirm Password** fields. The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters
Upload Certificate File	To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate. When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used. The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system. Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

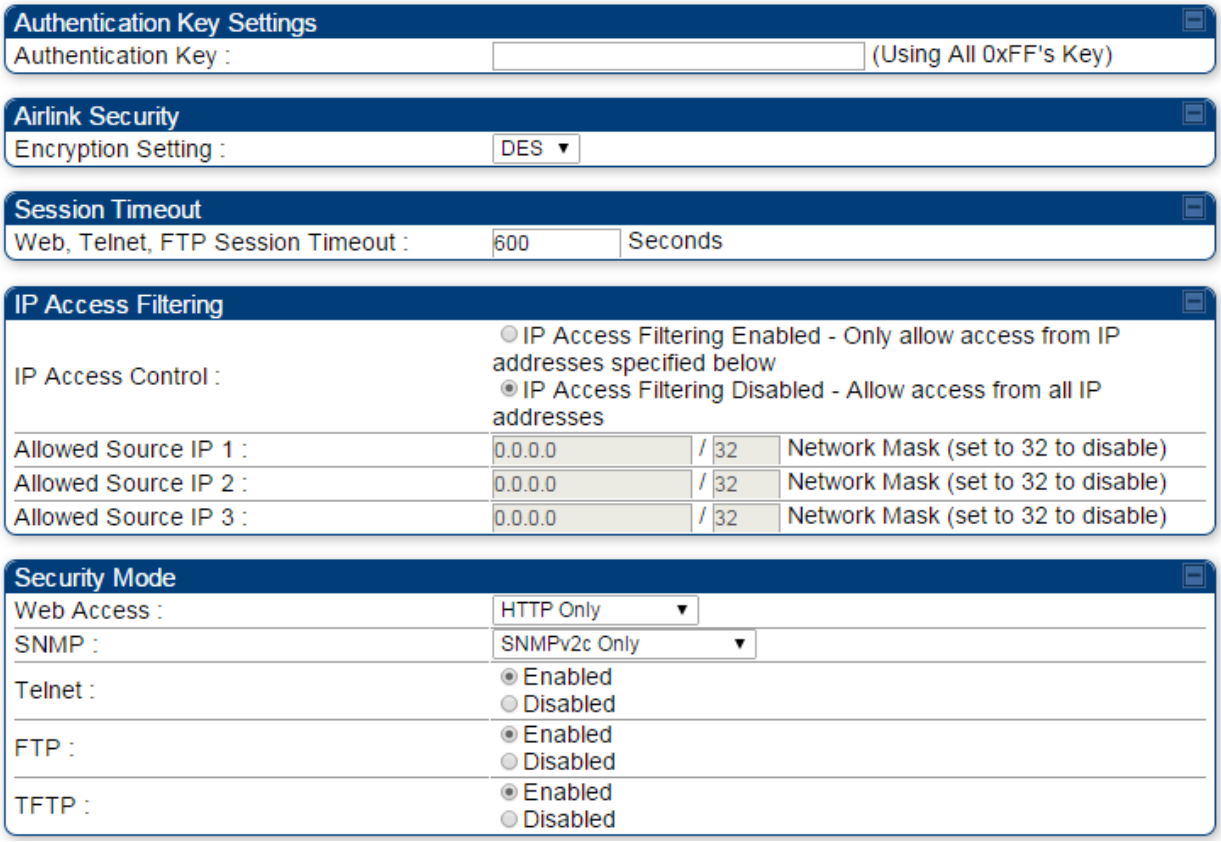
Encryption Setting	Specify the type of airlink security to apply to this SM. The encryption setting must match the encryption setting of the AP. **None** provides no encryption on the air link. **DES** (Data Encryption Standard): An over-the-air link encryption option that uses secret 56-bit keys and 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. **Note** 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. 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 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*	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.

	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. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent 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.
Site Name	Specify a string to associate with the physical module.
Site Contact	Enter contact information for the module administrator.
Site Location	Enter information about the physical location of the module.
Enable Security Banner during Login	**Enable**: The Security Banner Notice will be displayed before login. **Disable**: The Security Banner Notice will not be displayed before login.
Security Banner Notice	User can enter ASCII (0-9a-zA-Z newline, line-feed are allowed) text up-to 1300 characters.
User must accept security banner before login	**Enable**: login area (username and password) will be disabled unless user accepts the security banner. **Disable**: User can't login to radio without accepting security banner.

Security page –450 Platform Family BHS

The Security page of 450 Platform Family BHS is explained in Table 140.

Table 140 Security attributes - 450 Platform Family BHS



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	Specify the type of airlink security to apply to this BHS. The encryption setting must match the encryption setting of the BHM. **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. It is factory default setting. **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 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*	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. 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. A subnet mask may be defined for each entry to allow for filtering control based on a range of IP addresses.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent 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.

Configuring radio parameters

PMP 450m Series – configuring radio

Radio page - PMP 450m AP 5 GHz

The **Radio** tab of the PMP 450m 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 are displayed.

Table 141 PMP 450m AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.7 GHz
Frequency Carrier :	5730.0
Channel Bandwidth :	10 MHz
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Cyclic Prefix :	One Sixteenth
Color Code :	49 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	100 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	20 Minutes (0 — 60)
Installation Color Code :	○ Enabled ◉ Disabled
Sector ID :	0

Frame Configuration	
Max Range :	16 Miles (Range: 1 — 40 miles)
Downlink Data :	50 % (Range: 15 — 85 %)
Contention Slots :	4 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
EIRP :	36 dBm (Range: +22 — +36 dBm)
SM Receive Target Level :	-52 dBm (Range: -77 — -37 dBm) combined power
Adjacent Channel Support :	○ Enabled ◉ Disabled

Multicast Data Control	
Multicast VC :	Disable
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 4062 kbps)

Advanced	
PMP 430 SM Registration :	○ Allow ◉ Deny
PMP 450/430 Legacy Mode :	◉ Enabled ○ Disabled
Receive Quality Debug :	○ Enabled ◉ 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.
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 MHz, 10 MHz, 15 MHz, 20 MHz, 30 MHz, and 40 MHz. **Note for PMP 450m:** 5 ms frame size is not available in 30 MHz and 40 MHz channel bandwidths. **Note:** 40 MHz is not supported on PMP 450 AP, but is supported on PMP 450 SMs.
Frame Period	Select the Frame Period of the radio. The supported Frame Periods are: 5 ms and 2.5 ms.
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.
Color Code	Specify a value from 0 to 254. For registration to occur, the color code of the SM and the AP *must* match. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. Color code allows you to force a SM to register to only a specific AP, even where the SM can communicate with multiple APs. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).
Subscriber Color Code Rescan (When not on a Primary Color Code)	This timer may be utilized to initiate SM rescans in order to register to an AP configured with the SM's primary color code. 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

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	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).
Max Range	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 • does not increase the power of transmission from the AP. • can reduce aggregate throughput. For example, with a 20 MHz channel and 2.5 ms frame, every additional 2.24 miles reduces the data air time by one symbol (around 1% of the frame). Regardless of this distance, the SM must meet the minimum requirements for an acceptable link. The parameters have to be selected so that there is no overlap between one AP transmitting and another AP receiving. A co-location tool is provided to help with selecting sets of parameters that allow co-location. The default value of this parameter is 2 miles (3.2 km).
Downlink Data	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.

	Note In order to prevent self-interference, the frame configuration needs to align which includes Downlink Data, Max Range and Contention slots. For DFS regions, the maximum Downlink % for a 5.4 GHz radio is 75% only.
Contention Slots (a.k.a. Control Slots)	This field indicates the number of (reserved) Contention slots configured by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page 7-178.
Broadcast Repeat Count	For PMP systems broadcast packets are not acknowledged. So they are sent at the lowest modulation rate 1X. This setting adds an automatic retransmission to broadcast packets to give SMs that have poor signal a higher chance to get the packet.
EIRP	This field indicates the combined power level at which the AP will transmit, based on the Country Code. It also includes the antenna gain and array gain.
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 what is set in this field. This value represents the transmitted and received power (combined power) perceived on the SM.
Adjacent Channel Support	For some frequency bands and products, this setting is needed if AP is operating on adjacent channels with zero guard band.
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 256-QAM) and per channel (polarization). **Note** Due to CPU load, this will slightly degrade packet per second processing.
Near Field Operation	This parameter is enabled by the Near Field Operation control. This is only available when the EIRP is set to 22 dBm or below. When Near Field Operation is enabled, the Near Field Range is used to apply compensation to the unit's calibration to support operation in the near field.
PMP 430 SM Registration	This field allows to control PMP 430 SMs. It allows to configure whether PMP 430 SMs are registered to AP or not. By default, it is enabled and PMP 430 SM registrations are accepted. When this field is set to disabled, PMP 430 SM's registrations fail with reject reason 8. This will cause SMs to lock out the AP for 15 minutes. **Note** This option is not displayed if the Frame Period is set to 5 ms.

PMP 450/430 Legacy Mode	This setting allows the AP to communicate with SMs on Legacy versions of software (450 SM earlier than 13.2, 430 SM earlier than 13.4.1). This is not recommended to be left enabled as it degrades performance. SMs should then be upgraded to the same version as the AP.
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.

PMP/PTP 450i Series – configuring radio

Radio page - PMP 450i AP 3 GHz

The **Radio** tab of the PMP 450i AP 3 GHz is shown in Figure 145.

Figure 145 PMP 450i AP Radio attributes - 3 GHz

Radio Configuration

Frequency Band :	3.5 GHz
Frequency Carrier :	3505.000
Channel Bandwidth :	10 MHz
Cyclic Prefix :	One Sixteenth
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Color Code :	43 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	○ Enabled ◉ Disabled

Frame Configuration

Max Range :	40 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control

Transmit Power :	15 dBm (Range: -30 — +25 dBm) (12 dBm B / 12 dBm A)
External Gain :	0 dBi (Range: 0 — +70 dBi)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power
Adjacent Channel Support :	○ Enabled ◉ Disabled

Multicast Data Control

Multicast VC :	Disable
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 6093 kbps)

Advanced

MIMO Rate Adapt Algorithm :	MIMO-A/B
Control Messages :	○ SISO ◉ MIMO-A
Receive Quality Debug :	○ Enabled ◉ Disabled
Frame Alignment Legacy Mode :	OFF Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

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

Note

Refer Table 143 PMP 450i SM Radio attributes – 5 GHz on page 7-141 for parameter details

Radio page - PMP 450i AP 5 GHz

The **Radio** tab of the PMP 450i 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 are displayed.

Table 142 PMP 450i AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.4 GHz ▾
Frequency Carrier :	5480.0 ▾
Channel Bandwidth :	10 MHz ▾
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Cyclic Prefix :	One Sixteenth
Color Code :	0 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	○ Enabled ◉ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	0 dBm (Range: -30 — +27 dBm) (-3 dBm V / -3 dBm H)
External Gain :	11 dBi (Range: 0 — +40 dBi)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power

Multicast Data Control	
Multicast VC :	Disable ▾
Multicast Repeat Count :	0 (Range : 0 — 2)
Multicast Downlink CIR :	0 (kbps) (Range: 0— 6093 kbps)

Advanced

SM Registration :	◉ All (450i/450/430) ○ 450i Only
PMP 430 SM Registration :	◉ Allow ○ Deny
PMP 450/430 Legacy Mode :	○ Enabled ◉ Disabled
Control Messages :	○ SISO ◉ MIMO-A
PMP 430 Interop Mode :	○ SISO ◉ MIMO-A
Receive Quality Debug :	○ Enabled ◉ Disabled
Frame Alignment Legacy Mode :	OFF ▾ Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

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

Attribute	Meaning
Frequency Band	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129
Frequency Carrier	
Alternate Frequency Carrier 1 and 2	These parameters are displayed based on Regional Settings. Refer Country on page 7-72
Channel Bandwidth	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129
Cyclic Prefix	
Frame Period	
Color Code	
Subscriber Color Code Rescan (When not on a Primary Color Code)	
Subscriber Color Code Wait Period for Idle	
Installation Color Code	
Max Range	
Downlink Data	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129

Contention Slots (a.k.a. Control Slots)	This field indicates the number of (reserved) Contention slots configured by the operator. The SM uses reserved Contention slots and unused data slots for bandwidth requests. See Contention slots on page7-178.
Broadcast Repeat Count	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). 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. 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.
Transmitter Output Power	This value represents the combined power of the AP's two transmitters. Nations and regions may regulate transmitter output power. For example • 900 MHz, 5.4 GHz and 5.8 GHz 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.
SM Receive Target Level	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129
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 Series and is not backward compatible with PMP 430 series of radios.

Multicast Repeat Count	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 *0*.
Multicast Downlink CIR	This value is the committed information rate for the multicast downlink VC (located under the **Radio** tab of **Configuration**). The default value is *0* 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.
SM Registration All	This field allows to control registration of all type 450 Platform Family SM including 430 Series SM(450i/450/430) or 450i Series SM only.
PMP 430 SM Registration	This field allows to control PMP 430 SMs. It allows to configure whether PMP 430 SMs are registered to AP or not. By default, it is enabled and PMP 430 SM registrations are accepted. When this field is set to disabled, PMP 430 SM's registrations fail with reject reason 8. This will cause SMs to lock out the AP for 15 minutes. **Note** This option is not displayed if the Frame Period is set to 5 ms. This option applies only to PMP 450/450i/450m Series APs - 5 GHz.
Control Message	Controls whether the control messages are sent in MIMO-B or MIMO-A mode. MIMO-A is recommended. However, if an AP on 13.2 is attempting to connect to an SM on 13.1.3 or before, changing to MIMO-B may aid in getting the SM registered.
PMP 450/430 Legacy mode	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129
PMP 430 Interop Mode	For n-1 compatibility, In SISO mode this forces the AP to only send Control and Beacons over one of the RF paths.
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.
Frame Alignment Legacy Mode	

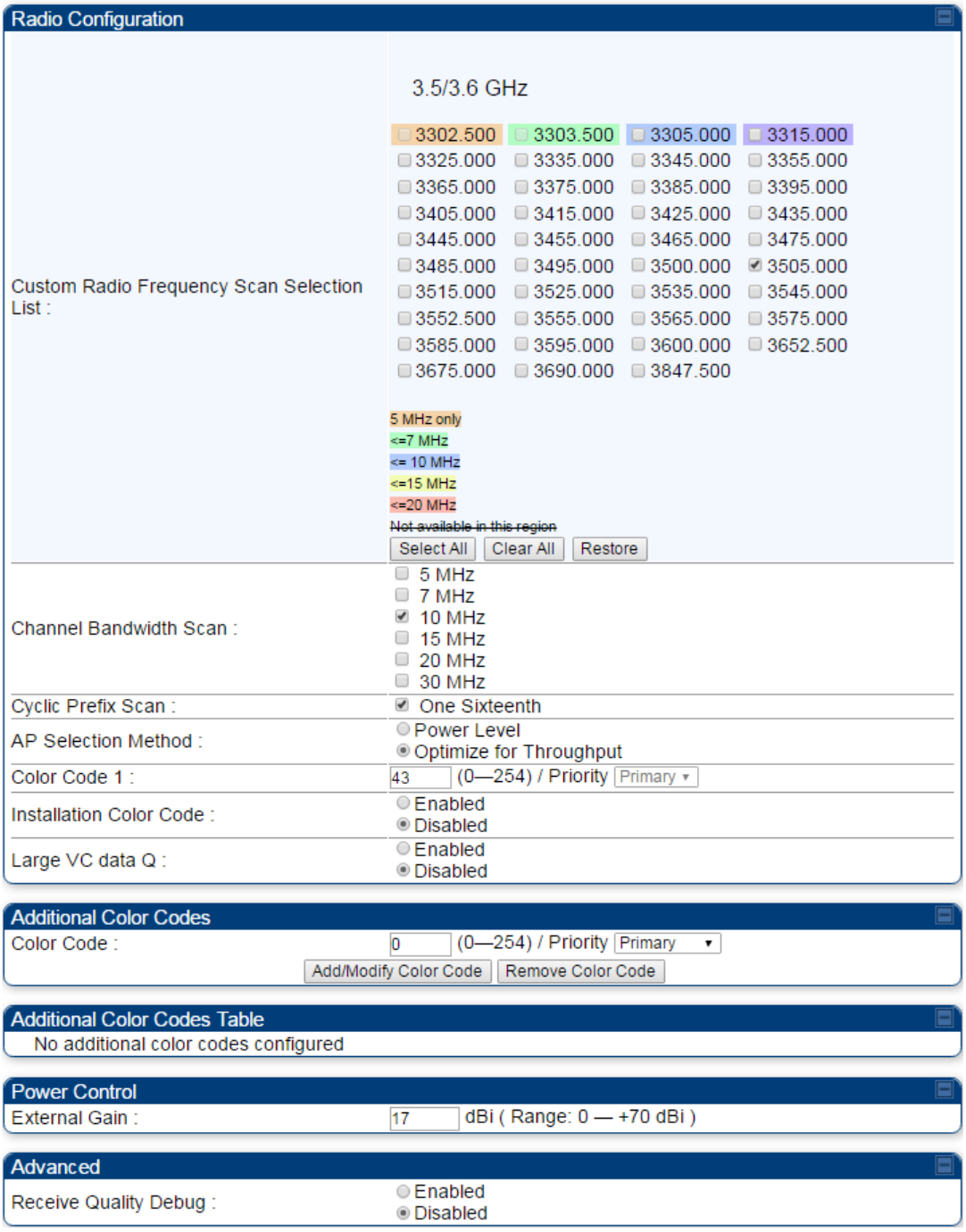
Mode	Behavior (non-900 MHz radios)	Behavior (FSK 900 MHz radios)

	OFF	By default frame start is aligned with devices with Timing Port synchronization If the synchronization source changes (due to Autosync or otherwise) the radio will dynamically adjust its frame start to maintain alignment with the default frame start timing	By default frame start is aligned with FSK 900 MHz devices with Timing Port synchronization If the synchronization source changes (due to Autosync or otherwise) the radio will dynamically adjust its frame start to maintain alignment with the default frame start timing
	ON (Mode 1)	The radio will align with devices running software versions from 12.0 to 13.4.	The radio will align with FSK 900 MHz devices running software versions from 12.0 to 13.4.
	ON (Mode 2)	N/A	The radio will align with FSK 900 MHz devices with software versions 11.2 or older.

Radio page - PMP 450i SM 3 GHz

The **Radio** tab of the PMP 450i SM 3 GHz is shown in Figure 146.

Figure 146 PMP 450i SM Radio attributes - 3 GHz



Note

Refer Table 143 PMP 450i SM Radio attributes – 5 GHz on page 7-141 for parameter details

Radio page – PMP 450i SM 5 GHz

The **Radio** page of PMP 450i SM is explained in Table 143.

Table 143 PMP 450i SM Radio attributes – 5 GHz

Radio Configuration

Custom Radio Frequency Scan Selection List :

4.9 GHz

~~4905.000~~	~~4907.500~~	~~4910.000~~	~~4912.500~~	~~4915.000~~
~~4917.500~~	~~4920.000~~	~~4922.500~~	~~4925.000~~	~~4927.500~~
~~4930.000~~	~~4932.500~~	~~4935.000~~	~~4937.500~~	~~4940.000~~
4942.500	4945.000	4947.500	4950.000	4952.500
4955.000	4957.500	4960.000	4962.500	4965.000
4967.500	4970.000	4972.500	4975.000	4977.500
4980.000	4982.500	4985.000	4987.500	~~4990.000~~
~~4992.500~~	~~4995.000~~			

5.1 GHz

~~5152.5~~	~~5155.0~~	5157.5	5160.0	5162.5	5165.0	5167.5
5170.0	5172.5	5175.0	5177.5	5180.0	5182.5	5185.0
5187.5	5190.0	5192.5	5195.0	5197.5	5200.0	5202.5
5205.0	5207.5	5210.0	5212.5	5215.0	5217.5	5220.0
5222.5	5225.0	5227.5	5230.0	5232.5	5235.0	5237.5
5240.0	5242.5	5245.0	5247.5			

5.4 GHz

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

5.7 GHz

~~5727.5~~	5730.0	5732.5	5735.0	5737.5	5740.0	5742.5
5745.0	5747.5	5750.0	5752.5	✓ 5755.0	5757.5	5760.0
5762.5	5765.0	5767.5	5770.0	5772.5	5775.0	5777.5
5780.0	5782.5	5785.0	5787.5	5790.0	5792.5	5795.0
5797.5	5800.0	5802.5	5805.0	5807.5	5810.0	5812.5
5815.0	5817.5	5820.0	5822.5	5825.0	5827.5	5830.0
5832.5	5835.0	5837.5	5840.0	5842.5	5845.0	~~5847.5~~
~~5850.0~~	~~5852.5~~	~~5855.0~~	~~5857.5~~	~~5860.0~~	~~5862.5~~	~~5865.0~~
~~5867.5~~	~~5870.0~~	~~5872.5~~	~~5875.0~~	~~5877.5~~	~~5880.0~~	~~5882.5~~
~~5885.0~~	~~5887.5~~	~~5890.0~~	~~5892.5~~	~~5895.0~~	~~5897.5~~	~~5900.0~~
~~5902.5~~	~~5905.0~~	~~5907.5~~	~~5910.0~~	~~5912.5~~	~~5915.0~~	~~5917.5~~
~~5920.0~~	~~5922.5~~					

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

Select All | Select All 4.9 | Select All 5.1 | Select All 5.2 | Select All 5.4 | Select All 5.7

Clear All | Restore

Channel Bandwidth Scan :	✓ 5 MHz 10 MHz 15 MHz ✓ 20 MHz 30 MHz ✓ 40 MHz
Cyclic Prefix :	One Sixteenth
AP Selection Method :	Power Level Optimize for Throughput
Color Code 1 :	212 (0—254) / Priority Primary
Installation Color Code :	Enabled Disabled
Large VC data Q :	Enabled Disabled

Additional Color Codes

Color Code : 0 (0—254) / Priority Primary

Add/Modify Color Code | Remove Color Code

Additional Color Codes Table

No additional color codes configured

Power Control

External Gain : 23 dBi (Range: 0 — +40 dBi)

Advanced

Receive Quality Debug : Enabled / Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-171.
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 AP scanning is executed.
AP Selection Method	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. **Power Level**: AP selection based solely on power level **Note** For operation with a PMP 450m AP, select the Power Level option *or* **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).
Color Code 1	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 *must* match. Specify a value from 0 to 254. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes). 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.

	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 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	This value represents the antenna gain. For ODUs with integrated antenna, this is set at the correct value in the factory. 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.
Large VC data Queue	SM 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 7-174) and cannot see it in the pull down menu.

Radio page - PMP 450i AP 900 MHz

The Radio tab of the PMP 450i AP 900 MHz is described in below table Table 144.

Table 144 PMP 450i AP Radio attributes - 900 MHz

Radio Configuration

Frequency Carrier :	917.00 ▼
Channel Bandwidth :	10 MHz ▼
Cyclic Prefix :	One Sixteenth ▼
Frame Period :	◉ 5.0 ms ○ 2.5 ms
Color Code :	65 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	○ Enabled ◉ Disabled

Frame Configuration

Max Range :	2 Miles (Range: 1 — 120 miles)
Downlink Data :	50 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control

Transmit Power :	25 dBm (Range: -30 — +25 dBm) (22 dBm B / 22 dBm A)
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

Control Messages :	○ SISO ◉ MIMO-A
Receive Quality Debug :	○ Enabled ◉ Disabled
Pager Reject Filter :	○ Enabled ◉ Disabled (NOTE: Frequencies 920 MHz and above will not work when enabled.)
Frame Alignment Legacy Mode :	OFF ▼ Choose Legacy Mode setting from the table below based on colocated 900 MHz FSK's software revision and sync source:

Sync Src.\ SW Rev.	13.4.1 or higher	12.0 to 13.4	below 12.0
Timing Port	OFF	OFF	OFF
Power Port	OFF	ON (Mode 1)	ON (Mode 2)

Attribute	Meaning
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 AP and the SM. The supported Channel Bandwidths are 5, 7, 10 and 20 MHz.
Cyclic Prefix	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129.
Frame Period	
Color Code	
Subscriber Color Code Rescan (When not on a Primary Color Code)	
Subscriber Color Code Wait Period for Idle	
Installation Color Code	
Max Range	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129.
Downlink Data	
Contention Slots (a.k.a. Control Slots)	
Broadcast Repeat Count	
Transmitter Output Power	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.
External Gain	
SM Receive Target Level	See Table 141 PMP 450m AP Radio attributes - 5 GHz on page 7-129
Multicast VC Data Rate	
Multicast Repeat Count	
Multicast Downlink CIR	
Control Message	
Receive Quality Debug	
Pager Reject Filter	In 900 MHz, Pager Reject filter is placed on the AP to block Pager signals which could cause interference to the whole band. The Pager signals typically operate in the 928-930 frequency range. When the filter is enabled, the signals of 920 MHz and above are attenuated which enables better reception of signals in the rest of the band. Note that the AP/SM should not be configured on the frequencies of 920 MHz and above when this filter is enabled.

Frame Alignment Legacy Mode	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page - PTP 450i BHM 5 GHz

The **Radio** page of PTP 450i BHM is explained in Table 145.

Table 145 PTP 450i BHM Radio page attributes – 5 GHz

Radio Configuration

Frequency Band :	5.4 GHz
Frequency Carrier :	5490.0
Channel Bandwidth :	20 MHz
Cyclic Prefix :	One Sixteenth
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Color Code :	254 (0—254)
Large VC data Q :	○ Enabled ◉ 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 :	○ Enabled ◉ Disabled
Frame Alignment Legacy Mode :	OFF Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

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

Attribute	Meaning
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 supported Frame Periods are: 5 ms and 2.5 ms.
Color Code	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. 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).
Large VC data Q	**Enable** Large VC Q for applications that burst data high rates. Large Qs may decrease effective throughput for TCP application. **Disable** Large VC Q if application need not handle bursts of data. Large Qs may decrease effective throughput for TCP application.
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. **Note** In order to prevent self-interference, the frame configuration needs to align. This includes Downlink Data, Max Range and Contention slots.
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 Series 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.
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 256-QAM) and per channel (polarization). **Note** Due to CPU load, this slightly degrades the packet during per second processing.
Frame Alignment Legacy Mode	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page – PTP 450i BHS 5 GHz

The **Radio** page of PTP 450i BHS is explained in Table 146.

Table 146 PTP 450i BHS Radio attributes – 5 GHz

Radio Configuration

Custom Radio Frequency Scan Selection List :

4.9 GHz

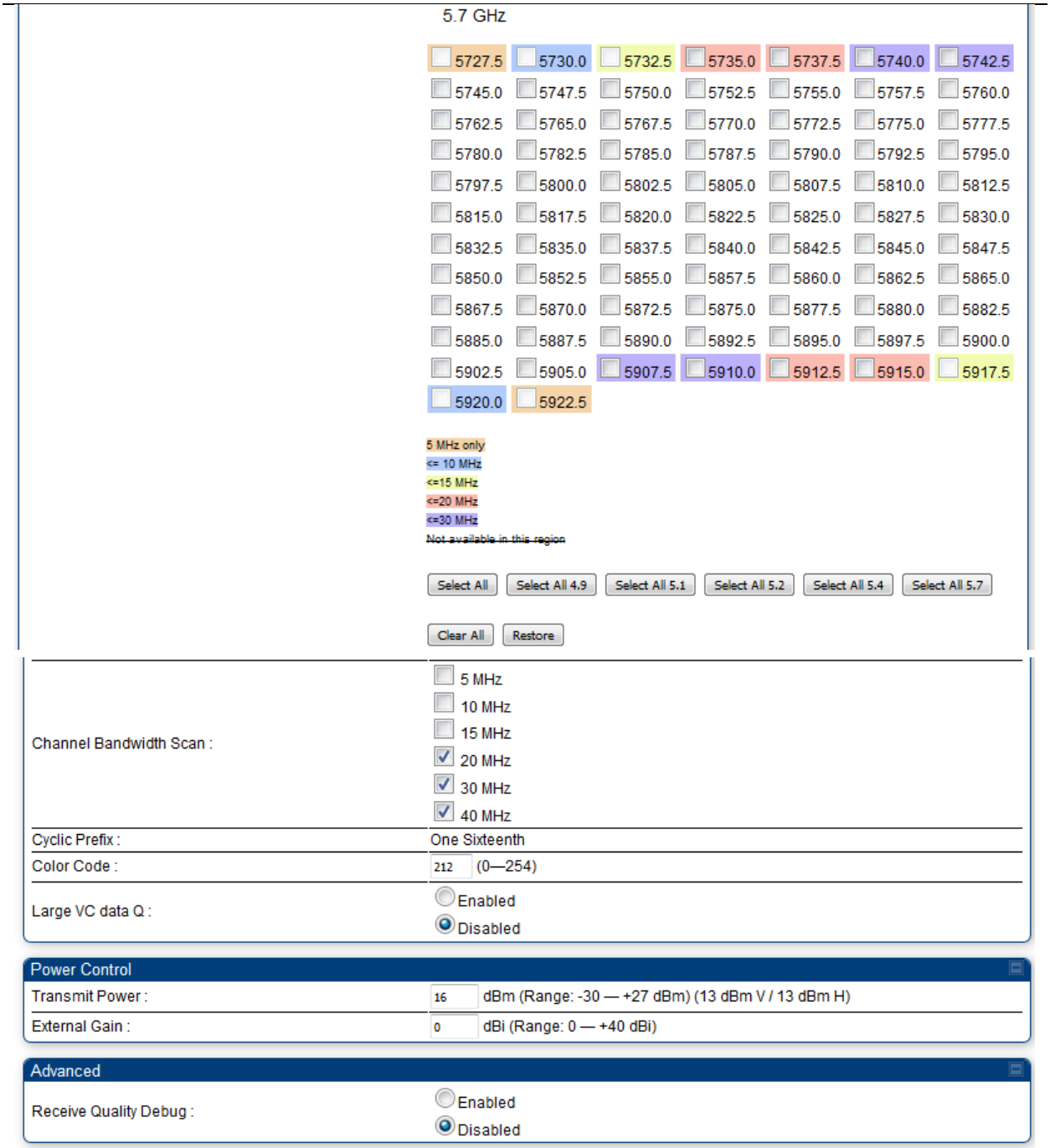
4905.000	4907.500	4910.000	4912.500	4915.000
4917.500	4920.000	4922.500	4925.000	4927.500
4930.000	4932.500	4935.000	4937.500	4940.000
4942.500	4945.000	4947.500	4950.000	4952.500
4955.000	4957.500	4960.000	4962.500	4965.000
4967.500	4970.000	4972.500	4975.000	4977.500
4980.000	4982.500	4985.000	4987.500	4990.000
4992.500	4995.000			

5.1 GHz

5152.5	5155.0	5157.5	5160.0	5162.5	5165.0	5167.5
5170.0	5172.5	5175.0	5177.5	5180.0	5182.5	5185.0
5187.5	5190.0	5192.5	5195.0	5197.5	5200.0	5202.5
5205.0	5207.5	5210.0	5212.5	5215.0	5217.5	5220.0
5222.5	5225.0	5227.5	5230.0	5232.5	5235.0	5237.5
5240.0	5242.5	5245.0	5247.5			

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				



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 7-171.
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	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 *must* match. Specify a value from 0 to 254. The color codes can be disabled, with the exception of the first color code.
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	Refer Table 145 PTP 450i BHM Radio page attributes – 5 GHz on page 7-147
External Gain	
Receive Quality Debug	

PMP 450b Series - configuring radio

Radio page – PMP 450b SM 5 GHz

The Radio page of PMP 450b SM is explained in Table 147.

Table 147 PMP 450b SM Radio attributes – 5 GHz

Radio Configuration

Custom Radio Frequency Scan Selection List :

4.9 GHz

No custom frequencies present.

5.1 GHz

5152.5	5155.0	5157.5	5160.0	5162.5	5165.0	5167.5
5170.0	5172.5	5175.0	5177.5	5180.0	5182.5	5185.0
5187.5	5190.0	5192.5	5195.0	5197.5	5200.0	5202.5
5205.0	5207.5	5210.0	5212.5	5215.0	5217.5	5220.0
5222.5	5225.0	5227.5	5230.0	5232.5	5235.0	5237.5
5240.0	5242.5	5245.0	5247.5			

5.2 GHz

5252.5	5255.0	5257.5	5260.0	5262.5	5265.0	5267.5
5270.0	5272.5	5275.0	5277.5	5280.0	5282.5	5285.0
5287.5	5290.0	5292.5	5295.0	5297.5	5300.0	5302.5
5305.0	5307.5	5310.0	5312.5	5315.0	5317.5	5320.0
5322.5	5325.0	5327.5	5330.0	5332.5	5335.0	5337.5
5340.0	5342.5	5345.0	5347.5			

5.4 GHz

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

5.7 GHz

5727.5	5730.0	5732.5	5735.0	5737.5	5740.0	5742.5
5745.0	5747.5	5750.0	5752.5	5755.0	5757.5	5760.0
5762.5	5765.0	5767.5	5770.0	5772.5	5775.0	5777.5
5780.0	5782.5	5785.0	5787.5	5790.0	5792.5	5795.0
5797.5	5800.0	5802.5	5805.0	5807.5	5810.0	5812.5
5815.0	5817.5	5820.0	5822.5	5825.0	5827.5	5830.0
5832.5	5835.0	5837.5	5840.0	5842.5	5845.0	5847.5
5850.0	5852.5	5855.0	5857.5	5860.0	5862.5	5865.0
5867.5	5870.0	5872.5	5875.0	5877.5	5880.0	5882.5
5885.0	5887.5	5890.0	5892.5	5895.0	5897.5	5900.0
5902.5	5905.0	5907.5	5910.0	5912.5	5915.0	5917.5
5920.0	5922.5					

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

Select All | Select All 4.9 | Select All 5.1 | Select All 5.2 | Select All 5.4 | Select All 5.7

Clear All | Restore

Channel Bandwidth Scan :	☐ 5 MHz ☑ 10 MHz ☐ 15 MHz ☐ 20 MHz ☐ 30 MHz ☐ 40 MHz
Cyclic Prefix :	One Sixteenth
AP Selection Method :	○ Power Level ◉ Optimize for Throughput
Color Code 1 :	182 (0—254) / Priority Primary
Installation Color Code :	○ Enabled ◉ Disabled
Large VC data Q :	○ Enabled ◉ Disabled

Additional Color Codes

Color Code : 0 (0—254) / Priority Primary

Add/Modify Color Code | Remove Color Code

Additional Color Codes Table

No additional color codes configured

Power Control

External Gain : 0 dBi (Range: 0 — +40 dBi)

Advanced

Receive Quality Debug : ○ Enabled ◉ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-171.
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 AP scanning is executed.
AP Selection Method	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. **Power Level**: AP selection based solely on power level **Note** For operation with a PMP 450m AP, select the Power Level option *or* **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).
Color Code 1	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 *must* match. Specify a value from 0 to 254. Color code is not a security feature. Instead, color code is a management feature, typically for assigning each sector a different color code. The default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes). 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.

	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 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	This value represents the antenna gain. For ODUs with integrated antenna, this is set at the correct value in the factory. 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.
Large VC data Queue	SM 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 7-174) and cannot see it in the pull down menu.

PMP/PTP 450 Series – configuring radio

Radio page - PMP 450 AP 5 GHz

The **Radio** tab of the AP for 5 GHz is as shown in Table 148.

Table 148 PMP 450 AP Radio attributes - 5 GHz

Radio Configuration	
Frequency Band :	5.4 GHz
Frequency Carrier :	5480.0
Channel Bandwidth :	20 MHz
Cyclic Prefix :	One Sixteenth
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Color Code :	5 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	◉ Enabled ○ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	16 dBm (Range: -30 — +22 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	
PMP 430 SM Registration :	◉ Allow ○ Deny
Control Messages :	○ SISO ◉ MIMO-A
PMP 430 Interop Mode :	○ SISO ◉ MIMO-A
Receive Quality Debug :	○ Enabled ◉ Disabled
Frame Alignment Legacy Mode :	OFF Choose Legacy Mode setting from the table below based on colocated radio's software revision and sync source:

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

Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.
PMP 430 SM Registration	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.
PMP 450/430 Legacy Mode	
Control Messages	
PMP 430 Interop Mode	
Receive Quality Debug	
Frame Alignment Legacy Mode	

Radio page - PMP 450 AP 3.65 GHz

Table 149 PMP 450 AP Radio attributes - 3.65 GHz

Radio Configuration	
Frequency Carrier :	3650.000
Channel Bandwidth :	20 MHz
Cyclic Prefix :	One Sixteenth
Frame Period :	○ 5.0 ms ◉ 2.5 ms
Color Code :	5 (0—254)
Subscriber Color Code Rescan (When not on a Primary Color Code) :	0 Minutes (0 — 43200)
Subscriber Color Code Wait Period for Idle :	0 Minutes (0 — 60)
Installation Color Code :	○ Enabled ◉ Disabled

Frame Configuration	
Max Range :	2 Miles (Range: 1 — 40 miles)
Downlink Data :	75 % (Range: 15 — 85 %)
Contention Slots :	3 (Range: 1 — 15)
Broadcast Repeat Count :	2 (Range : 0 — 2)

Power Control	
Transmit Power :	25 dBm (Range: -30 — +25 dBm) (22 dBm A / 22 dBm B)
External Gain :	0 dB (Range: 0 — +70 dB)
SM Receive Target Level :	-52 dBm (Range : -77 — -37 dBm) combined power
Adjacent Channel Support :	○ Enabled ◉ Disabled

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	
Control Messages :	○ SISO ◉ MIMO-A
Receive Quality Debug :	○ Enabled ◉ Disabled

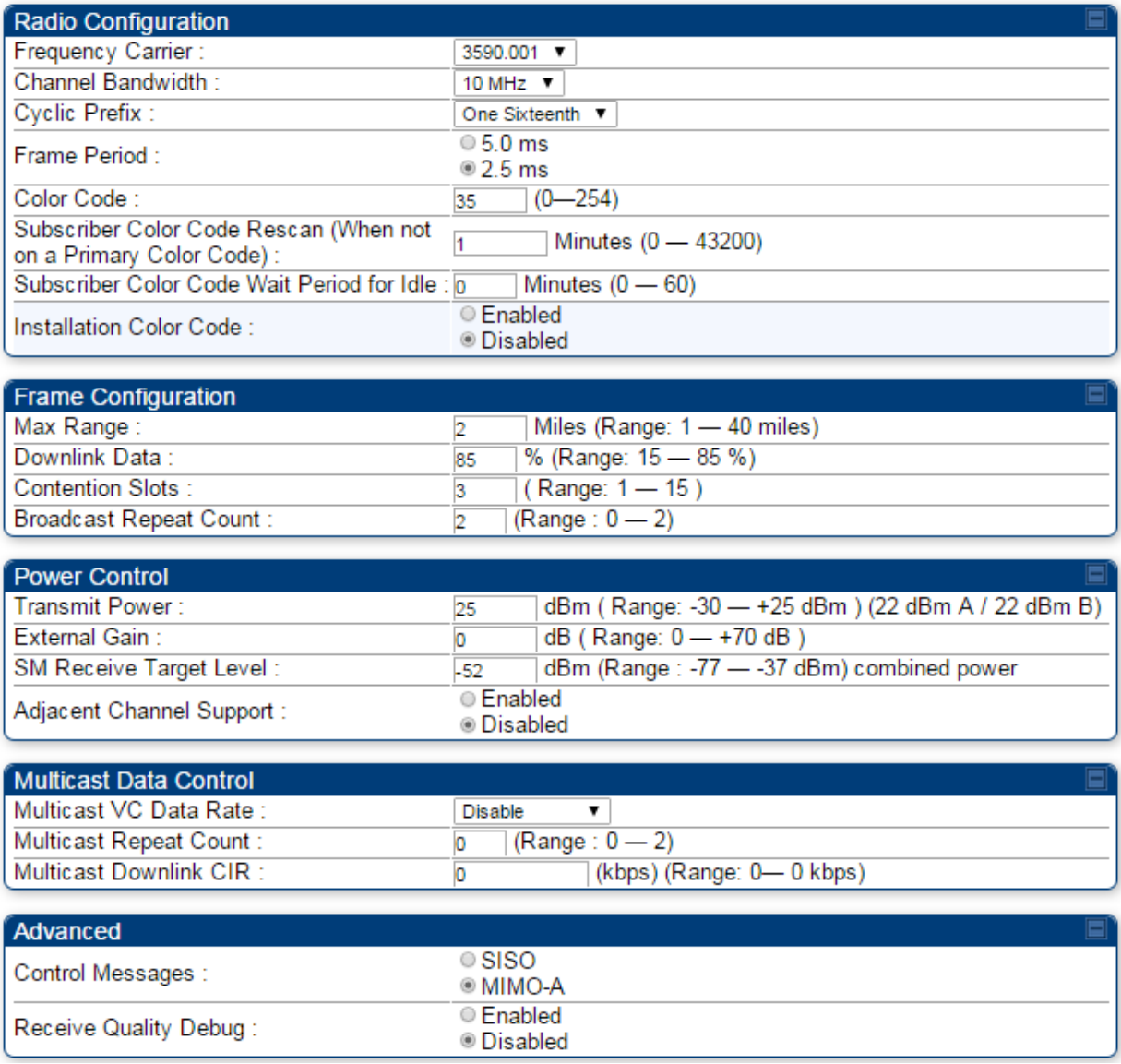
Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Note

When the Channel bandwidth is updated from 20 MHz to 30 MHz not more than 59 subscriber can be registered.

Radio page - PMP 450 AP 3.5 GHz

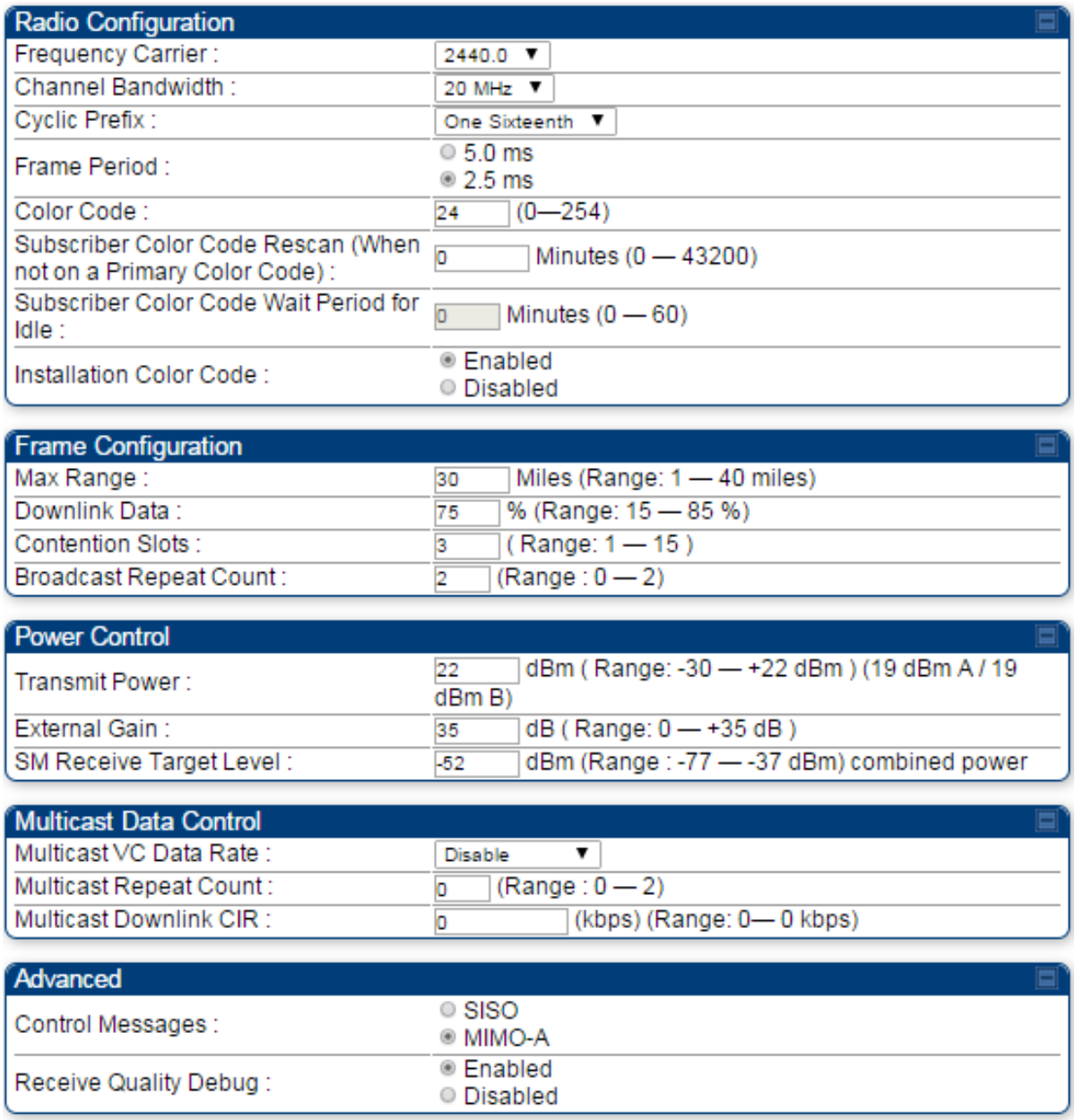
Table 150 PMP 450 AP Radio attributes - 3.5 GHz



Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page - PMP 450 AP 2.4 GHz

Table 151 PMP 450 AP Radio attributes - 2.4 GHz



Attribute	Meaning
Radio Configuration, Frame Configuration, Power Control, Multicast Data Control and Advance tab	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page - PMP 450 SM 5 GHz

Table 152 PMP 450 SM Radio attributes – 5 GHz

Radio Configuration

Custom Radio Frequency Scan Selection List :

5.4 GHz

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

5.7 GHz

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

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

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

Channel Bandwidth Scan :	☐ 5 MHz ☐ 10 MHz ☐ 15 MHz ☑ 20 MHz ☐ 30 MHz ☑ 40 MHz
Cyclic Prefix :	One Sixteenth
AP Selection Method :	○ Power Level ◉ Optimize for Throughput
Color Code 1 :	212 (0—254) / Priority Primary
Installation Color Code :	◉ Enabled ○ Disabled
Large VC data Q :	○ Enabled ◉ Disabled

Additional Color Codes

Color Code : 0 (0—254) / Priority Primary

Add/Modify Color Code | Remove Color Code

Additional Color Codes Table

Color Code	Priority
0	Primary
10	Primary
20	Primary
30	Secondary
50	Tertiary
100	Tertiary
120	Primary
130	Secondary
140	Secondary
1	Primary
200	Secondary

Power Control

External Gain : 0 dBi (Range: 0 — +40 dBi)

Advanced

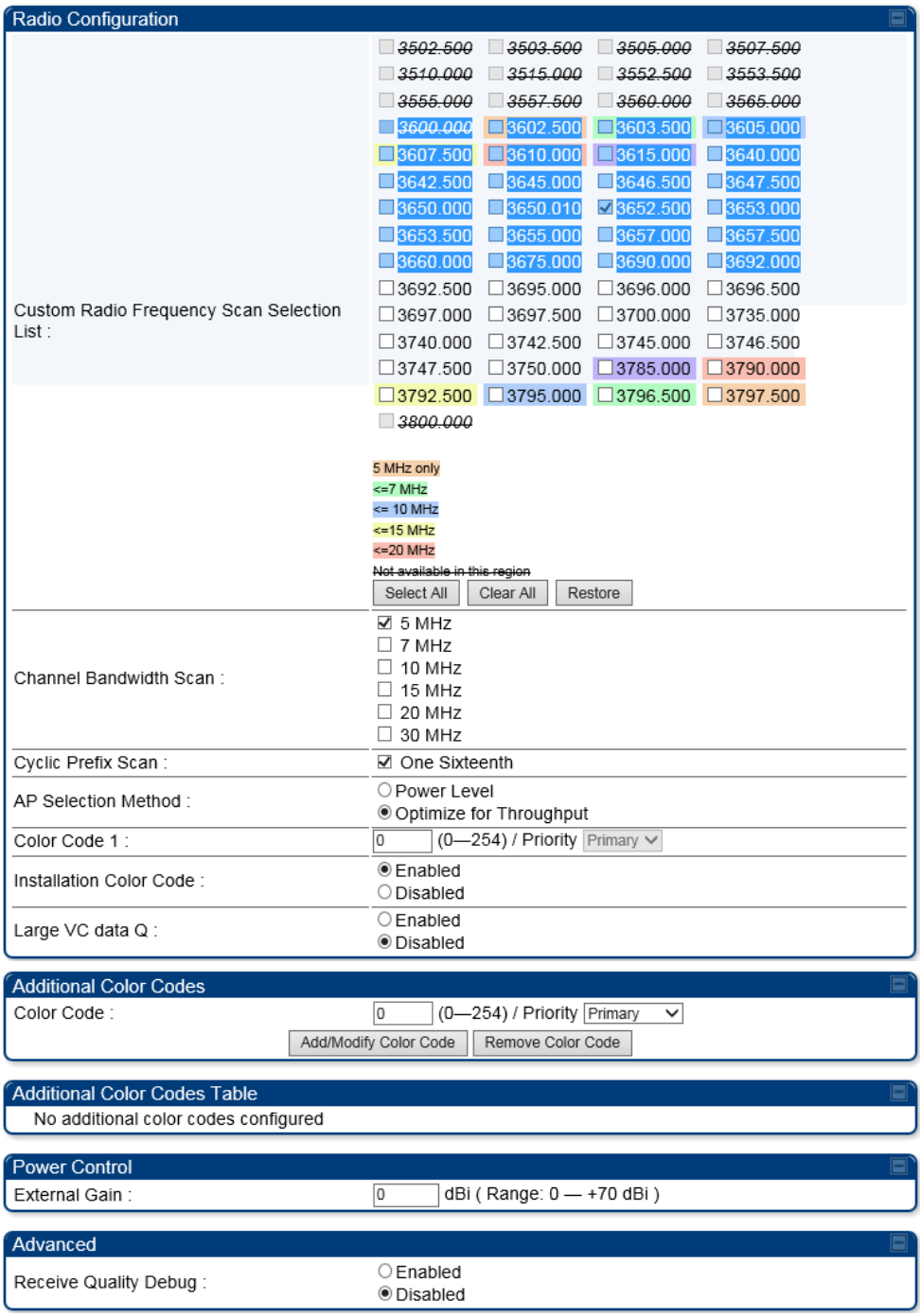
Receive Quality Debug : ○ Enabled ◉ Disabled

Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-171.

See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page - PMP 450 SM 3.65 GHz

Table 153 PMP 450 SM Radio attributes – 3.65 GHz

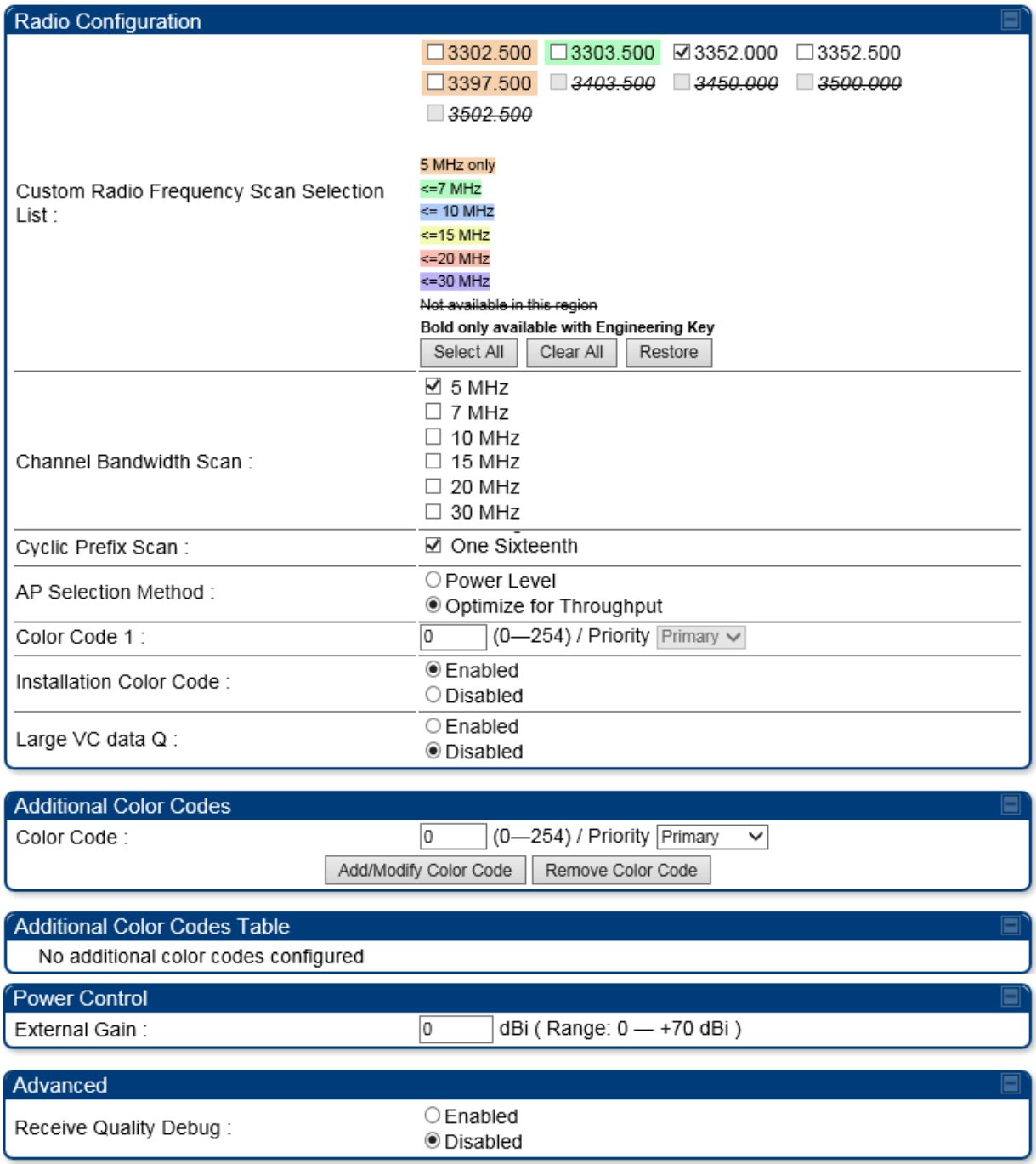


Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-171.

See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page - PMP 450 SM 3.5 GHz

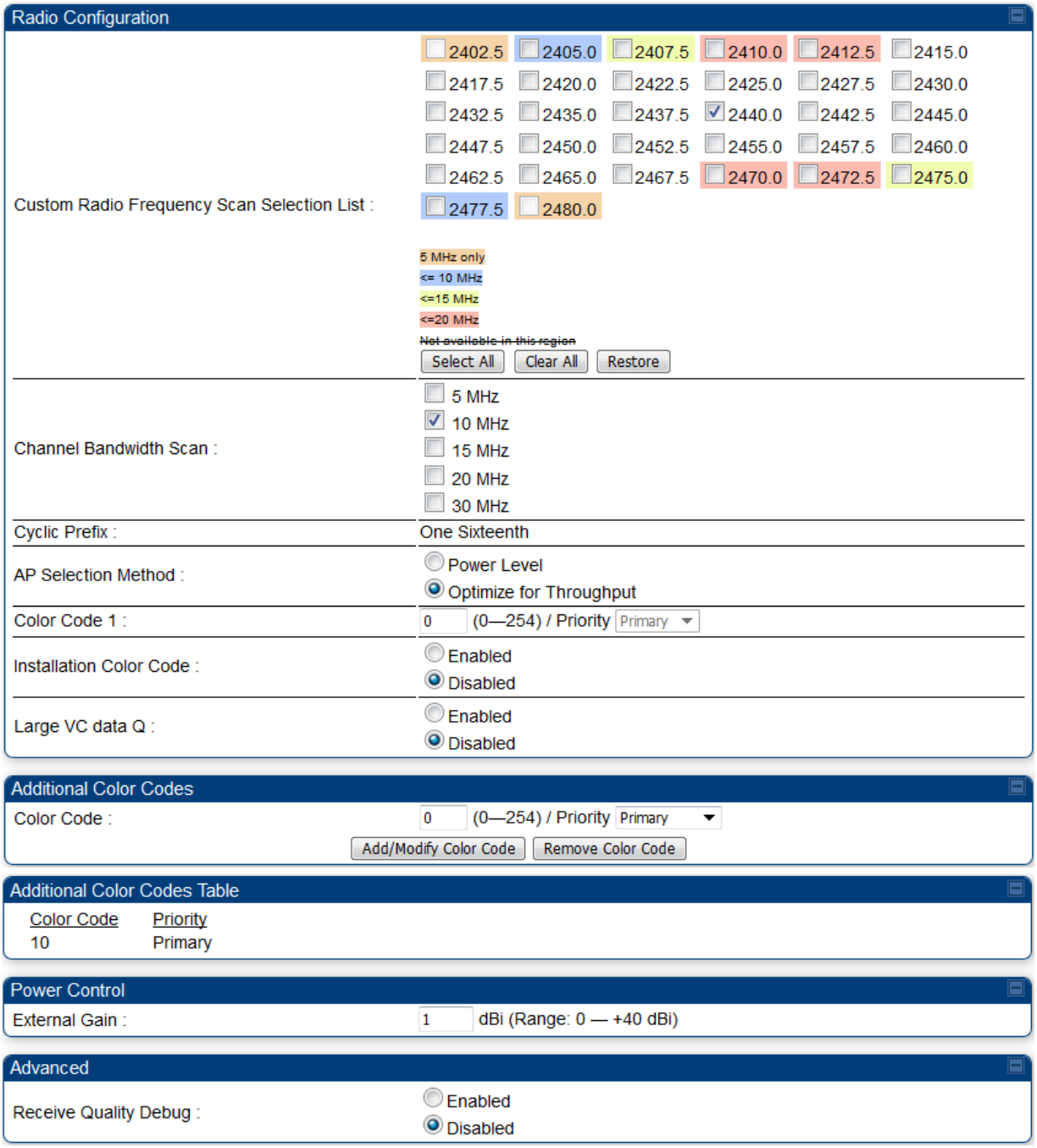
Table 154 PMP 450 SM Radio attributes – 3.5 GHz



Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-171.
See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.	

Radio page - PMP 450 SM 2.4 GHz

Table 155 PMP 450 SM Radio attributes – 2.4 GHz

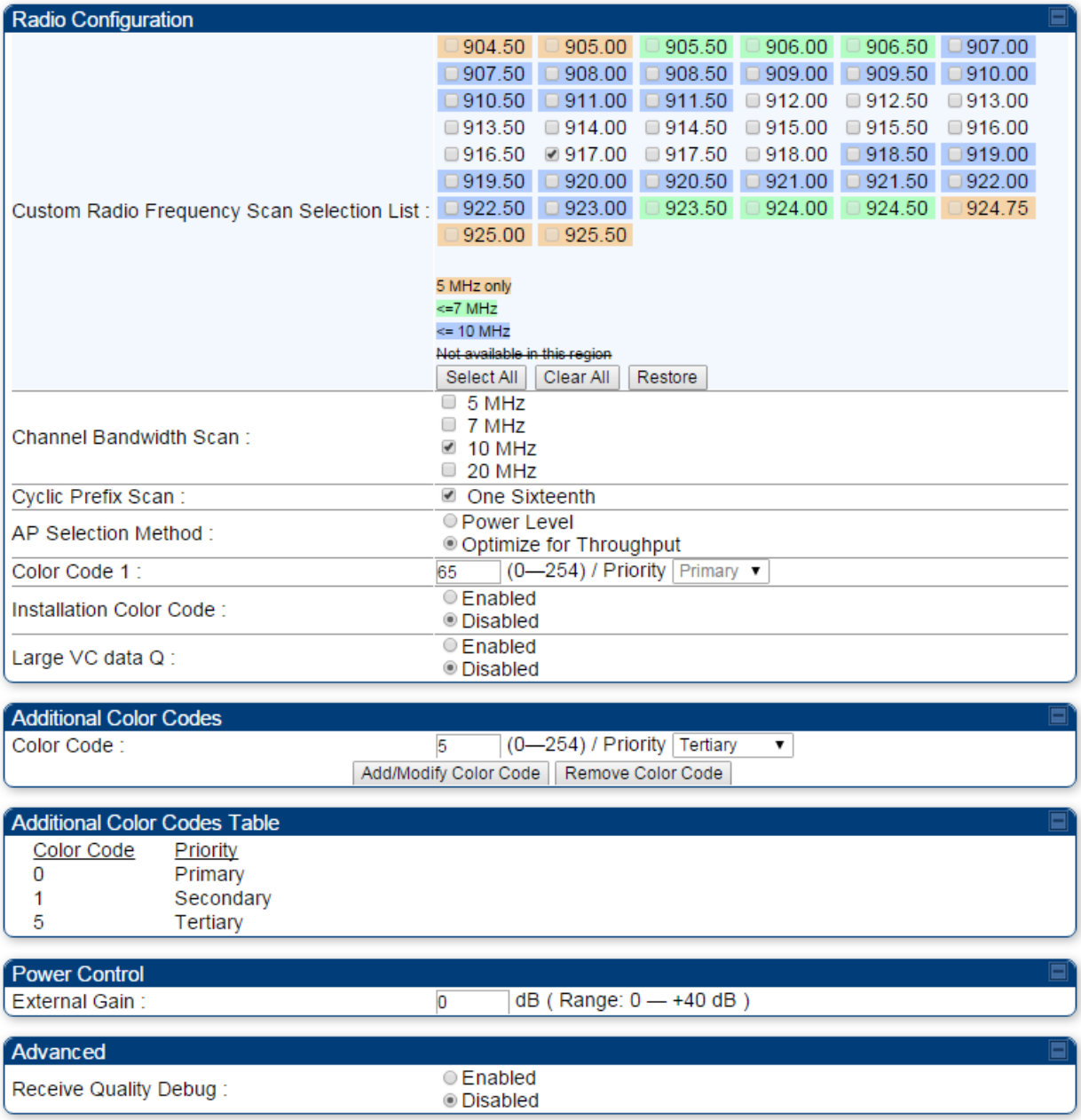


Attribute	Meaning
Custom Radio Frequency Scan Selection List	Check the frequencies that SM has to scan for AP transmissions. See Radio Frequency Scan Selection List on page 7-171.

See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

Radio page - PMP 450 SM 900 MHz

Table 156 PMP 450 SM Radio attributes –900 MHz



Attribute	Meaning
Custom Radio Frequency Scan Selection List	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.
Channel Bandwidth Scan	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.
Cyclic Prefix Scan	
AP Selection Method	

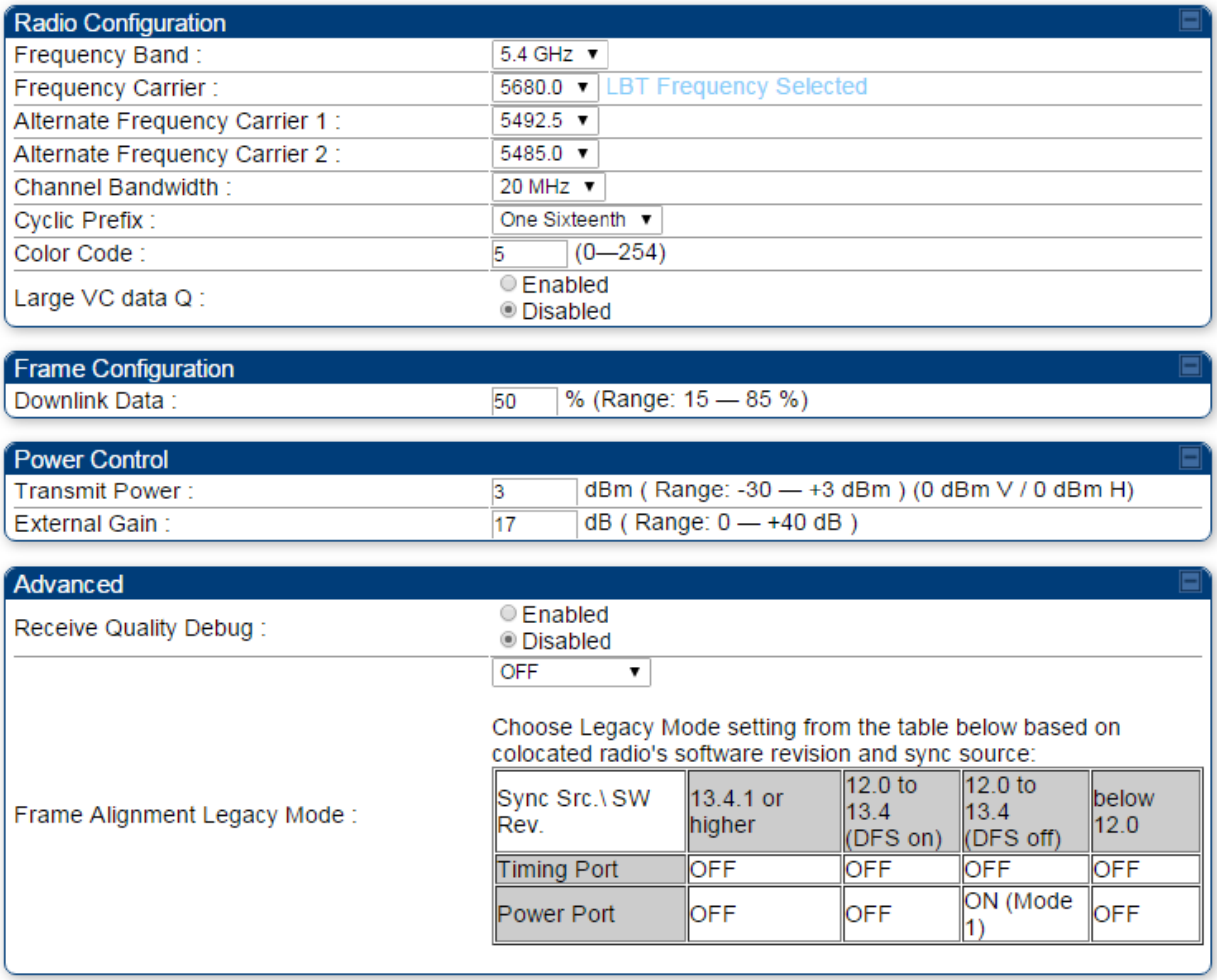
Color Code 1	
Installation Color Code	
Large VC data Queue	
Color Code	
External Gain	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135
Receive Quality Debug	See Table 142 PMP 450i AP Radio attributes - 5 GHz on page 7-135.

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 7-174) and cannot see it in the pull down menu.

Radio page - PTP 450 BHM 5 GHz

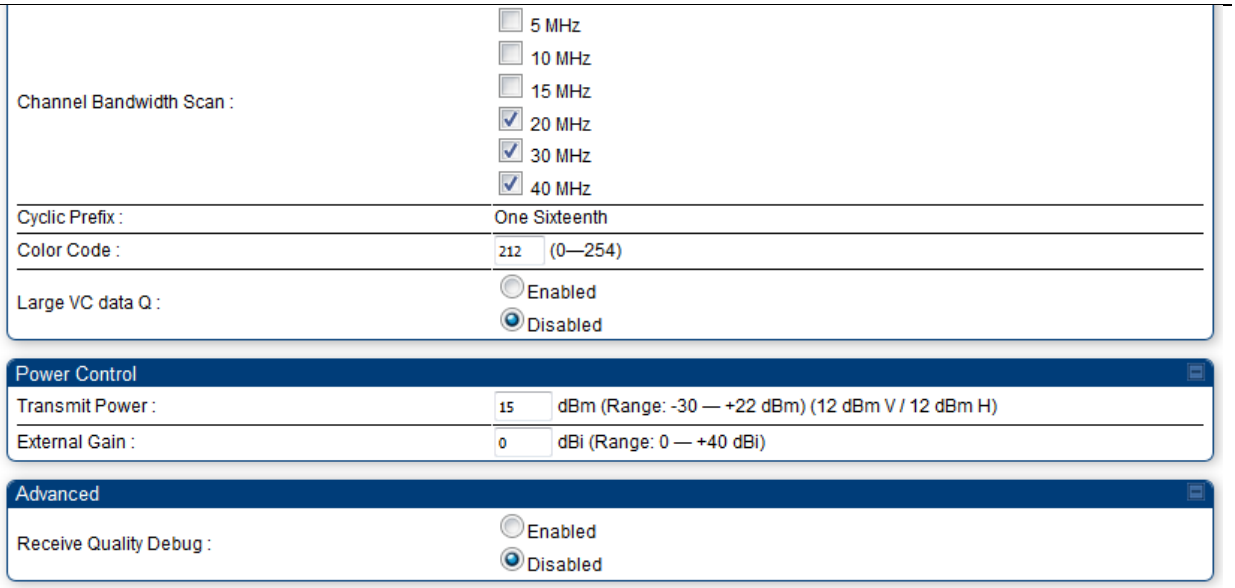
Table 157 PTP 450 BHM Radio attributes –5 GHz



Attribute	Meaning
Refer Table 145 PTP 450i BHM Radio page attributes – 5 GHz on page 7-147 for all parameters details.	

Radio page - PTP 450 BHS 5 GHz

Table 158 PTP 450 BHM Radio attributes –5 GHz



Attribute	Meaning
Refer Table 146 PTP 450i BHS Radio attributes – 5 GHz on page 7-150 for all parameters details.	

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

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

Note

- Actual Multicast CIR honored by the AP = Configured Multicast CIR/ (Multicast Repeat Count + 1).
- Increasing the Multicast data rate has no impact on the Unicast data rate.
- For multicast and unicast traffic mix scenario examples, see Table 159.

Table 159 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 450 Platform Family AP. The SM displays the multicast row if it is a PMP 450 Platform Family.

Figure 147 Multicast VC statistics

Data VC Statistics (CoS: 00 = Lowest Priority, 07 = Highest Priority)

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

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	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 148.

Figure 148 Multicast scheduler statistics

Radio Statistics

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

Custom Frequencies page

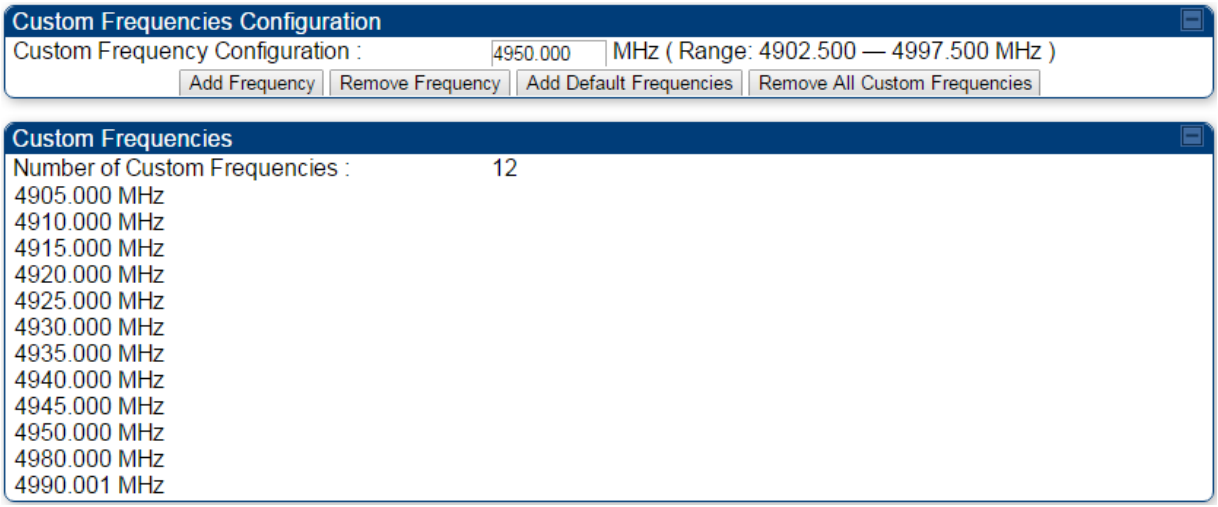
In addition to the **Radio** tab, AP/SM/BH has another tab called **Custom Frequencies** as shown in Table 160.

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

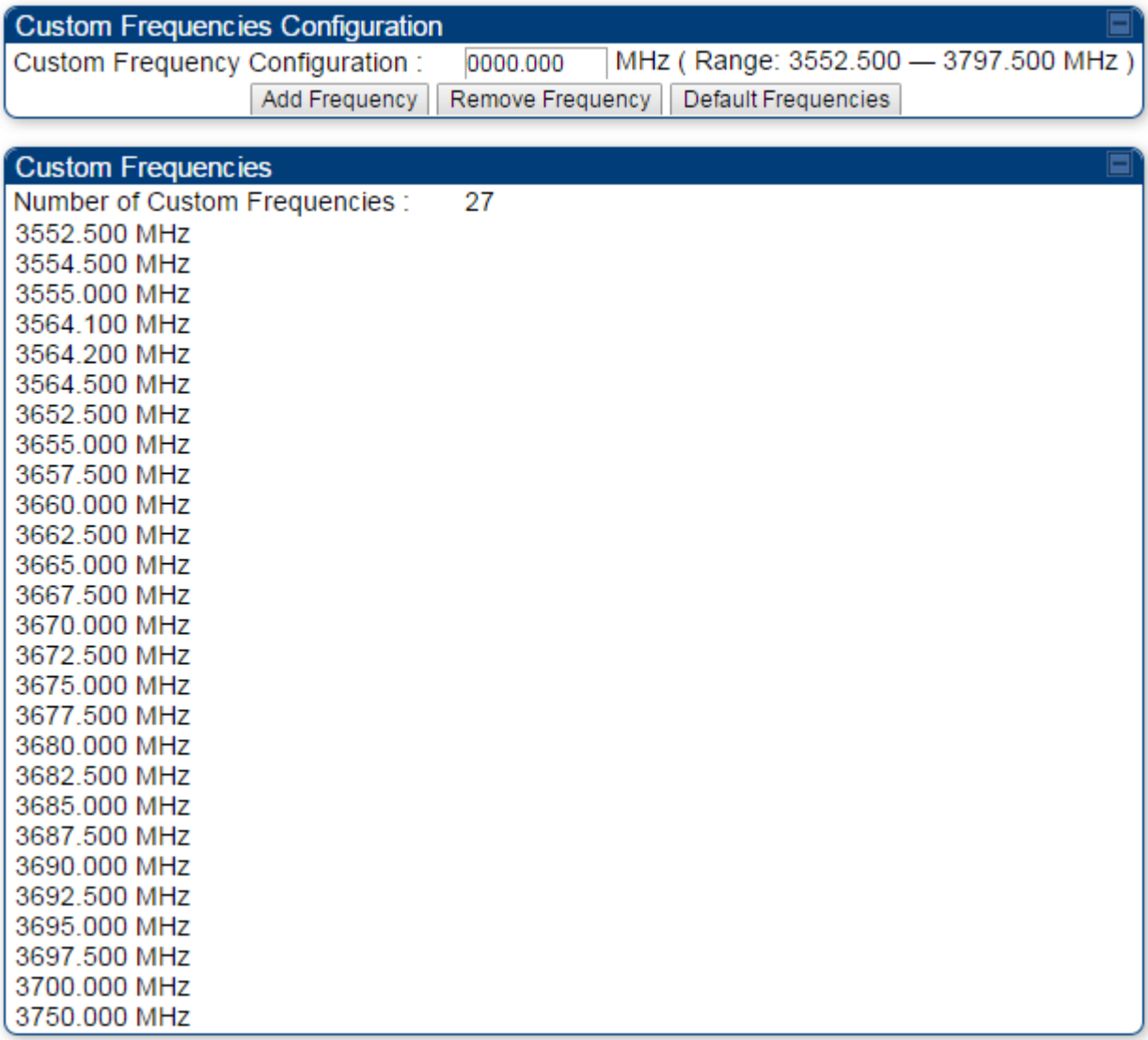
Ensure that a customer frequency exists before using SNMP to set the radio to a Custom Frequency.

Table 160 450 Platform Family AP/SM/BH Custom Frequencies page – 5 GHz



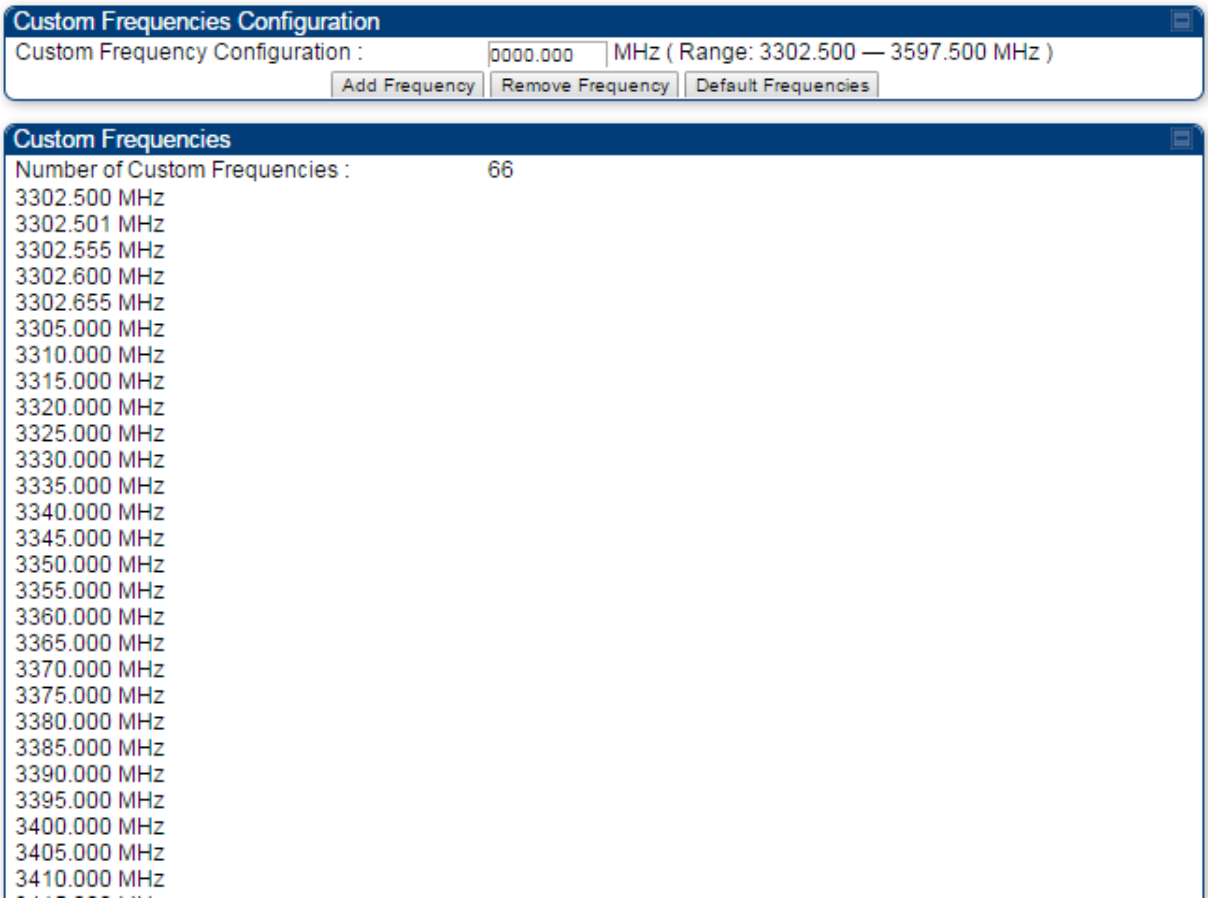
Attribute	Meaning
Custom Frequency Configuration	Custom frequencies with a channel raster of 1 KHz can be added from the available range by keying in the frequency and then clicking the **Add Frequency** button. Click **Remove Frequency** button to delete a specific frequency keyed in the text box. Click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

Table 161 PMP/PTP 450 SM/BH Custom Frequencies page – 3.65 GHz



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

Table 162 PMP/PTP 450 SM/BH Custom Frequencies page – 3.5 GHz



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

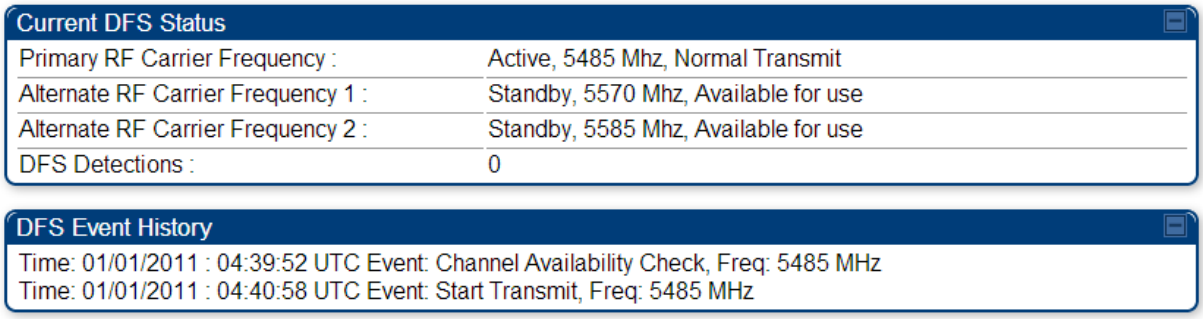
DFS for 5 GHz Radios

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

- Country Code
- Primary Frequency
- Alternate 1 and Alternate 2 Frequencies
- External Antenna Gain

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

Figure 149 AP DFS Status



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

DFS Event History

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

DFS operation

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

The details of DFS operation for each Country Code, including whether DFS is active on the AP, SM, and which DFS regulations apply is shown in Table 261 on page 10-48.

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 SMs in the sector are shown in the table below.

Table 163 Contention slots and number of SMs

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

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 450/450i Series 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.

For co-location of radios with mismatched configuration parameters, see the co-location tool available here:

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

MIMO-A mode of operation

450 Platform Family 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 radio sends different streams of data over the two antennas whereas with MIMO-A, the radio uses a scheme that tries to optimize coverage by transmitting the same data over both antennas. This redundancy improves the signal to noise ratio at the receiver making it more robust, at the cost of throughput.

In addition to introducing MIMO-A modes, improvements have been made to the existing rate adapt algorithm to switch between MIMO-A and MIMO-B seamlessly without any intervention or added configuration by the operator. The various modulation levels used by the 450 Platform Family are shown in Table 164.

Table 164 450 Platform Family 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
265-QAM	8X MIMO-B	4X MIMO-A

System Performance

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

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

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

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

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

Table 165 Co-channel Interference per (CCI) MCS

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

Table 166 Adjacent Channel Interference (ACI) per MCS

MCS of Victim	MCS of Interferer	Channel BW (MHz)	ACI	Guard Band
1X (QPSK SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
2X (16-QAM SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
3X (64-QAM SISO)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
1X (QPSK MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-13 dB	None
2X (16-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-13 dB	None

3X (64-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-13 dB	None
4X (256-QAM MIMO-A)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-10 dB	None
2X (QPSK MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
4X (16-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
6X (64-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-16 dB	None
8X (256-QAM MIMO-B)	6X (64-QAM MIMO-B)	5, 7, 10, 15, 20, 30, or 40	-10 dB	None

Guard Band

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

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

Improved PPS performance of 450 Platform Family

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

Through hardware and software enhancements, the PPS performance of the PMP 450i Series AP and PMP 450b SM has been improved to 40k packets/second, measured through a standard RFC2544 test using 64 bytes packets. With this enhancement, operators are able to provide higher bandwidth including better VoIP and video services to end customers using existing SM deployments.

PMP 450m supports 100k packets/second.

Setting up SNMP agent

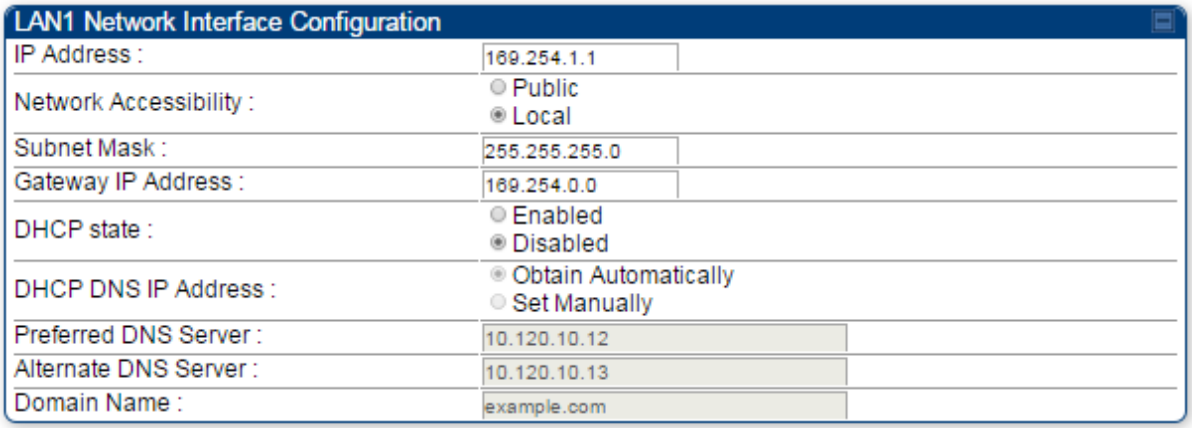
Operators may use SNMP commands to set configuration parameters and retrieve data from the AP and SM modules. Also, if enabled, when an event occurs, the SNMP agent on the 450 Platform Family sends a trap to whatever SNMP trap receivers configured in the management network.

- SNMPv2c
- SNMPv3

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

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

Table 167 LAN1 Network Interface Configuration tab of IP page attributes



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

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

Configuring SNMP

The SNMP page configuration is explained below.

Note

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

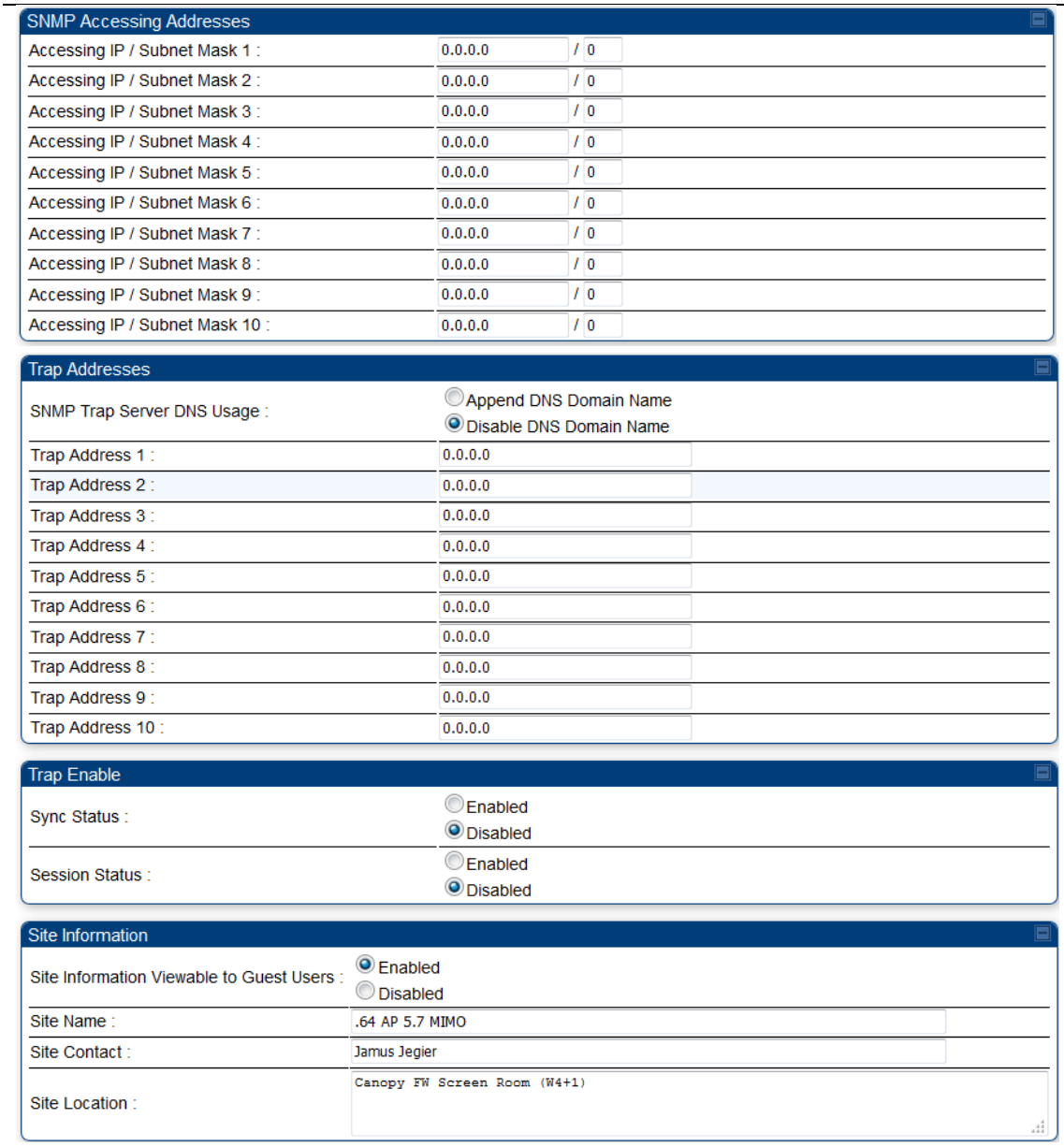
SNMP page – AP/SM/BHM/BHS

The SNMP page is explained in Table 168.

Table 168 SNMP page attributes

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

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



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 devices. The default values for the Read-Only users is: • Username = Canopyro • Authentication Password = authCanopyro • Privacy Password = privacyCanopyro
SNMPv3 Read/Write User	Read-write user by default is disabled. The default values for the Read/Write users is : • Username = Canopy • Authentication Password = authCanopy • Privacy Password = privacyCanopy
Additional SNMP v3 User 1	This field allows to configure the Additional SNMP v3 User 1. The configurations include: • Enable/Disable User: These fields allow to enable or disable the user using the Enable User or Disable User radio buttons. • Authorizaton Key: This field allows to configure an authorization key for the user. • Privacy Key: This field allows to configure a privacy key for the user. **Note:** Set SNMP v3 Security Level field to :auth,priv to enable the Authorization Key and Privacy Key fields. Enabled User can be set with following privacy settings: • ReadWrite User • ReadOnly User

Additional SNMP v3 User 2	This field allows to configure the Additional SNMP v3 User 2. The configurations include: • Enable/Disable User: These fields allow to enable or disable the user using the Enable User or Disable User radio buttons. • Authorizaton Key: This field allows to configure an authorization key for the user. • Privacy Key: This field allows to configure a privacy key for the user. NOTE Set SNMP v3 Security Level field to :auth,priv to enable the Authorization Key and Privacy Key fields. Enabled User can be set with following Privacy settings: • ReadWrite User • ReadOnly User
Additional SNMP v3 User 3	This field allows to configure the Additional SNMP v3 User 3. The configurations include: • Enable/Disable User: These fields allow to enable or disable the user using the Enable User or Disable User radio buttons. • Authorizaton Key: This field allows to configure an authorization key for the user. • Privacy Key: This field allows to configure a privacy key for the user. NOTE Set SNMP v3 Security Level field to :auth,priv to enable the Authorization Key and Privacy Key fields. Enabled User can be set with following Privacy settings: • ReadWrite User • ReadOnly User
SNMPv3 Trap Configuration	When enabling transmission of SNMPv3 traps the read-only or read-write user credentials must be used and selected properly in order for the SNMP manager to correctly interpret the traps. By default transmission of SNMPv3 traps is disabled and all traps sent from the radios are in SNMPv2c format.
Accessing IP / Subnet Mask *1 to 10*	Specify the addresses that are allowed to send SNMP requests to this AP. The NMS has an address that is among these addresses (this subnet). You must enter both • The network IP address in the form xxx.xxx.xxx.xxx • The CIDR (Classless Interdomain Routing) prefix length in the form /xx For example: • the /16 in 198.32.0.0/16 specifies a subnet mask of 255.255.0.0 (the first 16 bits in the address range are identical among all members of the subnet).

	• 192.168.102.0 specifies that any device whose IP address is in the range 192.168.102.0 to 192.168.102.254 can send SNMP requests to the AP, presuming that the device supplies the correct **Community String** value. The default treatment is to allow all networks access. For more information on CIDR, execute an Internet search on "Classless Interdomain Routing." You are allowed to specify as many as 10 different accessing IP address, subnet mask combinations. **RECOMMENDATION:** The subscriber can access the SM/BHS by changing the subscriber device to the accessing subnet. This hazard exists because the **Community String** and **Accessing Subnet** are both visible parameters. To avoid this hazard, configure the SM/BHS to filter (block) SNMP requests.
SNMP Trap Server DNS Usage	The management DNS domain name may be toggled such that the name of the trap server only needs to be specified and the DNS domain name is automatically appended to that name. The default SNMP trap server addresses for all 10 available servers is 0.0.0.0 with the appending of the DNS domain name disabled.
Trap Address *1 to 10*	Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) or DNS names to which SNMP traps must be sent. Traps inform Wireless Manager or an NMS that something has occurred. For example, trap information is sent • after a reboot of the module. • when an NMS attempts to access agent information but either • supplied an inappropriate community string or SNMP version number. • is associated with a subnet to which access is disallowed.
Trap Enable, Sync Status	If the sync status traps (sync lost and sync regained) have to be sent to Wireless Manager or an NMS, select **Enabled**. If these traps have to be suppressed, select **Disabled**.
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 *sysName* SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.
Site Contact	Enter contact information for the module administrator. This parameter is written into the *sysContact* SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.

Site Location	Enter information about the physical location of the module. This parameter is written into the *sysLocation* SNMP MIB-II object and can be polled by Wireless Manager or an NMS. The buffer size for this field is 128 characters.

Configuring syslog

450 Platform Family includes:

- Syslog event logging
- Configuring system logging

Syslog event logging

Following events are logged in syslog as explained in Table 169.

Table 169 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.

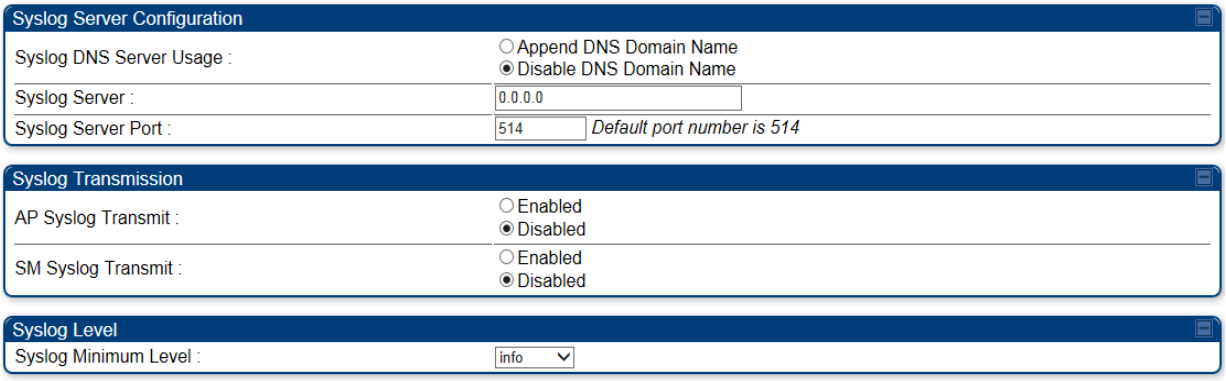
Configuring system logging

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 170.

Table 170 Syslog Configuration attributes - AP

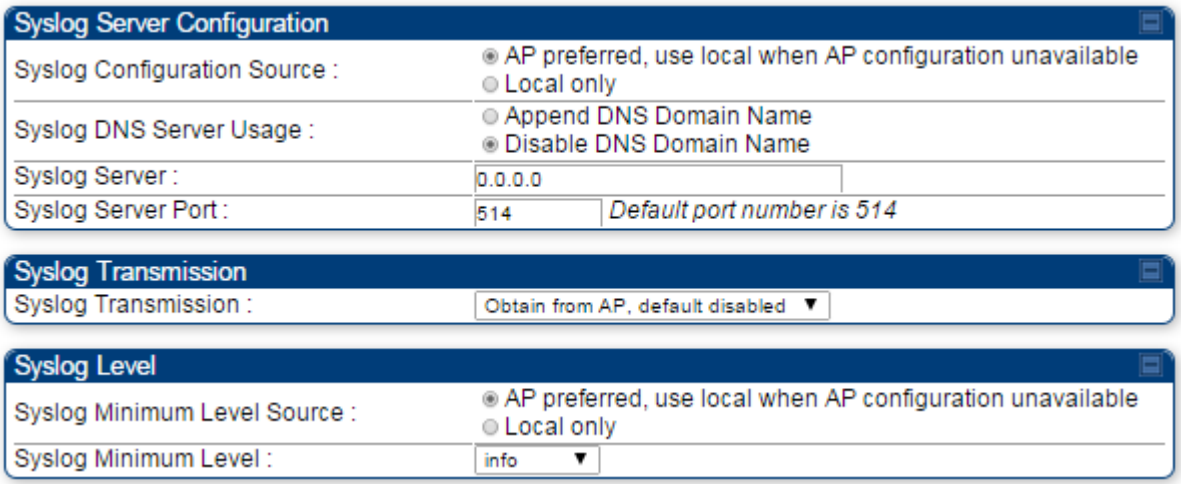


Attribute	Meaning
Syslog DNS Server Usage	To configure the AP/BHM to append or not append the DNS server name to the syslog server name.
Syslog Server	The dotted decimal or DNS name of the syslog server address.
Syslog Server Port	The syslog server port (default 514) to which syslog messaging is sent.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

Syslog page of SM

To configure system logging, select the menu option **Configuration > Syslog**. The Syslog Configuration page is shown in Table 171.

Table 171 Syslog Configuration attributes - SM



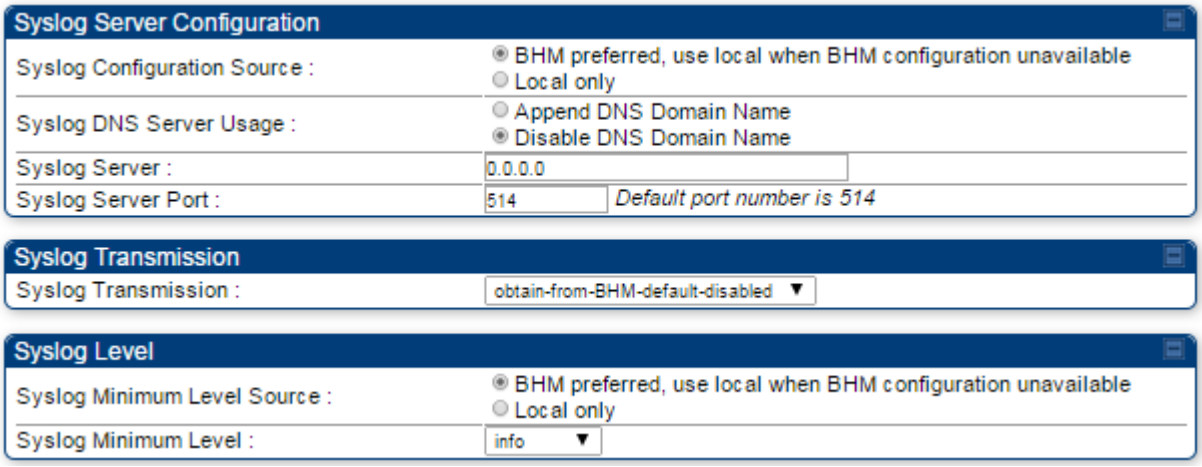
Attribute	Meaning
Syslog Configuration Source	This control determines whether the SM will attempt to use the syslog server definition from the AP, or whether it will use a local server definition. When set to **AP preferred, use local when AP configuration unavailable**, and if the SM can register with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

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

Syslog page of BHS

The Syslog Configuration page is shown in Table 172.

Table 172 Syslog Configuration attributes - BHS



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

	whether it sends syslog messages. This allows an operator to override the BHM settings for individual BHSs in a sector.
Syslog Minimum Level Source	This control determines whether the BHS attempts to use the minimum syslog level defined by the BHM, or whether it uses a local defined value using the **Syslog Minimum Level** parameter. • When set to **BHM preferred, use local when BHM configuration unavailable**, and if the BHS can register with a BHM, then it uses the Syslog Minimum Level defined on that BHM. If the BHS cannot register then it uses its own Syslog Minimum Level setting. When set to **Local only** the BHS will always use its own Syslog Minimum Level setting and ignores the BHM's setting.
Syslog Minimum Level	This provides a selection for the minimum syslog message severity that is sent to the syslog server. Values range from fatal (highest severity and least verbose) to info (lowest severity, maximum verbosity). For example: If the Syslog Minimum Level is set to notice, then only messages with severity notice and above are sent.

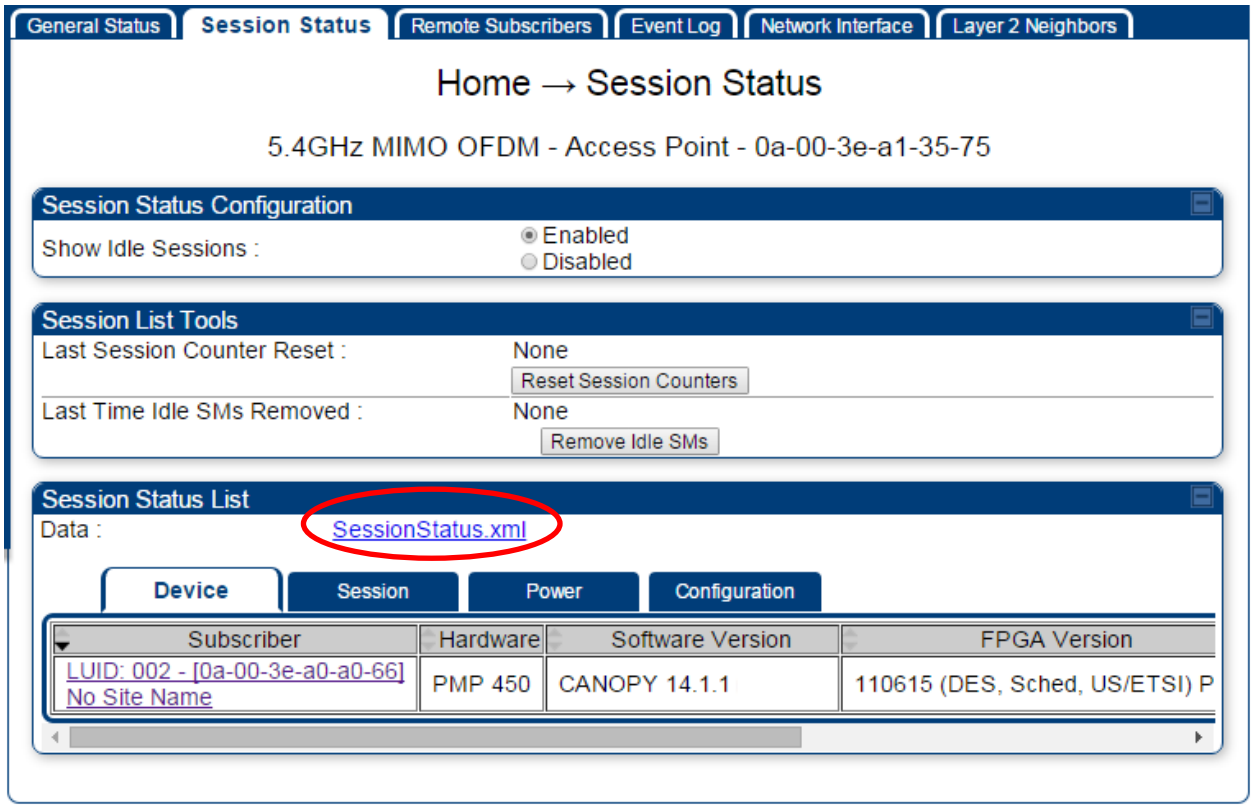
Configuring remote access

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

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

For example, to access one of the SMs, click **LUID: 002 – [0a-00-3e-37-b9-fd]**, as shown in Figure 150.

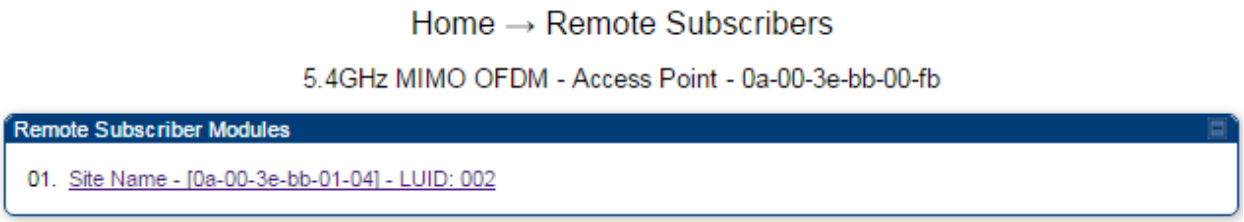
Figure 150 AP Session Status page



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

To access any one of the SMs, click 450 Platform Family - SM hyperlink, as shown in Figure 151.

Figure 151 AP Remote Subscribers page



Monitoring the Link

Link monitoring procedure

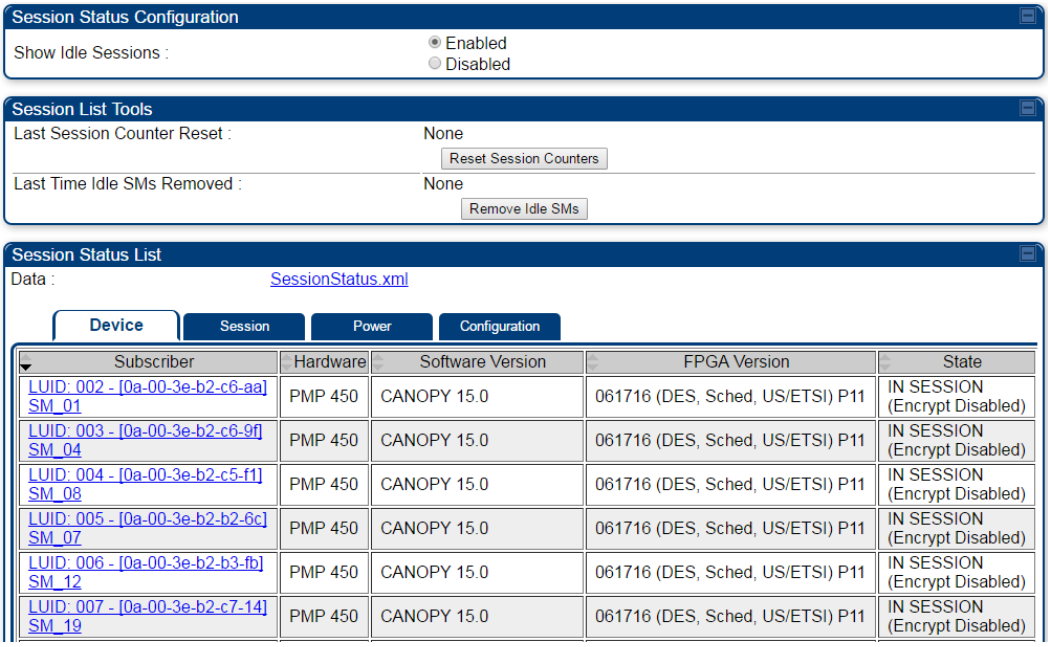
After configuring the link, either an operator in the network office or the SM/BHS INSTALLER user in the field (if read access to the AP/BHM is available to the INSTALLER) must perform the following procedure. Who is authorized and able to do this depends on local operator password policy, management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

To monitor the link for performance, follow these instructions:

Procedure 22 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 152 Session Status page



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

4. The **Device** tab of Session Status List display all displayed SMs – MAC address, PMP/PTP Hardware, Software Version, FPGA Version and State

5 Click **Session Count** tab of Session Status List to display values for **Session Count**, **Reg Count**, and **Re-Reg Count**.

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

See Session tab on page 9-21

6 Click **Power** tab of Session Status list to display Downlink Rate, AP Rx Power (dBm), Signal Strength Radio (dB) for Uplink and Signal to Noise Radio (dB) for Uplink.

See Power tab on page 9-23

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)

See

Configuration tab on page 9-25

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.

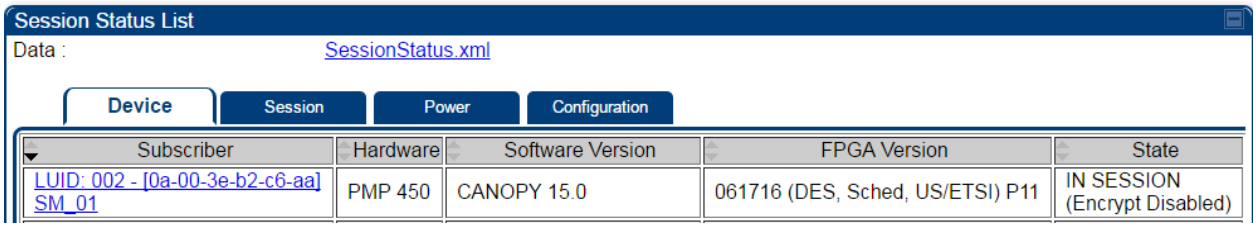
If these values are greater than 1, 1, and 0, or they increase while you are monitoring them, troubleshoot the link. (For example, Use **Receive Power Level** for aiming and then use Link Tests to confirm alignment).

Refer Viewing Session Status on page 9-20 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 153 Exporting Session Status page of PMP 450m AP



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

Export from command line

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

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.

Note

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

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

Token Bucket Algorithm

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

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

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

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

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

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

MIR Data Entry Checking

Uplink and downlink MIR is enforced as shown in Figure 154.

Note

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

Figure 154 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 155.

Figure 155 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 an SM successfully registers and authenticates, CIR information is retrieved from the RADIUS server.

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

Bandwidth from the SM Perspective

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

Interaction of Burst Allocation and Sustained Data Rate Settings

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

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

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

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 7-62. 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 173.

Table 173 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 *uplink* high-priority traffic on amount of high-priority traffic	Dynamic, based on amount of high-priority traffic
	Allocation for *downlink* 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 174 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 175 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 is operating on an Authentication Server release that did not support the feature. This is also the case where the feature enable/disable flag in Authentication Server is set to disabled. The values are those previously set or, if none ever were, then the default values.

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

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

For any SM whose **Authentication Mode** parameter *is not* set to 'Authentication Required', the listed settings are derived as shown in Table 176.

Table 176 MIR, VLAN, HPC, and CIR Configuration Sources, Authentication Disabled

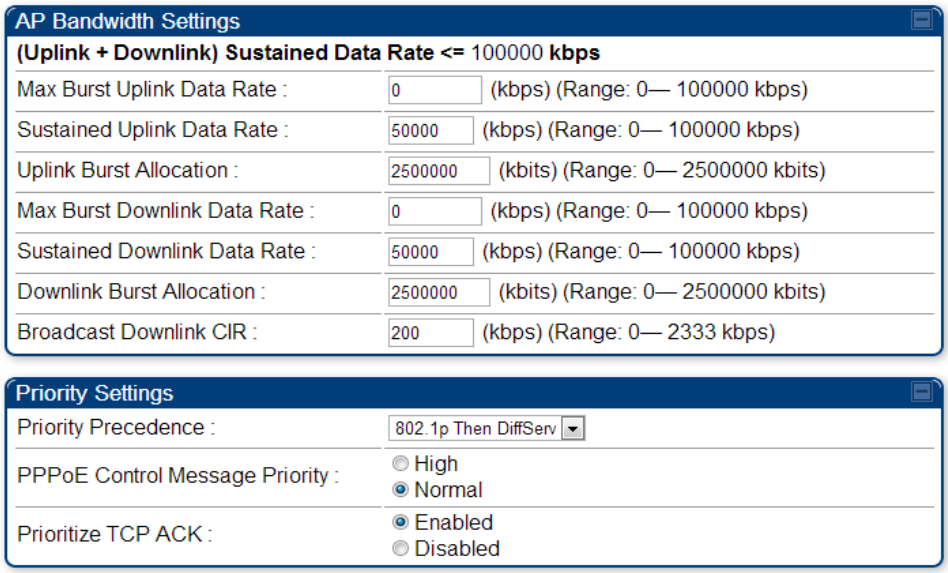
Configuration Source Setting in the AP	Values are obtained from			
	MIR Values	VLAN Values	High Priority Channel State	CIR Values
Authentication Server	AP	AP	AP	AP
SM	SM	SM	SM	SM
Authentication Server+SM	SM	SM	SM	SM

Configuring Quality of Service (QoS)

Quality of Service (QoS) page of AP

The QoS page of AP is explained in Table 177.

Table 177 QoS page attributes - AP



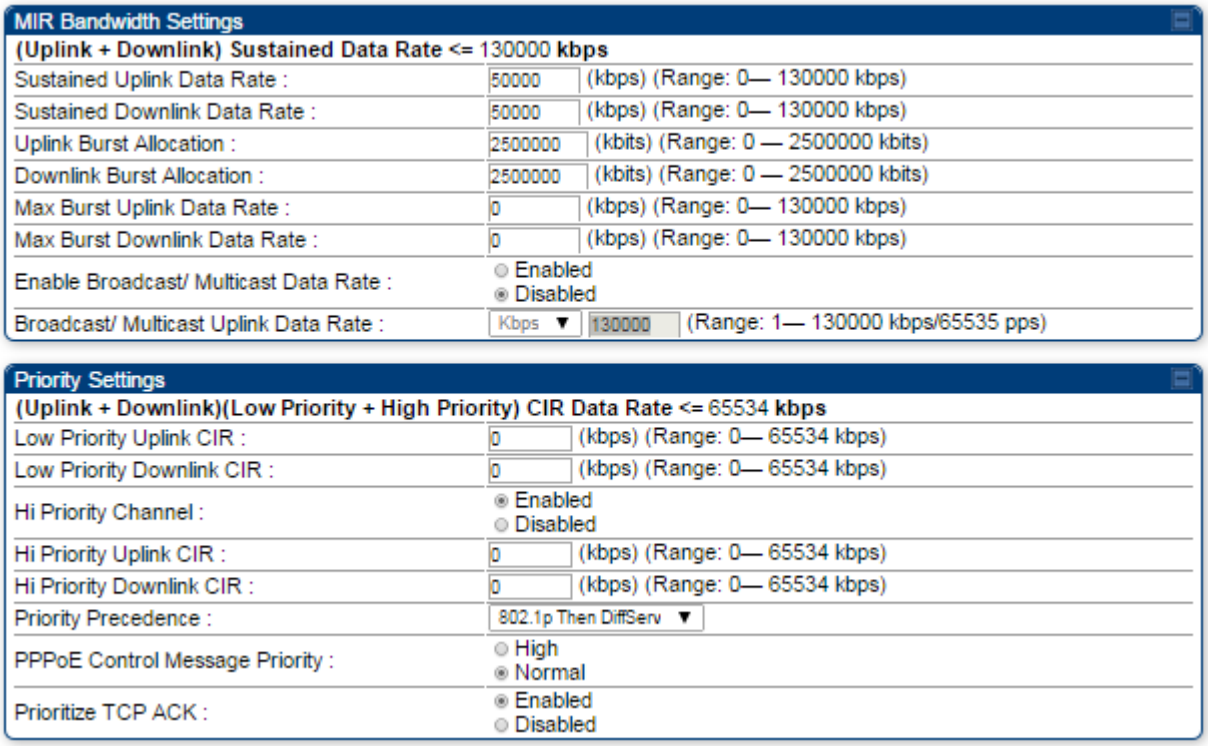
Attribute	Meaning
Max Burst Uplink Data Rate	These parameters allow operators to specify the data rate at which a SM is allowed to transmit (until burst allocation limit is reached) before being recharged at the **Sustained Uplink Data Rate** with credits to transit more. When set to 0 (default), the 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 • Maximum Information Rate (MIR) Parameters on page 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • 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 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • 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	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 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • Configuration Source on page 7-71
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to any registered SM before the AP is replenished with transmission credits at the **Sustained Downlink Data Rate**. See • Maximum Information Rate (MIR) Parameters on page 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • Configuration Source on page 7-71
Broadcast Downlink CIR	Broadcast Downlink CIR (Committed Information Rate, a minimum) supports system designs where downlink broadcast is desired to have higher priority than other traffic. For many other system designs, especially typical internet access networks, leave the Broadcast Downlink CIR at the default. Broadcast Downlink CIR is closely related to the Broadcast Repeat Count parameter, which is settable in the Radio tab of the Configuration page in the AP: when the Broadcast Repeat Count is changed, the total of available bandwidth is also changed, since packets are being sent one, two, or three times, according to the setting in the Broadcast Repeat Count parameter.
Priority Precedence	Allows operator to decide if 802.1p or DiffServ priority bits must be used first when making priority decisions.
PPPoE Control Message Priority	Operators may configure the SM to utilize the high priority channel for PPPoE control messages. Configuring the SM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the SM.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to **Enabled**. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements.

Quality of Service (QoS) page of SM

The QoS page of SM is explained in Table 178.

Table 178 QoS page attributes - SM



Attribute	Meaning
Sustained Uplink Data Rate	Specify the rate that this SM is replenished with credits for transmission. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters on page 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • Configuration Source on page 7-71
Sustained Downlink Data Rate	Specify the rate at which the AP is replenished with credits (tokens) for transmission to this SM. This default imposes no restriction on the uplink. See Maximum Information Rate (MIR) Parameters on Page 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • Configuration Source on page 7-71
Uplink Burst Allocation	Specify the maximum amount of data to allow this SM to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more. See Maximum Information Rate (MIR) Parameters on page 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203

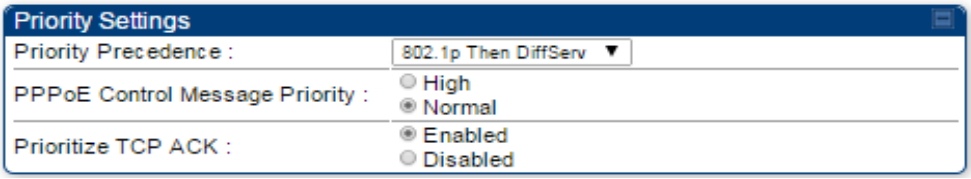
	• Configuration Source on page 7-71
Downlink Burst Allocation	Specify the maximum amount of data to allow the AP to transmit to this SM before the AP is replenished at the **Sustained Downlink Data Rate** with transmission credits. See Maximum Information Rate (MIR) Parameters on page 7-201 • Interaction of Burst Allocation and Sustained Data Rate Settings on page 7-203 • 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	This field indicates the minimum rate at which low priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-202 • Setting the Configuration Source on page 7-206
Low Priority Downlink CIR	This field indicates the minimum rate at which low priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-202 • Setting the Configuration Source on page 7-206
Hi Priority Channel	See • High-priority Bandwidth on page 7-203 • Configuration Source on page 7-71
Hi Priority Uplink CIR	This field indicates the minimum rate at which high priority traffic is sent over the uplink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-202 • Setting the Configuration Source on page 7-206

Hi Priority Downlink CIR	This field indicates the minimum rate at which high priority traffic is sent over the downlink (unless CIR is oversubscribed or RF link quality is degraded). • Committed Information Rate (CIR) on page 7-202 • Setting the Configuration Source on page 7-206
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 179.

Table 179 QoS page attributes - BHM

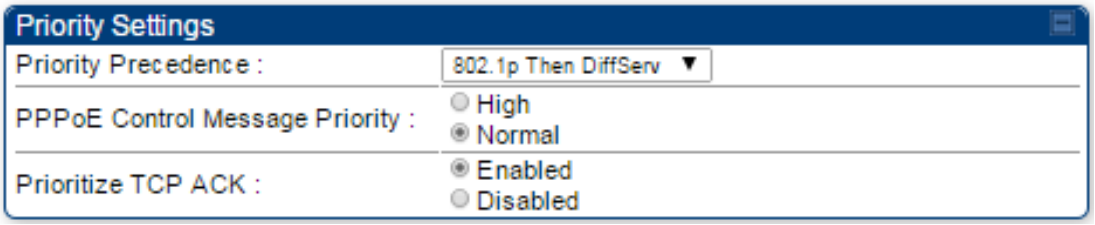


Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHM to utilize the high priority channel for PPPoE control messages. Configuring the BHM in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to **Disabled**.

Quality of Service (QoS) page of BHS

The QoS page of BHS is explained in Table 180.

Table 180 QoS page attributes - BHS

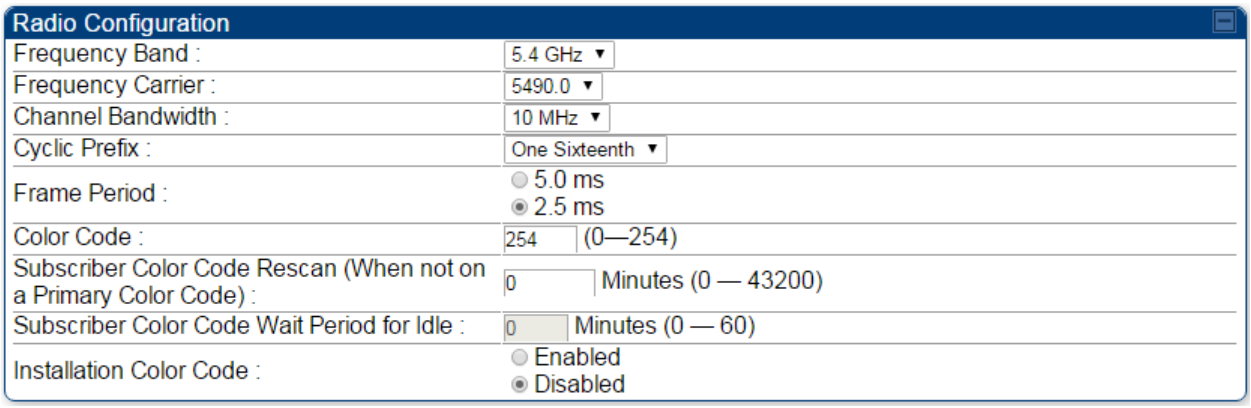


Attribute	Meaning
PPPoE Control Message Priority	Operators may configure the BHS to utilize the high priority channel for PPPoE control messages. Configuring the BHS in this fashion can benefit the continuity of PPPoE connections when there are issues with PPPoE sessions being dropped in the network. This prioritization may be configured in the DiffServ tab in the Configuration menu of the BHS.
Prioritize TCP ACK	To reduce the likelihood of TCP acknowledgement packets being dropped, set this parameter to Enabled. This can improve throughput that the end user perceives during transient periods of congestion on the link that is carrying acknowledgements. This parameter, when enabled, can be particularly useful when running bi-direction FTP sessions over the link. If a link is primarily used for video surveillance, it is recommended to configure this parameter to **Disabled**.

Installation Color Code

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

Figure 156 Installation Color Code of AP



Zero Touch Configuration Using DHCP Option 66

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

- When the SM boots up, if it is set to use DHCP client, it will send out a DHCP Discover packet which includes a request for DHCP Option 66.
- In case of a brand new SM out of the box, the DHCP Discover packet is sent out if the SM connects to an AP using Installation Color Code (ICC), even though DHCP client is not enabled in factory default config.
- An appropriately configured DHCP server will respond with a DHCP Offer and include a URL in response to the Option 66 request. The URL should point to the configuration file.
- The device will download the configuration file and apply it. The device will reboot automatically if needed. (Note: this requires "rebootIfRequired" flag to be added to the config file. See Creating a Golden config file on page 7-216.

Configuration Steps

Procedure 23 Zero Touch Configuration steps

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

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

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

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

User can also create one config file per SM. This provides the most flexibility, but is practical only if you have a software tool/script to generate the config files for each MAC address. The files should be named <mac>.cfg where <mac> is the MAC address of the SM, and stored in the same directory on the file server. The DHCP server should be configured to return the directory name ending with a '/' in option 66. The SM will automatically add "<mac>.cfg" to the path and get its config file.

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

Creating a Golden config file

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

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

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

```
"cfgUtcTimestamp": "cfgUtcTimestamp",
"swVersion": "CANOPY 15.1 SM-AES",
"cfgFileString": "Canopy configuration file",
"srcMacAddress": "0a-00-3e-a2-c2-74",
"deviceType": "5.4/5.7GHz MIMO OFDM - Subscriber Module",
"cfgFileVersion": "1.0"
```

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

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

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

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

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

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

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

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

Hosting the config file

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

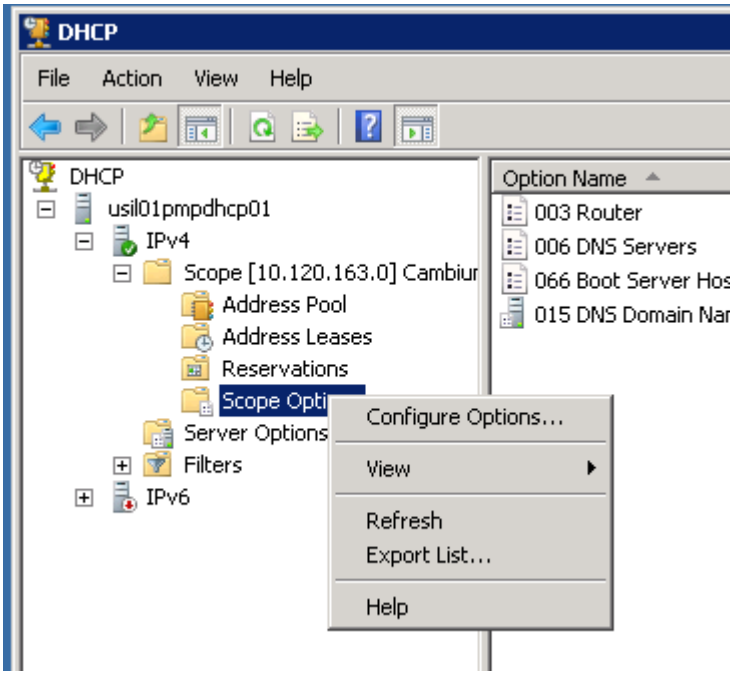
DHCP server configuration

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

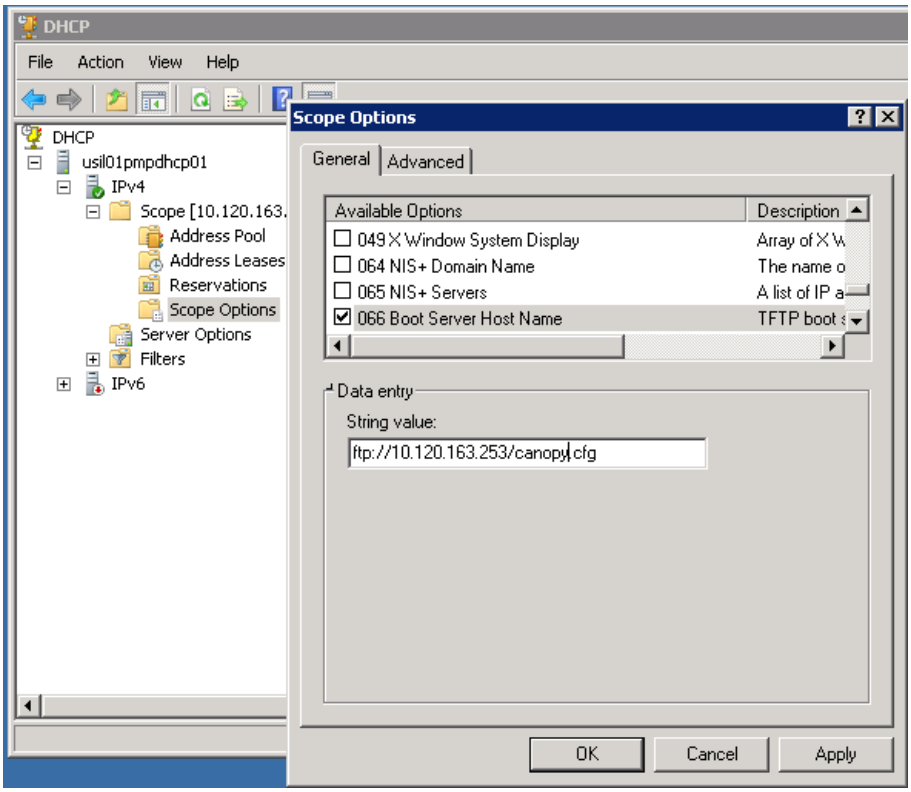
The following example explains how to make the change for Windows Server 2008. Adapt it to your specific DHCP server.

Procedure 24 DHCP server configuration

1. Click “Start > Administrative Tools > DHCP”
2. If you have multiple “Scopes” defined, identify the correct “Scope” that will serve IP addresses for the SMs
3. Right click on “Scope Option” under the correct “Scope” and select “Configure Options”



4 In the “Scope Options” dialog, scroll down to “066 Boot Server Host Name”, select the checkbox and enter the full URL to the golden config file as the “String value”. Then click “OK”.



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

Supported URL Formats

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

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

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

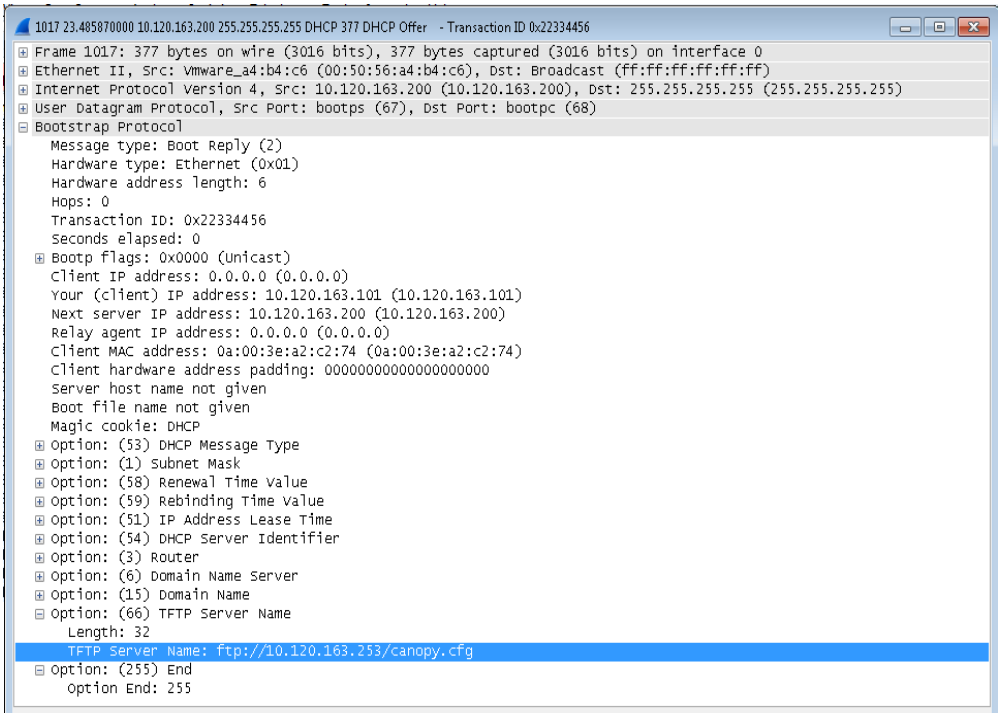
For example:

ftp://10.120.163.253/smconfig/

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

Troubleshooting

1. Ensure that the___14 SM is running 13.3 or newer version of software.
2. If the SM has factory default config, confirm ICC is enabled on the AP, so the SM can connect to it.
3. If the SM is connecting to the AP using a color code other than ICC, make sure the SM has “Network Accessibility” set to “Public” and “DHCP State” set to “Enabled” in the “Configuration > IP” page.
4. Make sure the golden config file does not turn off “Network Accessibility” or “DHCP State”. If it does, the SM will no longer request the config file when it is rebooted.
5. Check the event log of the SM to see the status of the configuration file import including any errors that prevented it from importing the file.
6. Capture the DHCP Offer packet from the DHCP server to the SM and verify that Option 66 has the expected URL.



Configuring Radio via config file

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

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

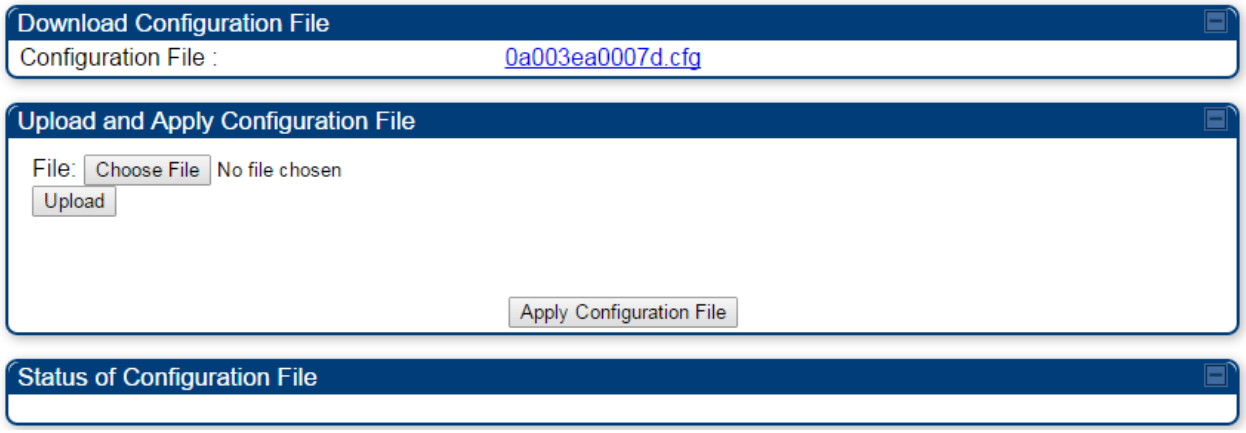
The exported configuration file contains the complete configuration including all the default values. To keep a backup of the current configuration, the file can be saved as-is and imported later.

While importing a configuration file, it can be either imported the full configuration or a sparse configuration containing only the items that need to be changed. If a sparse configuration file is imported, only the items in the file will be imported. Other configuration will remain unchanged. There could also be used a special flag in the configuration file to tell the device to apply the configuration starting from factory default (Refer Special Headers for configuration file on page 7-222).

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 157 Configuration File upload and download page



The DHCP server configuration procedure is as follows:

Procedure 25 DHCP server configuration

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

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

Procedure 26 Import the configuration from the GUI

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

The special headers for config file is explained below:

Procedure 27 Special Headers for configuration file

1. A “configFileParameters” section can be added to the header to control the behavior of the device when importing configuration.
2. The “**setToDefaults**” when set to “true” tell the device to reset to factory default configuration and apply the configuration in the file on top of that. So any attribute not in the configuration file will be set to its factory default value. By default, the configuration in the file is merged with the existing configuration on the device.

   The “**rebootIfRequired**” flag when set to “true” tell the device to reboot automatically if needed to apply the configuration change. By default, the device will not reboot automatically.

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

Configuring cnMaestro™ Connectivity

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

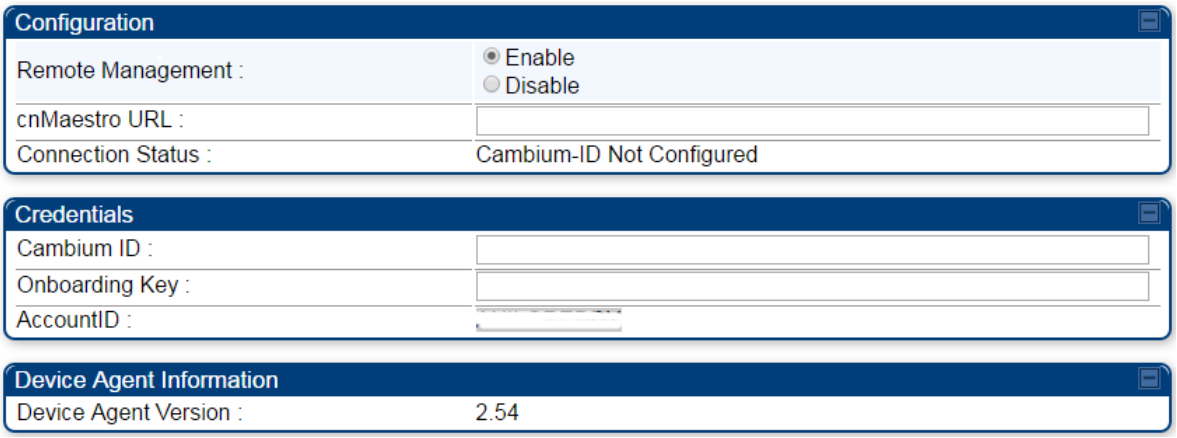
Onboarding

Onboarding can be done in one of several ways:

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

To configure the PMP devices, enable Remote Management under Configuration->cnMaestro as shown in Table 181.

Table 181 Configuring cnMaestro



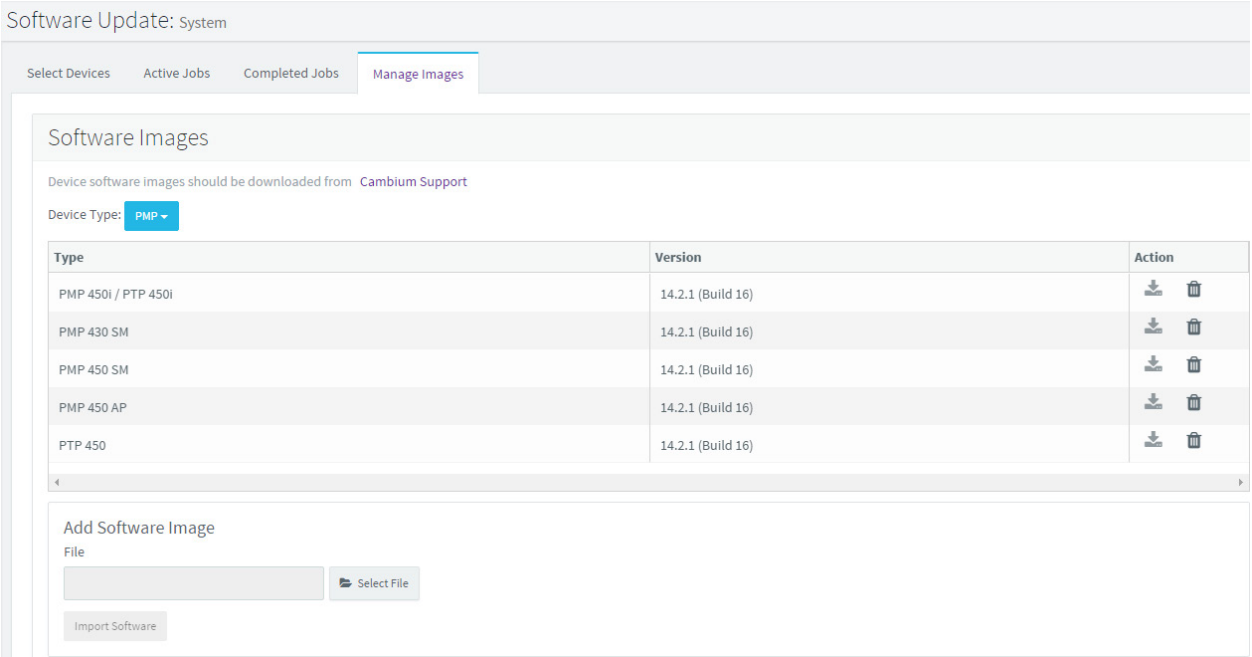
Attribute	Meaning
Remote Management	This field enables/disables remote management of 450 Platform Family products.
cnMaestro URL	This field allows to enter cnMaestro URL e.g. https://cloud.cambiumnetworks.com Or cnMaestro on premises URL
Connection Status	This field indicates cnMaestro connectivity status.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

Device Agent Version	This field shows device agent version.

Prerequisites for onboarding to cnMaestro™

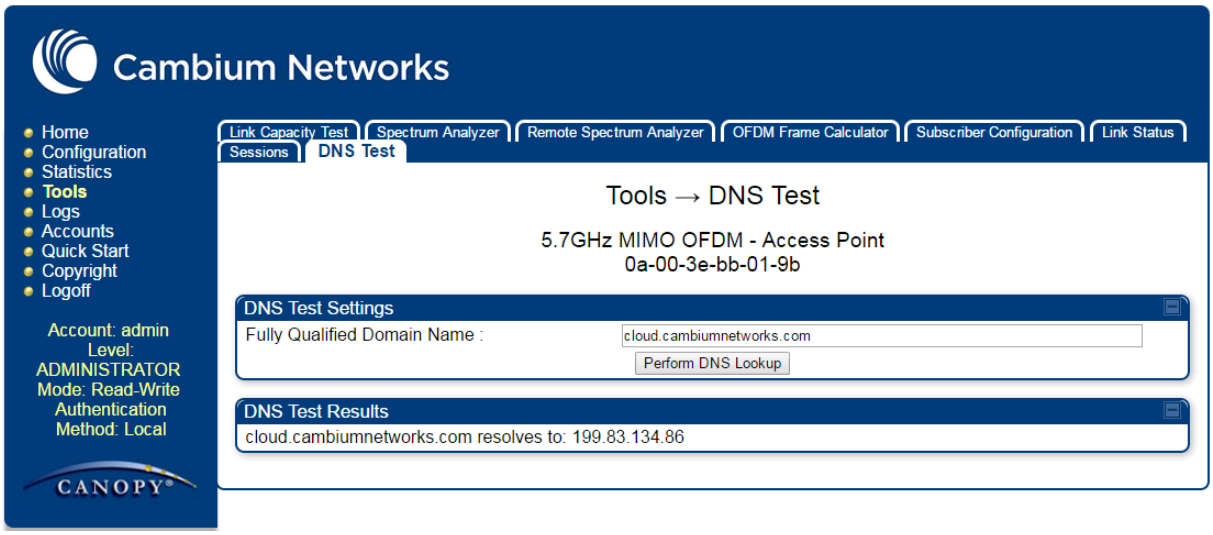
- Devices types must be PMP 450m Series, PMP/PTP 450 Series, PMP/PTP 450i/450b Series or PMP 430 Series SMs (interoperability mode only).
- Minimum required software version of 14.2.1. Device software images can be downloaded from http://support.cambiumnetworks.com or from the On Premises cnMaestro server by navigating to Operate >Software Update->Manage Images. Select
- Device type to display the available images and then click the download icon as shown in Figure 158.

Figure 158 Software Upgrade from cnMaestro™



- IP connectivity between PMP Device and the cnMaestro server is established. Ensure Port 443 is open in the firewall as this port is used for secure communication between the PMP device and the cnMaestro server through web sockets. In addition, if the PMP device and cnMaestro™ server are on different subnets, proper routes should be established for communication.
- For PMP AP, a valid DNS setting is required so that the AP will be able to resolve the cnMaestro URL. DNS settings can be verified by performing a DNS lookup under Tools->DNS Test on the AP as shown in Figure 159.

Figure 159 DNS Test for cnMaestro™ connectivity



- If the SM is in Bridge mode, then LAN1 must have public 7-225equest7-225ility with a public IP assigned and corresponding DNS setting.
- If the SM is in NAT mode, then Remote Management should be enabled with the standalone configuration option and DNS settings.

Knowledge Based articles for onboarding

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

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

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

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

Order of Device Onboarding

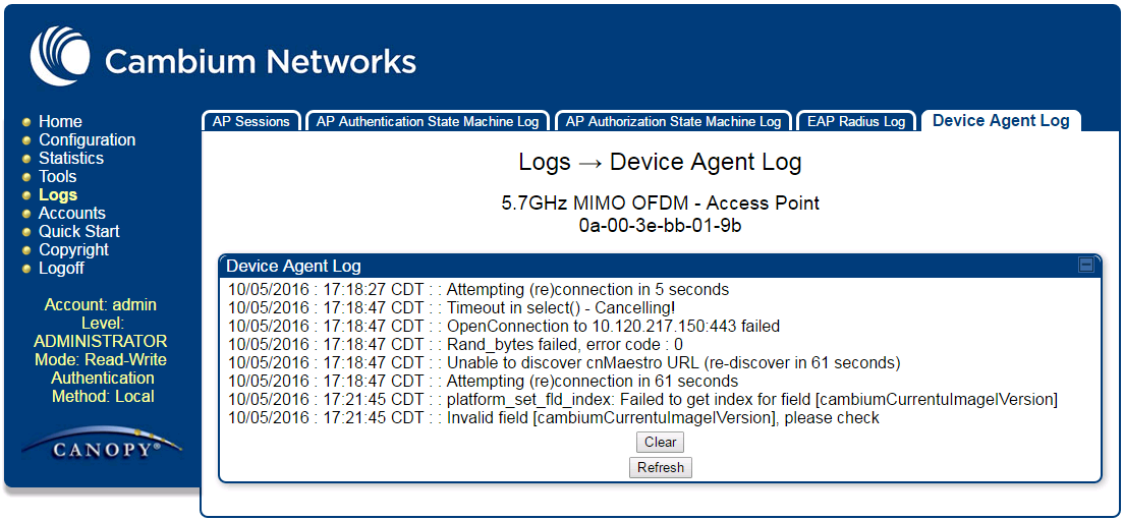
The device discovery order is as follows in On Permises cnMaestro™ Server. If any of the options is not configured, the discovery method will fallback to the next option:

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

Device Agent Logs

For debugging any onboarding issues please check the device agent logs by navigating to Logs->Device Agent Logs on the PMP device GUI as shown in Figure 160. In addition, a tech support dump can for the PMP device can be obtained from cnMaestro™ by navigating to Monitor->Tools menu after selecting the particular PMP device in the tree and clicking the tech support file icon. This can be send to Cambium support for further troubleshooting.

Figure 160 Device Agent Logs

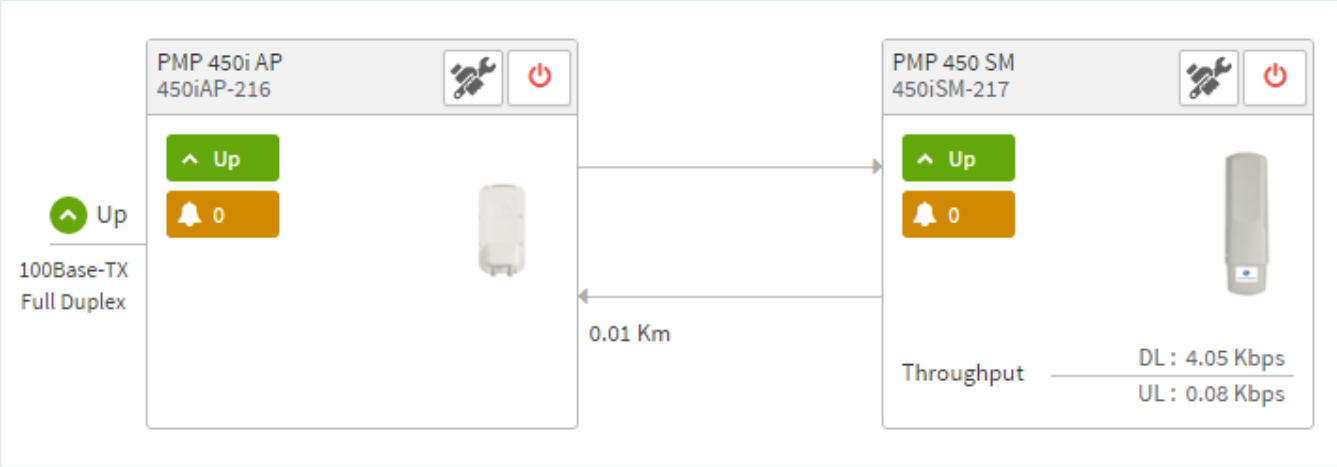


Monitoring Tools for PMP Devices on cnMaestro™

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

- Pictorial view of network hierarchy
- Device status
- Tech support file
- Throughput
- Alarms
- Reboot
- Debug Logs
- Network connectivity – ping and DNS lookup

Figure 161 Example cnMaestro™ screenshot



For more information on these tools please see

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

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

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

The following operations for PMP Devices are available on cnMaestro™

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

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

Configuring a RADIUS server

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

Understanding RADIUS for PMP 450 Platform Family

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

RADIUS Functions

RADIUS protocol support provides the following functions:

- **SM Authentication** allows only known SMs onto the network (blocking "rogue" SMs), and can be configured to ensure SMs are connecting to a known network (preventing SMs from connecting to "rogue" APs). RADIUS authentication is used for SMs, but is not used for APs.
- **SM Configuration:** Configures authenticated SMs with MIR (Maximum Information Rate), CIR (Committed Information Rate), High Priority, and VLAN (Virtual LAN) parameters from the RADIUS server when a SM registers to an AP.
- **User Authentication** allows users to configure a separate User authentication server along with the SM authentication server. If firmware is upgraded while using this functionality and no User authentication servers are configured, then AP continues to use the SM authentication server for User authentication
- **SM Accounting provides** support for RADIUS accounting messages for usage-based billing. This accounting includes indications for subscriber session establishment, subscriber session disconnection, and bandwidth usage per session for each SM that connects to the AP.
- **Centralized AP and SM user name and password management** allows AP and SM usernames and access levels (Administrator, Installer, Technician) to be centrally administered in the RADIUS server instead of on each radio and tracks access events (logon/logoff) for each username on the RADIUS server. This accounting does *not* track and report specific configuration actions performed on radios or pull statistics such as bit counts from the radios. Such functions require an Element Management System (EMS) such as Cambium Networks Wireless Manager. This accounting is *not* the ability to perform accounting functions on the subscriber/end user/customer account.
- **Framed IP** allows operators to use a RADIUS server to assign management IP addressing to SM modules (framed IP address).

Tested RADIUS Servers

The Canopy RADIUS implementation has been tested and is supported on

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

- Cisco ACS, Version 5.7.0.15

Note

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

Choosing Authentication Mode and Configuring for Authentication Servers - AP

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

- **Disabled:** Requires no authentication. Any SM (except a SM that itself has been configured to *require* RADIUS authentication by enabling Enforce Authentication as described below) is allowed to register to the AP.
- **Authentication Server:** Authentication Server in this instance refers to Wireless Manager in BAM-only mode. Authentication is required for a SM to register to the AP. Only SMs listed by MAC address in the Wireless Manager database is allowed to register to the AP.
- **AP Pre-Shared Key:** Canopy offers a pre-shared key authentication option. In this case, an identical key must be entered in the Authentication Key field on the AP’s Configuration > Security tab and in the Authentication Key field on each desired SM’s Configuration > Security tab.
- **RADIUS AAA:** To support RADIUS authentication of SMs, on the AP’s Configuration > Security tab select RADIUS AAA. Only properly configured SMs with a valid certificate is allowed to register to the AP.

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

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

Table 182 Security tab attributes

Authentication Server Settings	
Authentication Mode :	Disabled
Authentication Server DNS Usage :	○ Append DNS Domain Name ◉ 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 *Default port number is 1812*
Authentication Key :	(Using All 0xFF's Key)
Select Key :	○ Use Key above ◉ Use Default Key

Airlink Security	
Encryption Setting :	None

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

Session Timeout	
Web, Telnet, FTP Session Timeout :	3600 Seconds

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

Security Mode	
Web Access :	HTTP Only
SNMP :	SNMPv3 Only
Telnet :	◉ Enabled ○ Disabled
FTP :	◉ Enabled ○ Disabled
TFTP :	◉ Enabled ○ Disabled

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

Selection Key	This option allows operators to choose which authentication key is used: **Use Key above** means that the key specified in **Authentication Key** is used for authentication **Use Default Key** means that a default key (based off of the SM's MAC address) is used for authentication
Encryption Key	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. **None** provides no encryption on the air link. **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.
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 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: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>. • **HTTPS Only** – provides a secured web access. The radio to be accessed via https1://<IP of Radio>.

	• **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.

SM Authentication Mode – Require RADIUS or Follow AP

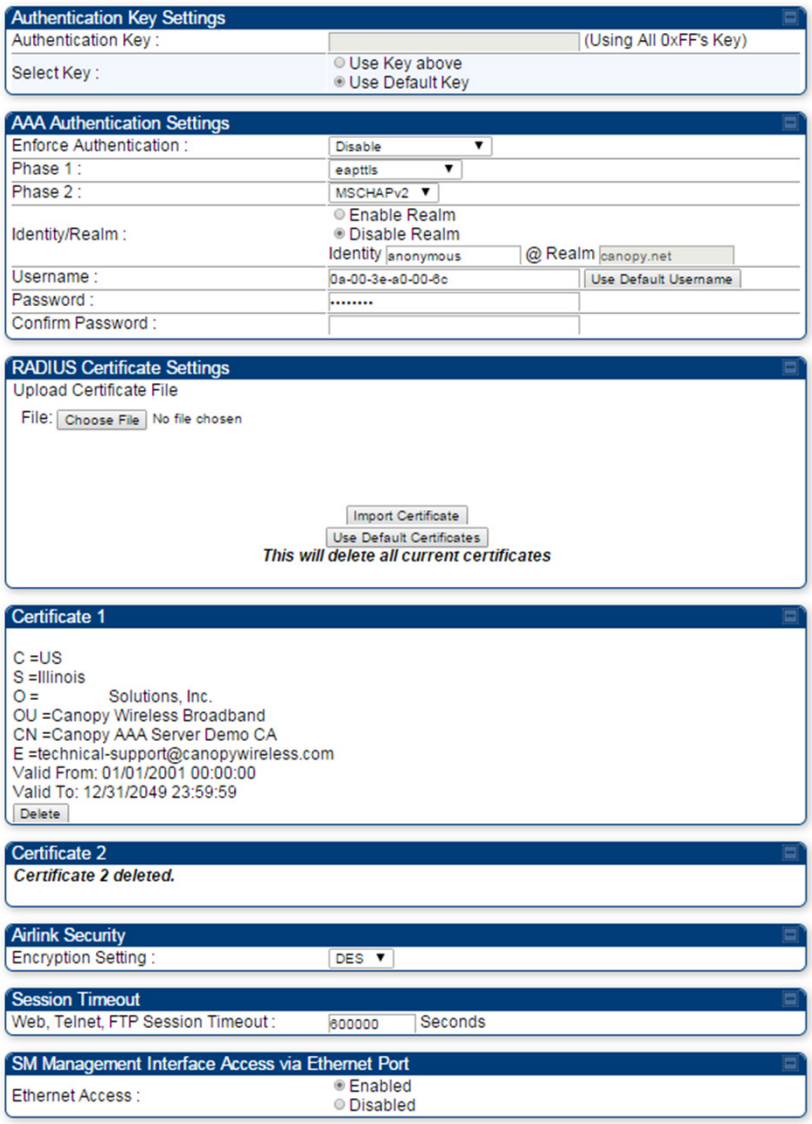
If it is desired that a SM will only authenticate to an AP that is using RADIUS, on the SM's Configuration Security tab set **Enforce Authentication** to **AAA**. With this enabled, SM does not register to an AP that has any **Authentication Mode** other than **RADIUS AAA** selected.

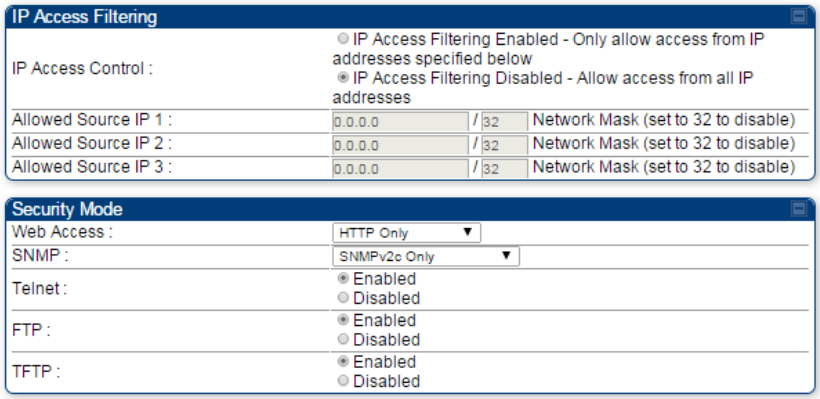
If it is desired that a SM use the authentication method configured on the AP it is registering to, set **Enforce Authentication** to **Disabled.** With **Enforce Authentication** disabled, a SM will attempt to register using whichever **Authentication Mode** is configured on the AP it is attempting 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 183 SM Security tab attributes





Attribute	Meaning
Authentication Key	The authentication key is a 32-character hexadecimal string used when **Authentication Mode** is set to **AP PreShared Key**. By default, this key is set to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.
Select Key	This option allows operators to choose which authentication key is used: **Use Key above** means that the key specified in **Authentication Key** is used for authentication **Use Default Key** means that a default key (based off of the SM's MAC address) is used for authentication
Enforce Authentication	The SM may enforce authentication types of **AAA** and **AP Pre-sharedKey**. The SM will not finish the registration process if the AP is not using the configured authentication method (and the SM locks out the AP for 15 minutes). Enforce Authentication default setting is **Disable.**
Phase 1	The protocols supported for the **Phase 1** (Outside Identity) phase of authentication are EAPTTLS (Extensible Authentication Protocol Tunneled Transport Layer Security) or MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).
Phase 2	Select the desired **Phase 2** (Inside Identity) authentication protocol from the **Phase 2** options of **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MSCHAP** (Microsoft's version of CHAP, version 2 is used). The protocol must be consistent with the authentication protocol configured on the RADIUS server.

Identity/Realm	If Realms are being used, select **Enable Realm** and configure an outer identity in the **Identity** field and a Realm in the **Realm** field. These must match the Phase 1/Outer Identity and Realm configured in the RADIUS server. The default **Identity** is "anonymous". The **Identity** can be up to 128 non-special (no diacritical markings) alphanumeric characters. The default **Realm** is "canopy.net". The **Realm** can also be up to 128 non-special alphanumeric characters. Configure an outer Identity in the **Username** field. This must match the Phase 1/Outer Identity username configured in the RADIUS server. The default Phase 1/Outer Identity **Username** is "anonymous". The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Username	Enter a **Username** for the SM. This must match the username configured for the SM on the RADIUS server. The default **Username** is the SM's MAC address. The **Username** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Password Confirm Password	Enter the desired password for the SM in the **Password** and **Confirm Password** fields. The **Password** must match the password configured for the SM on the RADIUS server. The default **Password** is "password". The **Password** can be up to 128 non-special (no diacritical markings) alphanumeric characters.
Upload Certificate File	To upload a certificate manually to a SM, first load it in a known place on your PC or network drive, then click on a **Delete** button on one of the Certificate description blocks to delete a certificate to provide space for your certificate. Click on **Choose File,** browse to the location of the certificate, and click the **Import Certificate** button, and then reboot the radio to use the new certificate. When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used. The public certificates installed on the SMs are used with the private certificate on the RADIUS server to provide a public/private key encryption system. Up to 2 certificates can be resident on a SM. An installed certificate can be deleted by clicking the **Delete** button in the certificate's description block on the Configuration > Security tab. To restore the 2 default certificates, click the **Use Default Certificates** button in the **RADIUS Certificate Settings** parameter block and reboot the radio.

Encryption Setting	Specify the type of airlink security to apply to this AP. The encryption setting must match the encryption setting of the SMs. **None** provides no encryption on the air link. **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 AP.
Ethernet Access	If you want to prevent any device that is connected to the Ethernet port of the SM from accessing the management interface of the SM, select **Ethernet Access Disabled**. This selection disables access through this port to via HTTP (the GUI), SNMP, telnet, FTP, and TFTP. With this selection, management access is available through only the RF interface via either an IP address (if **Network Accessibility** is set to **Public** on the SM) or the Session Status or Remote Subscribers tab of the AP. See **IP Access Control** below. If you want to allow management access through the Ethernet port, select **Ethernet Access Enabled**. This is the factory default setting for this parameter.
IP Access Control	You can permit access to the AP from any IP address (**IP Access Filtering Disabled**) or limit it to access from only one, two, or three IP addresses that you specify (**IP Access Filtering Enabled**). If you select **IP Access Filtering Enabled**, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted from any IP address
Allowed Source IP 1 Allowed Source IP 2 Allowed Source IP 3	If you selected **IP Access Filtering Enabled** for the **IP Access Control** parameter, then you must populate at least one of the three **Allowed Source IP** parameters or have no access permitted to the AP from any IP address. You may populate as many as all three. If you selected **IP Access Filtering Disabled** for the **IP Access Control** parameter, then no entries in this parameter are read, and access from all IP addresses is permitted.
Web Access	The Radio supports secured and non-secured web access protocols. Select suitable web access from drop down list: • **HTTP Only** – provides non-secured web access. The radio to be accessed via http://<IP of Radio>.

	• **HTTPS Only** – provides a secured web access. The radio to be accessed via https://<IP of Radio>. • **HTTP and HTTPS** – If enabled, the radio can be accessed via both http and https.
SNMP	This option allows to configure SNMP agent communication version. It can be selected from drop down list : • **SNMPv2c Only** – Enables SNMP v2 community protocol. • **SNMPv3 Only** – Enables SNMP v3 protocol. It is secured communication protocol. • **SNMPv2c and SNMPv3** – It enables both the protocols.
Telnet	This option allows to **Enable** and **Disable** Telnet access to the Radio.
FTP	This option allows to **Enable** and **Disable** FTP access to the Radio.
TFTP	This option allows to **Enable** and **Disable** TFTP access to the Radio.

SM - Phase 1 (Outside Identity) parameters and settings

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

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

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

SM - Phase 2 (Inside Identity) parameters and settings

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

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

Handling Certificates

Managing SM Certificates via the SM GUI

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

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

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

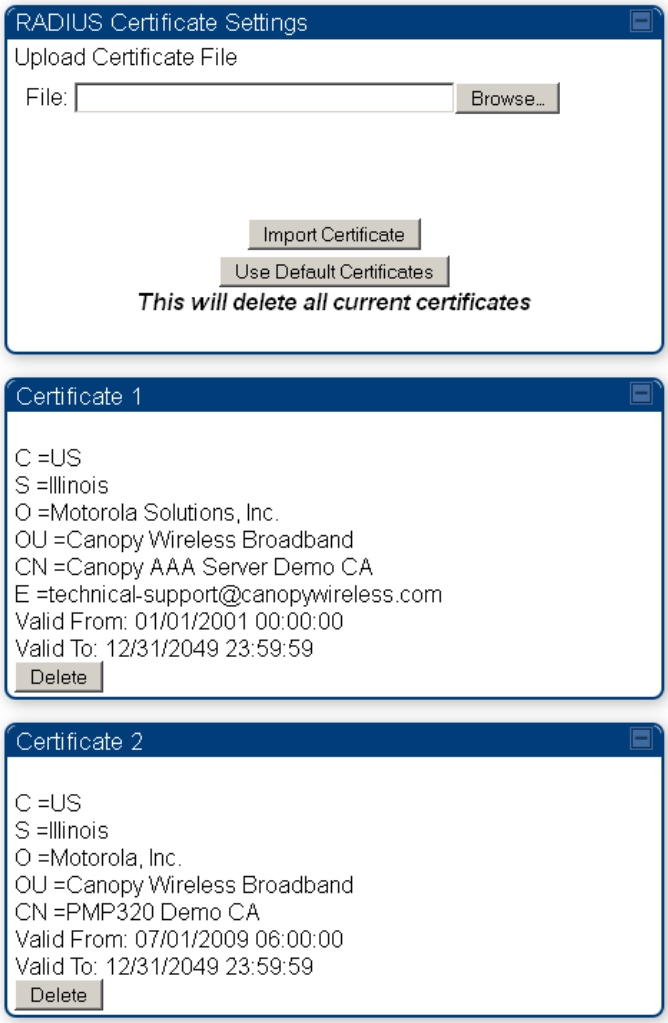
When a certificate is in use, after the SM successfully registers to an AP, an indication of **In Use** will appear in the description block of the certificate being used.

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

Note

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

Figure 162 SM Certificate Management



Configuring RADIUS servers for SM authentication

Your RADIUS server must be configured to use the following:

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

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

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

Note

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

Assigning SM management IP addressing via RADIUS

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

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

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

Configuring RADIUS server for SM configuration

Canopy Vendor Specific Attributes (VSAs) along with VSA numbers and other details are listed in Table 184. 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 184).

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 184). 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 184 RADIUS Vendor Specific Attributes (VSAs)

Name	Number	Type	Required	Value	
MS-MPPE-Send-Key*	26.311.16	-	Y	-	
-				-	-
MS-MPPE-Recv-Key*	26.311.17	-	Y	-	
-				-	-
Cambium-Canopy-LPULCIR	26.161.1	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Uplink CIR				0 kbps	32 bits
Cambium-Canopy-LPDLCIR	26.161.2	integer	N	0-65535 kbps	
Configuration > Quality of Service > Low Priority Downlink CIR				0 kbps	32 bits
Cambium-Canopy-HPULCIR	26.161.3	integer	N	0-65535 kbps	
Configuration > Quality of Service > 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	
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	0-2500000 kbps	
Configuration > Quality of Service > Uplink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-DLBR	26.161.8	integer	N	0-100000 kbps	
Configuration > Quality of Service > Sustained Downlink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-DLBL	26.161.9	integer	N	0-2500000 kbps	
Configuration > Quality of Service > Downlink Burst Allocation				dependent on radio feature set	32 bits
Cambium-Canopy-VLLEARNEN	26.161.14	integer	N	0-disable, 1-enable	
Configuration > VLAN > Dynamic Learning				1	32 bits
Cambium-Canopy-VLFRAMES	26.161.15	integer	N	0-all, 1-tagged, 2-untagged	
Configuration > VLAN > Allow Frame Types				0	32 bits
Cambium-Canopy-VLIDSET	26.161.16	integer	N	VLAN Membership (1-4094)	
Configuration > VLAN Membership				0	32 bits
Cambium-Canopy-VLAGETO	26.161.20	integer	N	5 - 1440 minutes	
Configuration > VLAN > VLAN Aging Timeout				25 mins	32 bits
Cambium-Canopy-VLIGVID	26.161.21	integer	N	1 – 4094	
Configuration > VLAN > Default Port VID				1	32 bits
Cambium-Canopy-VLMGVID	26.161.22	integer	N	1 – 4094	
Configuration > VLAN > Management VID				1	32 bits
Cambium-Canopy-VLSMMGPASS	26.161.23	integer	N	0-disable, 1-enable	
Configuration > VLAN > SM Management VID Pass-through				1	32 bits
Cambium-Canopy-BCASTMIR	26.161.24	integer	N	0-100000 kbps, 0=disabled	
Configuration > Quality of Service > Broadcast/Multicast Uplink Data Rate				dependent on radio feature set	32 bits
Cambium-Canopy-Gateway	26.161.25	ipaddr	N	-	
Configuration > IP > Gateway IP Address				0.0.0.0	-

Cambium-Canopy-ULMB	26.161.26	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Uplink Data Rate				0	32 bits
Cambium-Canopy-DLMB	26.161.27	integer	N	0-100000 kbps	
Configuration > Quality of Service > Max Burst Downlink Data Rate				0	32 bits
Cambium-Canopy-UserLevel	26.161.50	integer	N	1-Technician, 2-Installer, 3-Administrator	
Account > Add User > Level				0	32 bits
Cambium-Canopy-DHCP-State	26.161.31	integer	N	1-Enable	
Configuration > IP > DHCP state				1	32 bits
Cambium-Canopy-BCASTMIRUNITS	26.161.28	integer	N		
Configuration > QoS > Broadcast Downlink CIR				0	32 bits
Cambium-Canopy-ConfigFileImportUrl	26.161.29	string	N		
Configuration > Unit Settings				0	32 bits
Cambium-Canopy-ConfigFileExportUrl	26.161.30	string	N		
Configuration > Unit Settings				0	32 bits
Cambium-Canopy-UserMode	26.161.51	integer	N	1=Read-Only 0=Read-Write	
Account > Add User > User Mode				0	32 bits

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

Note

VSA numbering:

26 connotes Vendor Specific Attribute, per RFC 2865

26.311 is Microsoft Vendor Code, per IANA

Configuring RADIUS server for SM configuration using Zero Touch feature

The RADIUS VSA (Vendor Specific Attributes) is updated for Zero Touch feature. This feature enables the ability for a SM to get its configuration via RADIUS VSA. The RADIUS VSA is updated for an URL which points to the configuration file of SM (see Table 184 for list of VSA).

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

The RADIUS VSA attributes concerning Zero Touch are as follows:

```
VSA                                     Type       String

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

The updated RADIUS dictionary can be downloaded from below link:

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

Note

The feature is not applicable to the AP.

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

AP – Technician/Installer/Administrator Authentication

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

Procedure 28 Centralized user name and password management for AP

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

○ User administration and authentication separation

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

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

To configure separate User Authentication and SM Authentication:

Procedure 29 User administration and authentication separation

1. Go to the AP's **Account** > **User Authentication And Access Tracking** tab
2. Set **User Authentication Mode** to **Remote** or **Remote then Local**.
3. Set **User Authentication Method** to **EAP-MD5** or **EAP-PEAP-MSCHAPv2**
4. Configure the Shared Secrets and IP Addresses of:

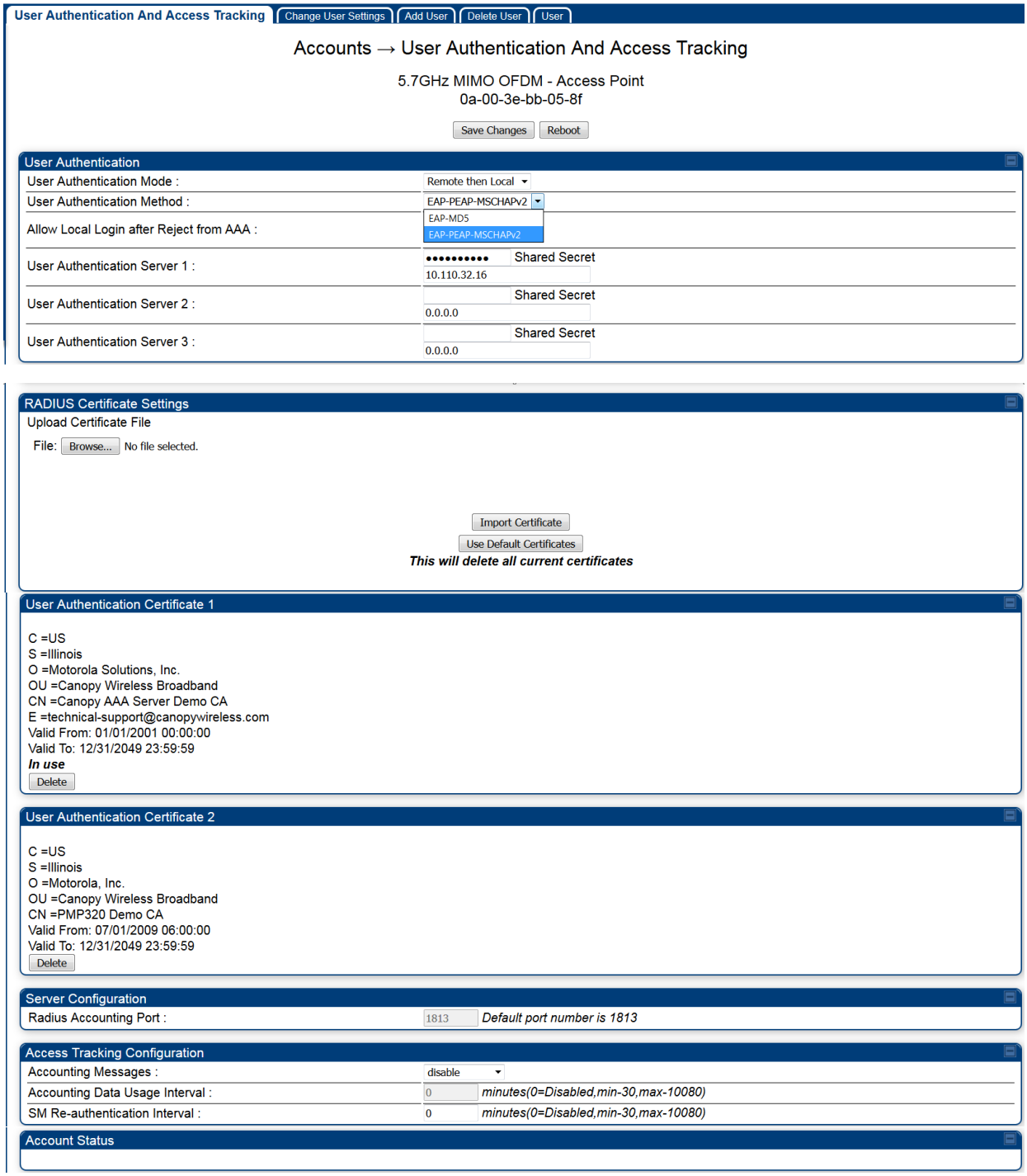
   User Authentication Server 1

   User Authentication Server 2

   User Authentication Server 3

   Note: If none of the above User Authentication servers are configured, only SM authentication will be performed.
5. Under **RADIUS Certificate Settings**, click **Browse** to upload the RADIUS Certificate files.

Table 185 AP User Authentication and Access Tracking attributes



Attribute	Meaning
User Authentication Mode	• **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed. • **Remote**: Authentication by the centralized RADIUS server is required to gain access to the AP. For up to 2 minutes a test pattern is displayed until the server responds or times out.

	• **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the AP.
User Authentication Method	The user authentication method employed by the radios: • EAP-MD5 • EAP-PEAP-MSCHAPv2
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user is allowed to login locally to the radio's management interface.
User Authentication Server 1	The IP address and the shared secret key of the User authentication RADIUS server 1.
User Authentication Server 2	The IP address and the shared secret key of the User Authentication Server 2 configured in RADIUS Server.
User Authentication Server 3	The IP address and the shared secret key of the User Authentication Server 3 configured in RADIUS Server.
RADIUS Certificate Settings	Import Cetificate – browse and select the file to be uploaded and click on "Import Certificate" to import a new certificate. Use Default Certificates – use the preloaded default certificates.
User Authentication Certificate 1	Cerificate provided by default for User authentication.
User Authentication Certificate 2	Cerificate provided by default for User authentication.
Radius Accounting Port	The destination port on the AAA server used for Radius accounting communication.
Accounting Messages	disable – no accounting messages are sent to the RADIUS server. deviceAccess – accounting messages regarding device access are sent to the RADIUS server (see Table 187). dataUsage – accounting messages regarding data usage are sent to the RADIUS server (see Table 187). All – accounting messages regarding device access and data usage are sent to the RADIUS server.
Accounting Data Usage Interval	The interval for which accounting data messages are sent from the radio to the RADIUS server. If 0 is configured for this parameter, no data usage messages are sent.
SM Re-authentication Interval	The interval for which the SM will re-authenticate to the RADIUS server.
Account Status	Displays the account status.

SM – Technician/Installer/Administrator Authentication

The centralized user name and password management for SM is same as AP. Follow AP – Technician/Installer/Administrator Authentication on page 7-248 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 163 User Authentication and Access Tracking tab of the SM

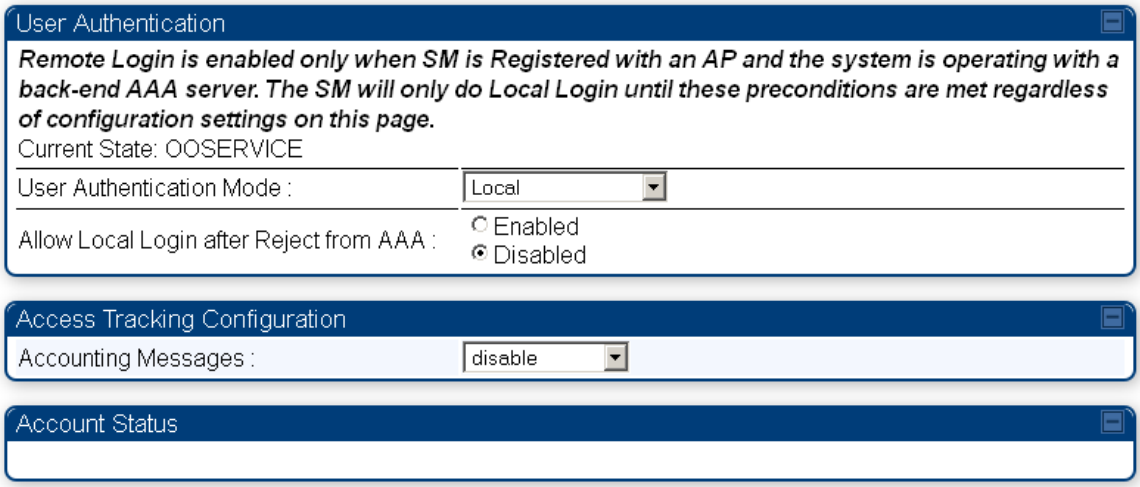
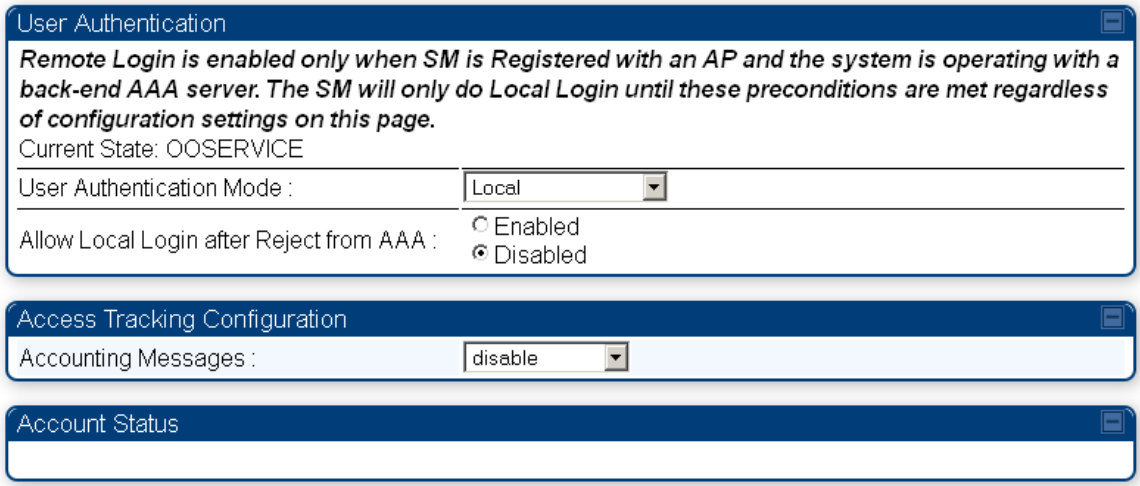


Table 186 SM User Authentication and Access Tracking attributes



Attribute	Meaning
User Authentication Mode	• **Local**: The local SM is checked for accounts. No centralized RADIUS accounting (access control) is performed.

	• **Remote**: Authentication by the centralized RADIUS server is required to gain access to the SM if the SM is registered to an AP that has **RADIUS AAA Authentication Mode** selected. For up to 2 minutes a test pattern is displayed until the server responds or times out. • **Remote then Local**: Authentication using the centralized RADIUS server is attempted. If the server sends a reject message, then the setting of **Allow Local Login after Reject from AAA** determines if the local user database is checked or not. If the configured servers do not respond within 2 minutes, then the local user database is used. The successful login method is displayed in the navigation column of the SM.
Allow Local Login after Reject from AAA	If a user authentication is rejected from the AAA server, the user is allowed to login locally to the radio's management interface. It is applicable ONLY when the **User Authentication Mode** is set to "**Remote then Local**". **Note** When the radio User Authentication Mode is set to "Local" or "Remote", the Allow Local Login after Reject from AAA does not any effect.
Accounting Messages	• disable – no accounting messages are sent to the RADIUS server • deviceAccess – accounting messages are sent to the RADIUS server regarding device access (see Table 187).

Access Tracking

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

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

RADIUS Device Data Accounting

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

Table 187 Device data accounting RADIUS attributes

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

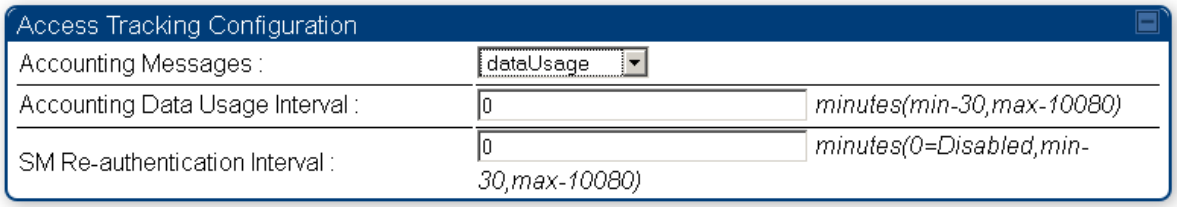
Sender	Message	Attribute	Value	Description
	Accounting-Request	Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	This message is sent every time a SM registers with an AP, and after the SM stats are cleared.
		Event-Timestamp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

Sender	Message	Attribute	Value	Description
		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. Interim update counts are cumulative over the course of the session
		Acct-Session-Id	Unique per AP session. Initial value is SM MAC, and increments after every start message sent of an in session SM.	
		Acct-Input-Octets	Sum of the input octets sent to the SM over regular data VC and the high priority data VC (if enabled). Will not include broadcast.	
		Acct-Output-Octets	Sum of the output octets set from the SM over regular data VC and the high priority data VC (if enabled).	
		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.	

Sender	Message	Attribute	Value	Description
		Acct-Input-Packets	Sum of unicast and multicast packets that are sent to a particular SM over the regular data VC and the high priority data VC (if enabled). It will not include broadcast.	
		Acct-Output-Packets	Sum of unicast and multicast packets that are sent from a particular SM over the 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 164 RADIUS accounting messages configuration



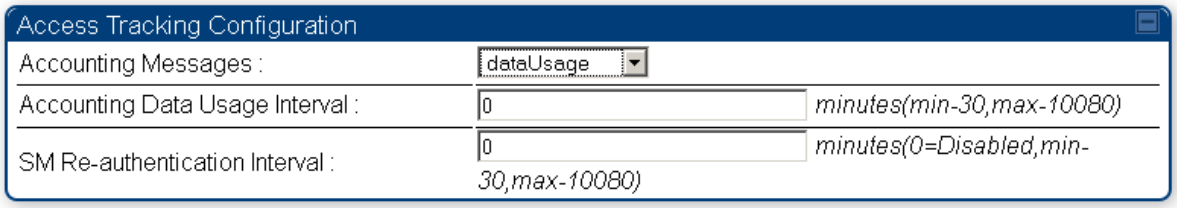
The data accounting message data is based on the SM statistics that the AP maintains, and these statistics may be cleared on the AP by an operator. If an operator clears these messages and data accounting is enabled, an accounting stop message is sent followed by an accounting start message to notify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

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

RADIUS Device Re-authentication

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

Figure 165 Device re-authentication configuration



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

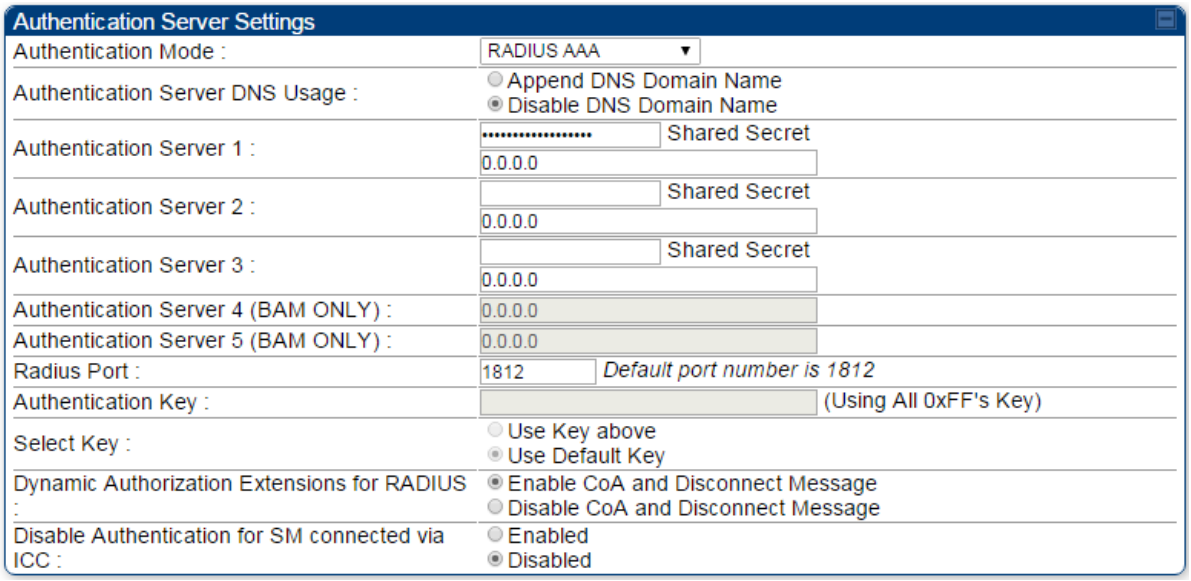
- **Success**: The SM continues normal operation
- **Reject**: The SM de-registers and will attempt network entry again after 1 minute and then if rejected will attempt re-entry every 15 minutes
- **Timeout or other error**: The SM remains in session and attempt 5 times to re-authenticate with the RADIUS-REQUEST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

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

RADIUS Change of Authorization and Disconnect Message

Prior to this feature, SM will get configuration parameters from a RADIUS server during authentication process. This feature allows an administrator to control configuration parameters in the SM while SM is in session. The configuration changes in SM are done using RADIUS Change of Authorization method (RFC 3576) on the existing RADIUS authentication framework for AP and SM. A typical use case could be changing the QOS parameters after a certain amount of bandwidth usage by a SM.

Figure 166 RADIUS CoA configuration for AP



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

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

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

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

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

Note

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

Microsoft RADIUS support

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

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

Note

All this configuration has been tested on Windows Server 2012 R2 version.

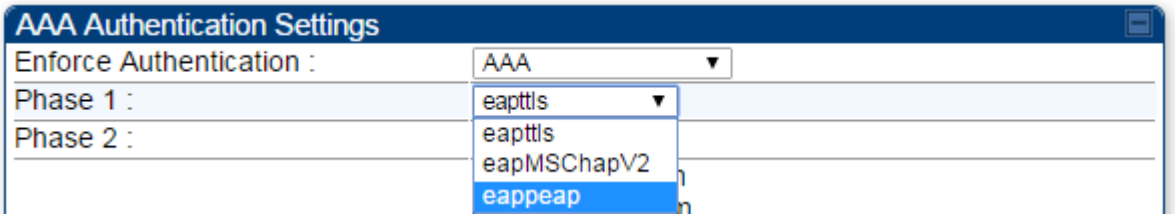
This feature is not supported on hardware board type P9 or lower platforms.

SM Authentication Configuration

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

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

Figure 167 EAPPEAP settings



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

Windows Server Configuration

Import Certificate

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

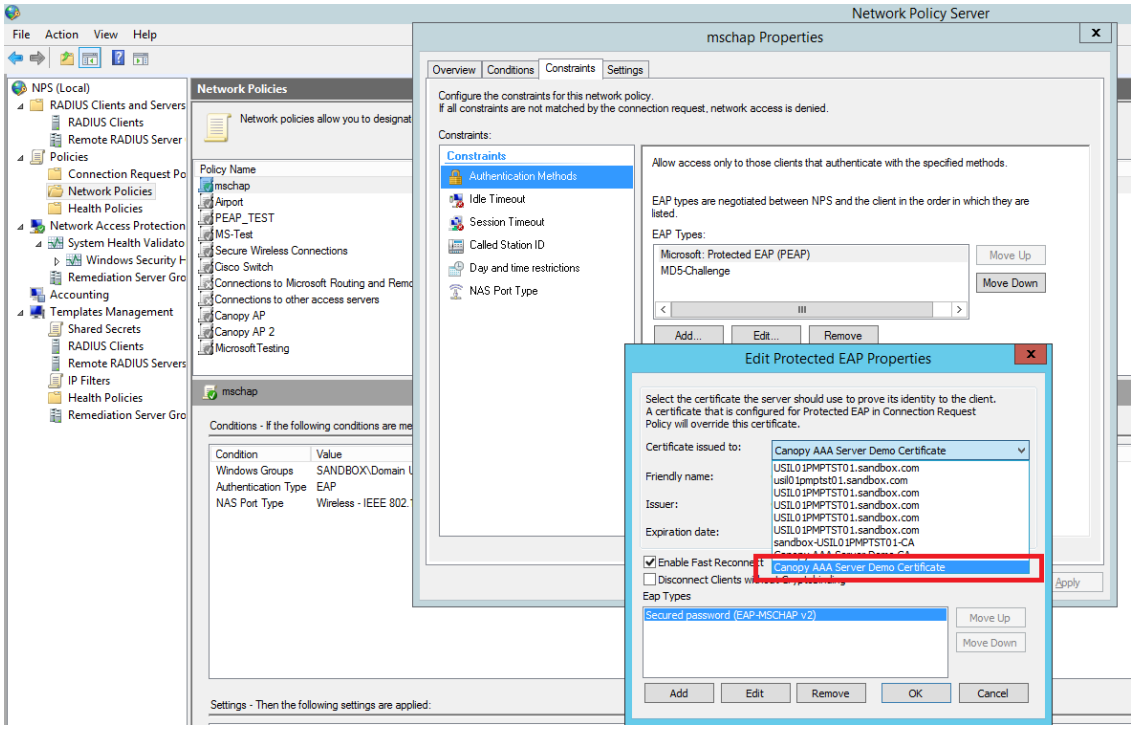
1. Copy the certificate which is configured in SM under **Configuration > Security -> Certificate1** to Windows Server machine.
2. Right click and select 'Install Certificate'. This will install the certificate and it's ready for use. This certificate will be used while configuring PEAP-MSCHAPv2 in NPS.

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

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

- RADIUS Client
  - https://technet.microsoft.com/en-us/library/cc732929
- Connection Request Policies
  - https://technet.microsoft.com/en-us/library/cc730866
  - Choose 'Wireless-Other' in NAS-Port-Type
- Network Policy
  - https://technet.microsoft.com/en-us/library/cc755309
  - Choose 'Wireless-Other' in NAS-Port-Type.
  - While configuring PEAP, select the above imported certificate.

Figure 168 Importing certificate in NPS



User Authentication Configuration

Enabling EAP-MD5

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

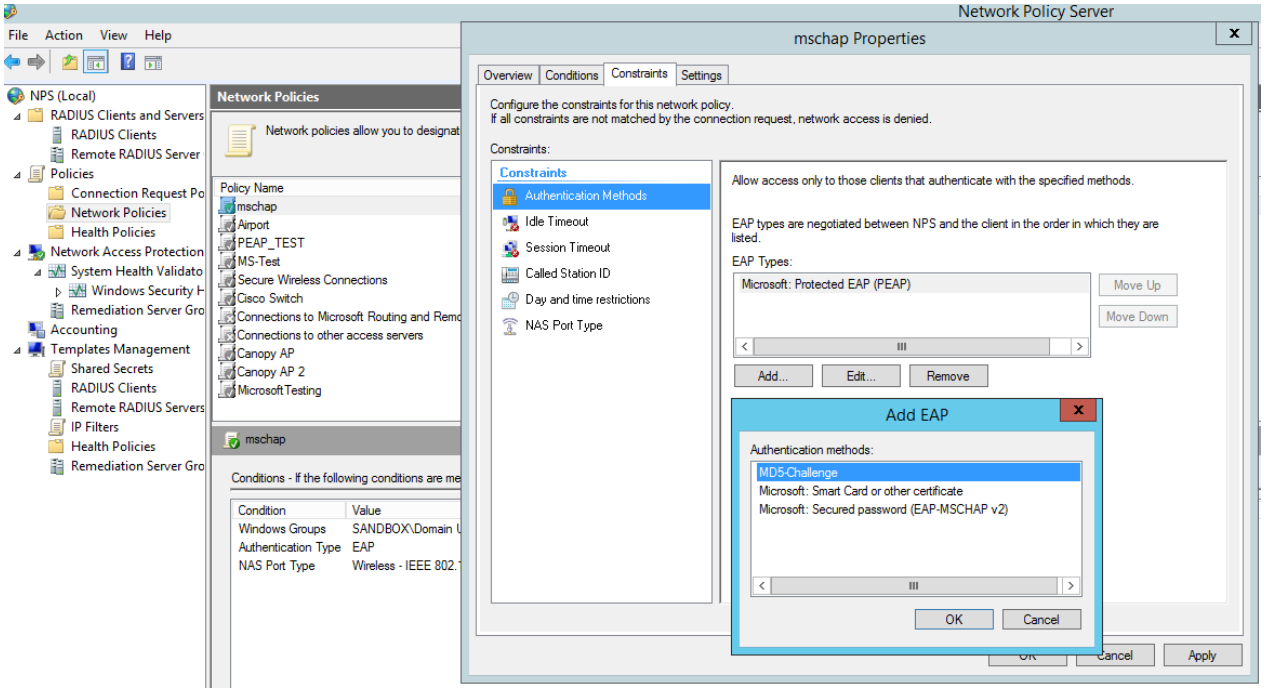
1. Follow the instructions:

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

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

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

Figure 169 Selecting MD5 from NPS console

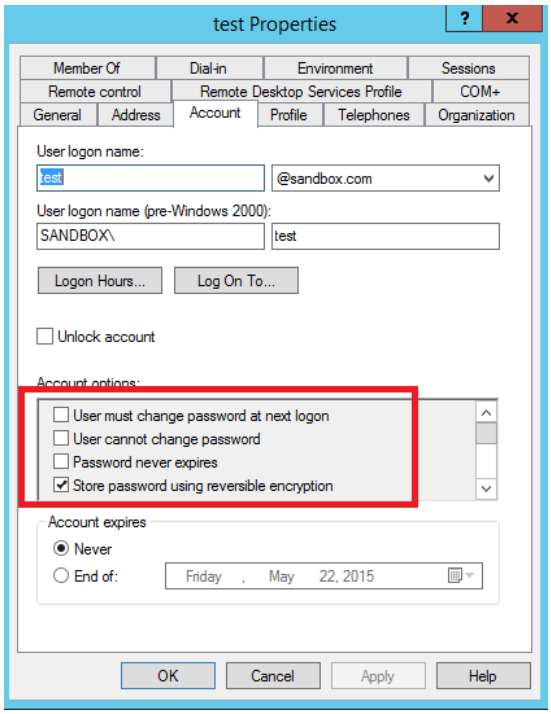


User Configuration in Active Directory

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

Make sure user property is configured as shown below.

Figure 170 User configuration



○ RADIUS VSA Configuration

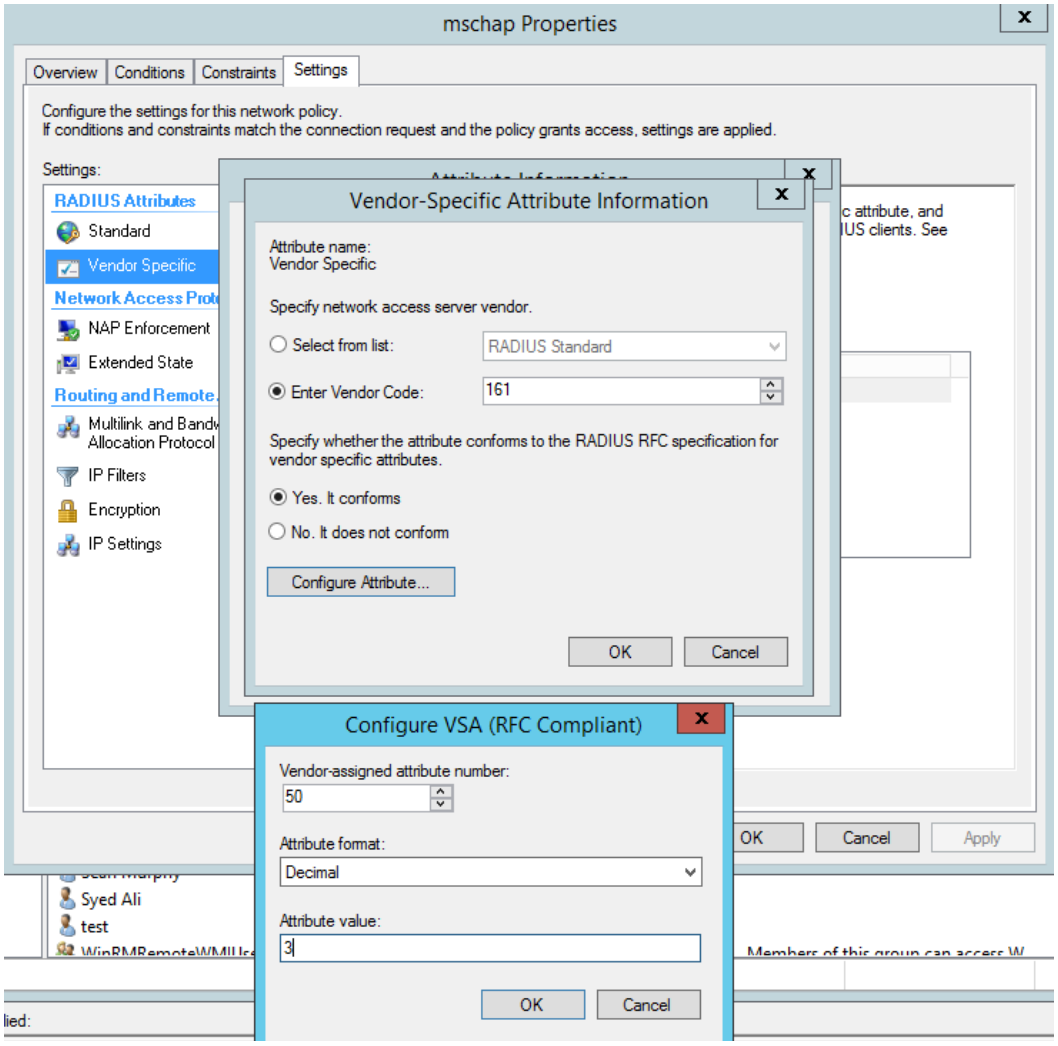
Before using VSA, the **Cambium-Canopy-UserLevel(50)** VSA must be configured with some access level say ADMIN(3).

Follow below link for configuring VSA:

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

The Cambium's vendor code is 161.

Figure 171 RADIUS VSA configuration



○ Accounting

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

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

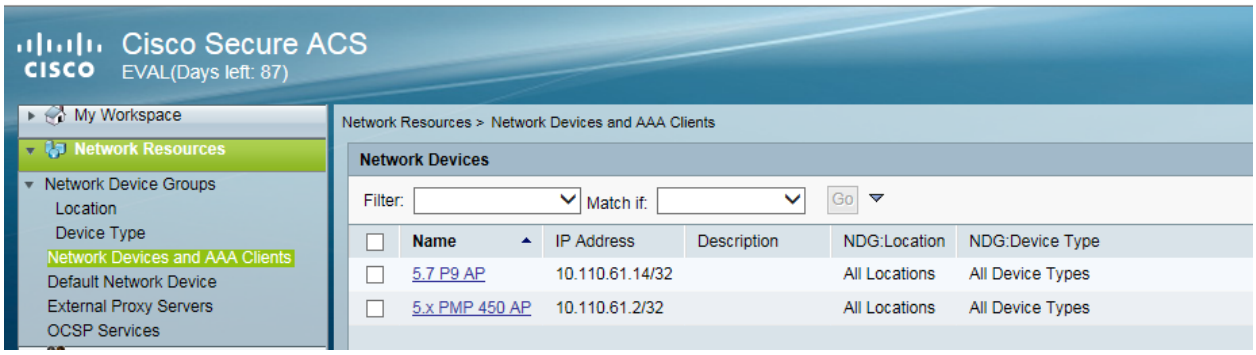
Cisco ACS RADIUS Server Support

This briefly explains how to configure Cisco ACS RADIUS server for PEAP-MSCHAPv2 authentication.

The configuration had been tested on **CISCO ACS Version : 5.7.0.15**

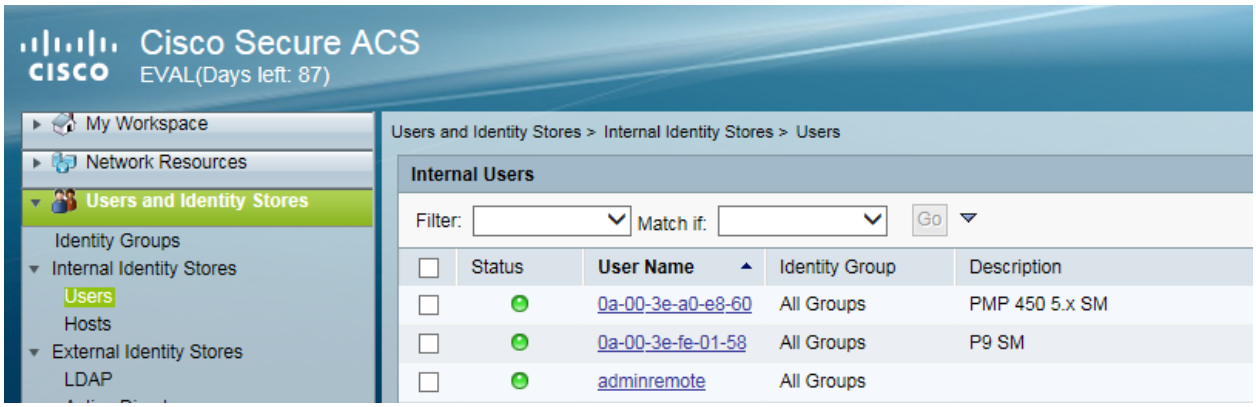
Adding RADIUS client

Figure 172 Adding RADIUS client



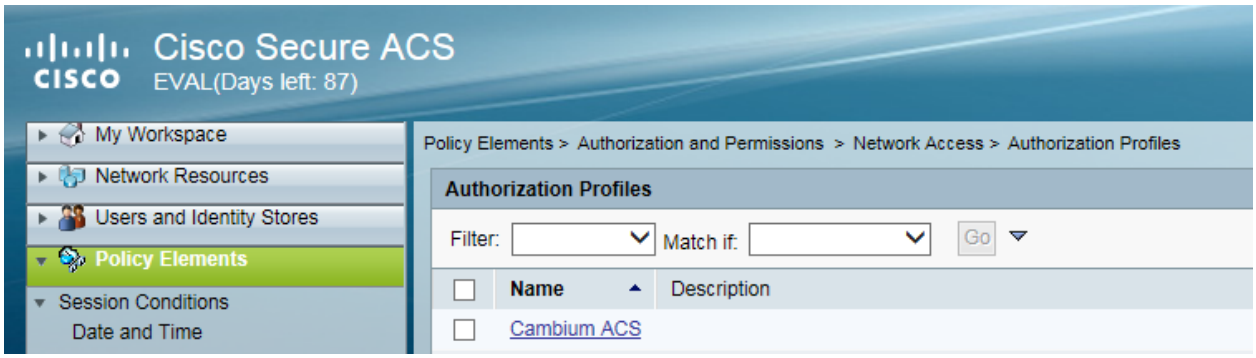
Creating Users

Figure 173 Creating users



Creating RADIUS instance

Figure 174 Creating RADIUS instance



RADIUS protocols

Figure 175 RADIUS protocols