RECOMMENDATION:
Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Sector ID

You can optionally enter an identifier to distinguish this link.

Downlink Data

The operator specifies the percentage of the aggregate (uplink and downlink total) throughput that is needed for the downlink. The default for this parameter is 50%.

Transmit Frame Spreading

If you select **Enable**, then a BHS between two BHMs can register in the assigned BHM (not the other BHM). Canopy *strongly recommends* that you select this option. With this selection, the BHM does not transmit a beacon in each frame, but rather transmits a beacon in only pseudo-random frames in which the BHS expects the beacon. This allows multiple BHMs to send beacons to multiple BHSs in the same range without interference.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900-MHz and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. In addition to setting the power in the 5.7-GHz connectorized module, the operator must set the antenna gain/cable loss such that the module can accurately report received power at the antenna.
- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of Canopy 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.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 326.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

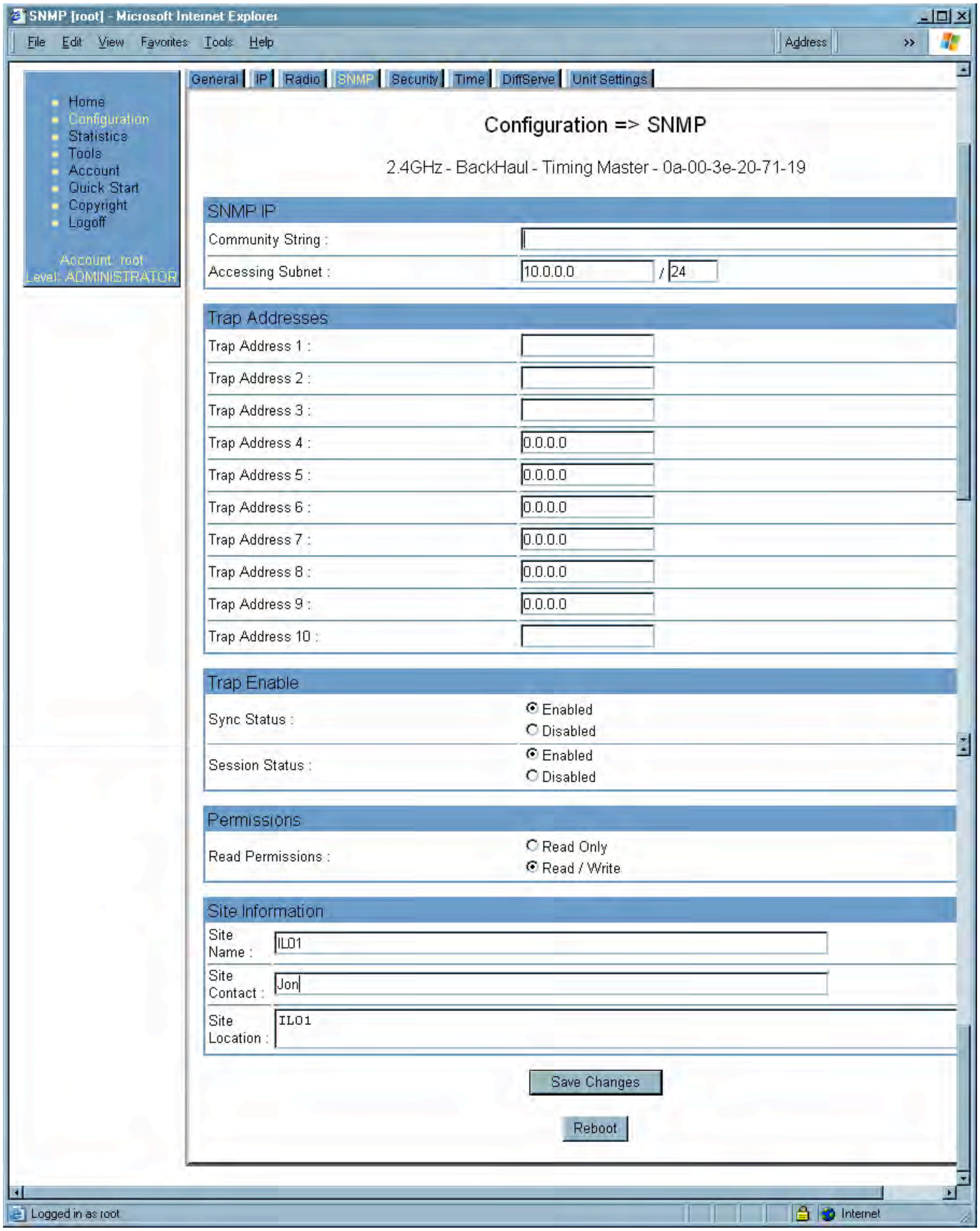
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.4 SNMP Tab of the BHM

An example of the SNMP tab in a BHM is displayed in Figure 109.



Account: root
Level: ADMINISTRATOR

Configuration => SNMP

2.4GHz - BackHaul - Timing Master - 0a-00-3e-20-71-19

SNMP IP

Community String :
Accessing Subnet : 10.0.0.0 / 24

Trap Addresses

Trap Address 1 :
Trap Address 2 :
Trap Address 3 :
Trap Address 4 : 0.0.0.0
Trap Address 5 : 0.0.0.0
Trap Address 6 : 0.0.0.0
Trap Address 7 : 0.0.0.0
Trap Address 8 : 0.0.0.0
Trap Address 9 : 0.0.0.0
Trap Address 10 :

Trap Enable

Sync Status : ● Enabled ○ Disabled
Session Status : ● Enabled ○ Disabled

Permissions

Read Permissions : ○ Read Only ● Read / Write

Site Information

Site Name : IL01
Site Contact : Jon
Site Location : IL01

Figure 109: SNMP tab of BHM, example

In the SNMP tab of the BHM, you may set the following parameters.

Community String

Specify a control string that allows Prizm or a Network Management Station (NMS) to access the module through SNMP. No spaces are allowed in this string. The default string is **Canopy**.

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.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this BHM. Prizm or 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 BHM, presuming that the device supplies the correct **Community String** value.

> *NOTE:*
> For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

The default treatment is to allow all networks access.

Trap Address *1 to 10*

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or 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

Select either **Sync Status** or **Session Status** to enable SNMP traps. If you select neither, then traps are disabled.

Read Permissions

Select **Read Only** if you wish to disallow any parameter changes by Prizm or an NMS.

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 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 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 an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

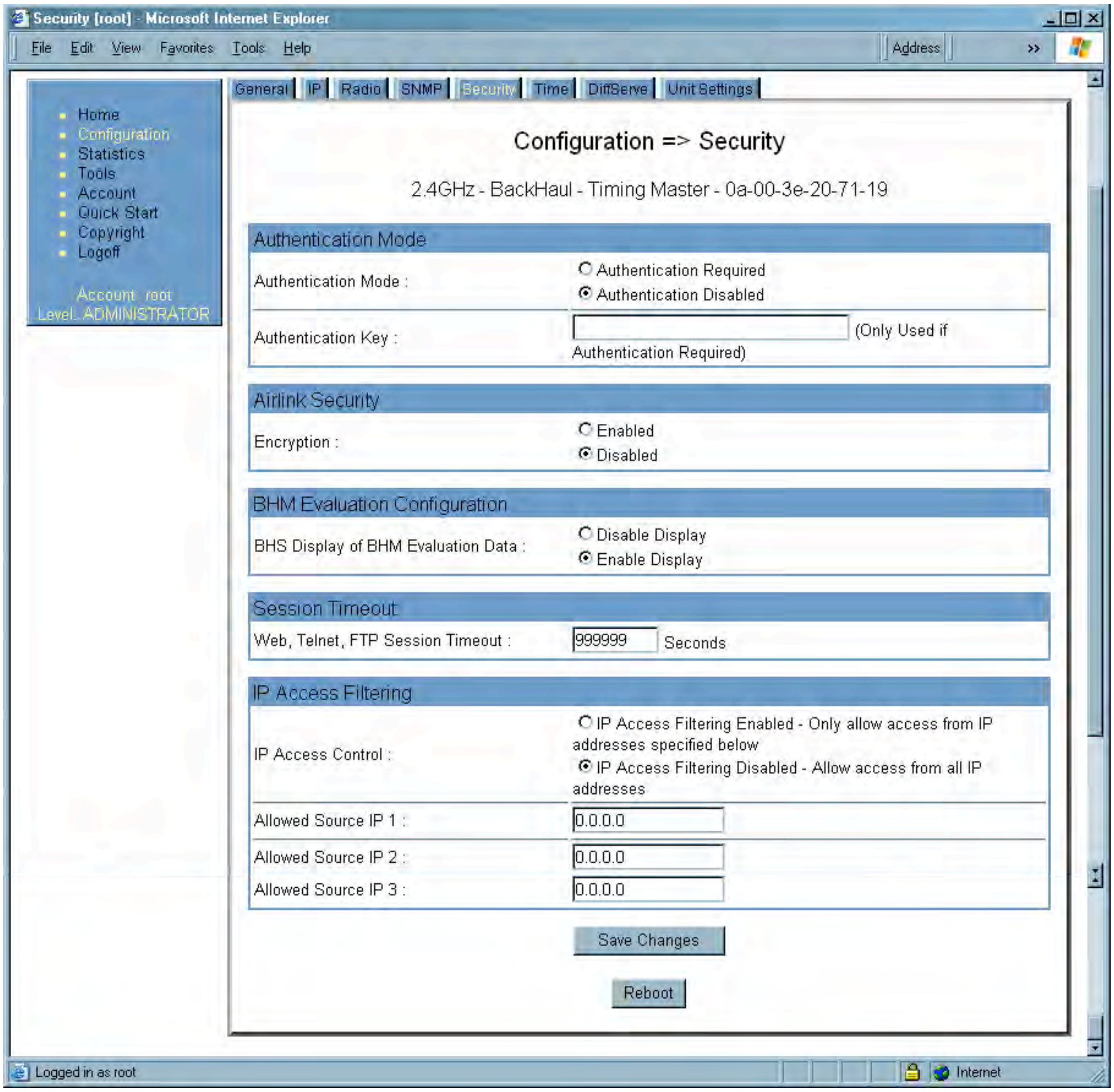
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.5 Security Tab of the BHM

An example of the Security tab in a BHM is displayed in Figure 110.



Configuration => Security

2.4GHz - BackHaul - Timing Master - 0a-00-3e-20-71-19

Authentication Mode

Authentication Mode : ○ Authentication Required ● Authentication Disabled

Authentication Key : (Only Used if Authentication Required)

Airlink Security

Encryption : ○ Enabled ● Disabled

BHM Evaluation Configuration

BHS Display of BHM Evaluation Data : ○ Disable Display ● Enable Display

Session Timeout

Web, Telnet, FTP Session Timeout : 999999 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

Allowed Source IP 2 : 0.0.0.0

Allowed Source IP 3 : 0.0.0.0

Figure 110: Security tab of BHM, example

In the Security tab of the BHM, you may set the following parameters.

Authentication Mode

Specify whether the BHM should require the BHS to authenticate.

Authentication Key

Only if you set the BHM in the previous parameter to require authentication, specify the key that the BHS should use when authenticating.

Encryption

Specify the type of air link security to apply to this BHM:

- **Encryption Disabled** provides no encryption on the air link. This is the default mode.
- **Encryption Enabled** provides encryption, using a factory-programmed secret key that is unique for each module.

> *NOTE:*
> In any BH link where encryption is enabled, the BHS briefly drops registration and re-registers in the BHM every 24 hours to change the encryption key.

BHS Display of BHM Evaluation Data

You can use this field to suppress the display of data (**Disable Display**) about this BHM on the BHM Evaluation tab of the Tools page in the BHS.

Web, Telnet, FTP Session Timeout

Enter the expiry in seconds for remote management sessions via HTTP, telnet, or ftp access to the BHM.

IP Access Control

You can permit access to the 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, including access and management by Prizm.

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 BHM 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.

The Security tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

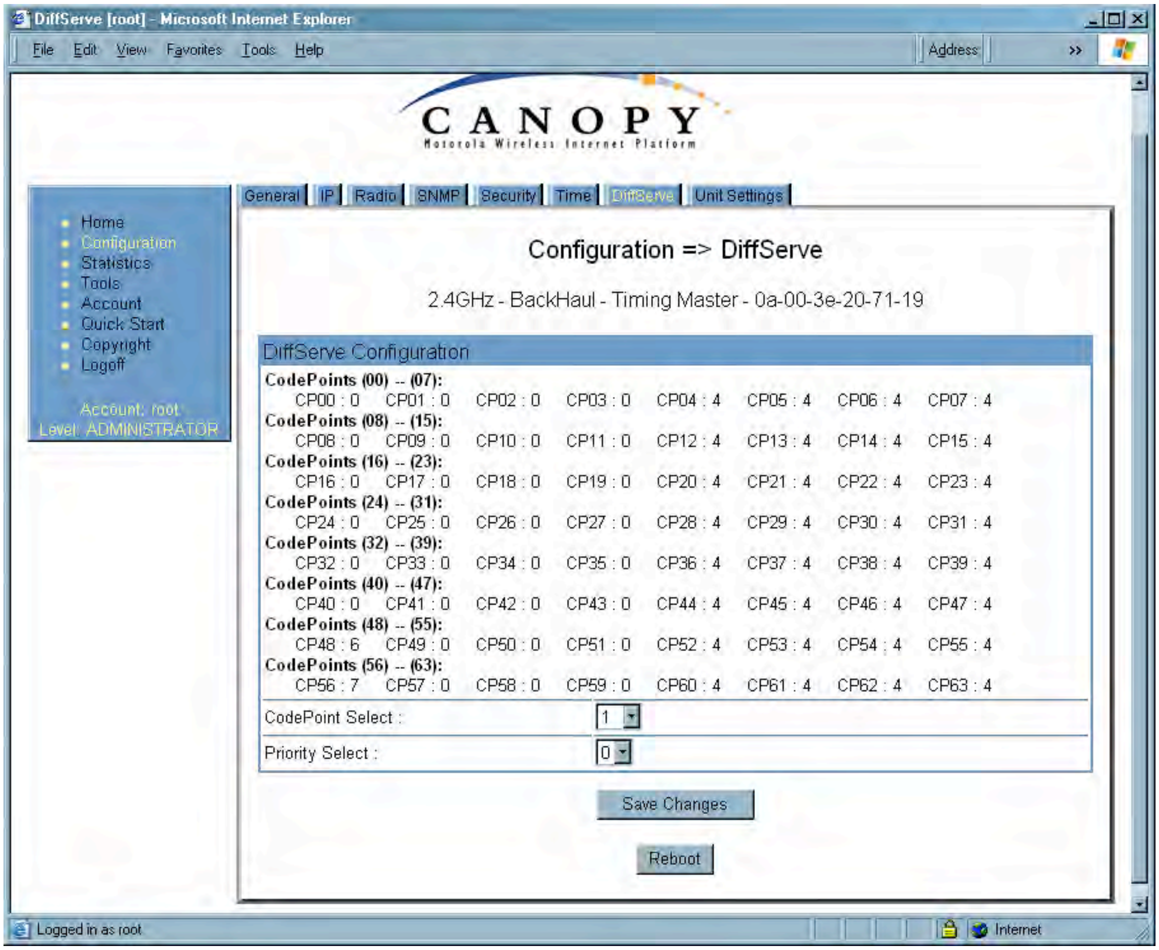
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.6 DiffServe Tab of the BHM

An example of the DiffServe tab in a BHM is displayed in Figure 111.


DiffServe [root] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CANOPY
Motorola Wireless Internet Platform
General IP Radio SNMP Security Time DiffServe Unit Settings
Home
Configuration
Statistics
Tools
Account
Quick Start
Copyright
Logoff
Account: root
Level: ADMINISTRATOR
Logged in as root
Internet

Configuration => DiffServe

2.4GHz - BackHaul - Timing Master - 0a-00-3e-20-71-19

DiffServe Configuration

CodePoints (00) -- (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4

CodePoints (08) -- (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4

CodePoints (16) -- (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4

CodePoints (24) -- (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4

CodePoints (32) -- (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4

CodePoints (40) -- (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 4

CodePoints (48) -- (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4

CodePoints (56) -- (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4

CodePoint Select :	1
Priority Select :	0

Figure 111: DiffServe tab of BHM, example

In the DiffServe tab of the BHM, you may set the following parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in Figure 119. Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the AP for all downlinks within the sector and in the SM for each uplink. See DSCP Field on Page 89.

The DiffServe tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

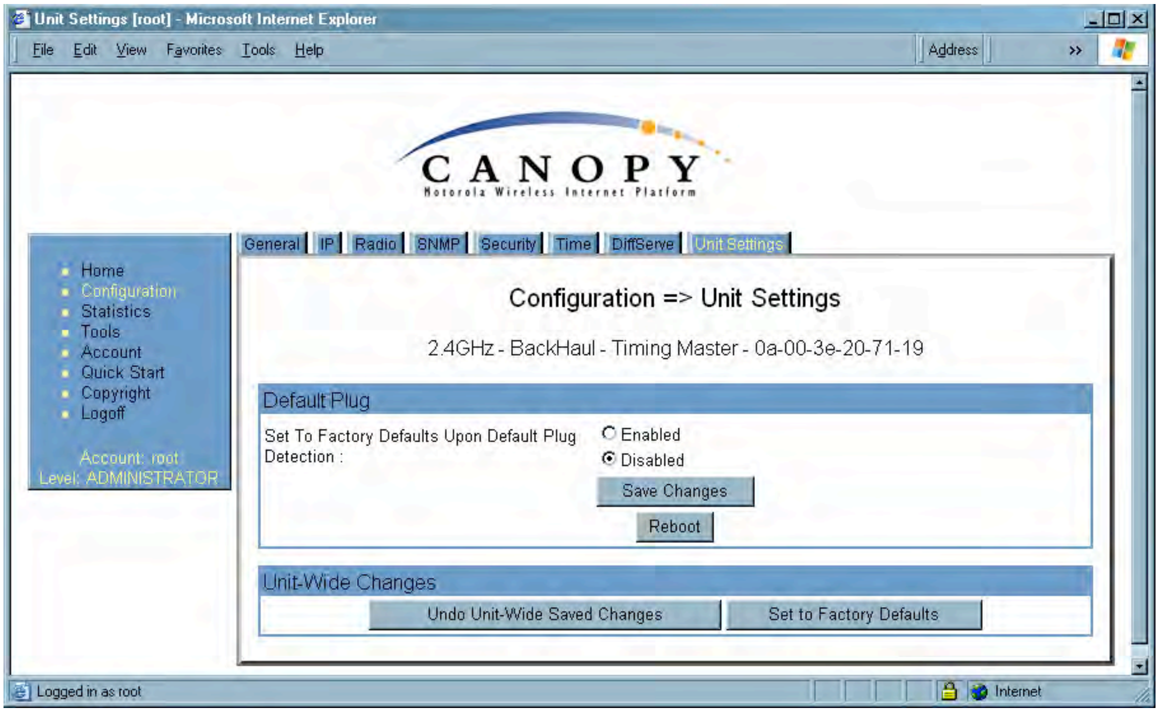
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.4.7 Unit Settings Tab of the BHM

An example of the Unit Settings tab of the BHM is displayed in Figure 112.



Configuration => Unit Settings

2.4GHz - BackHaul - Timing Master - 0a-00-3e-20-71-19

Default Plug

Set To Factory Defaults Upon Default Plug Detection : ○ Enabled ● Disabled

Unit-Wide Changes

Figure 112: Unit Settings tab of BHM, example

The Unit Settings tab of the BHM contains an option for how the BHM should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults.
A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 375.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

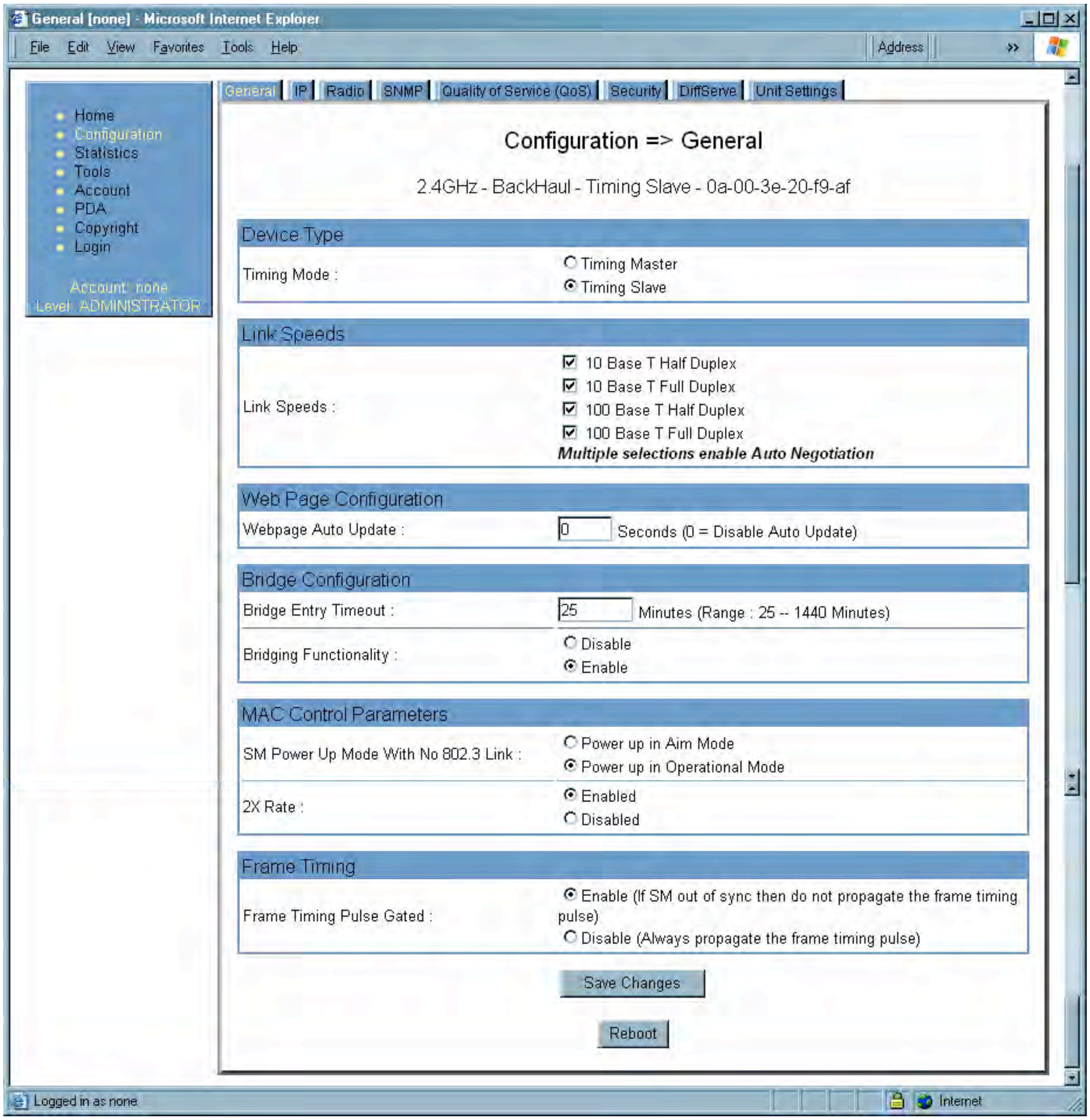
1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5 CONFIGURING A BH TIMING SLAVE FOR THE DESTINATION

If an ADMINISTRATOR-level password has been set in the BHS, you must log into the module before you can configure its parameters. See Managing Module Access by Passwords on Page 373.

18.5.1 General Tab of the BHS

An example of the General tab in a BHS is displayed in Figure 113.


General [none] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Home
Configuration
Statistics
Tools
Account
PDA
Copyright
Login
Account: none
Level: ADMINISTRATOR
General IP Radio SNMP Quality of Service (QoS) Security DiffServe Unit Settings
Save Changes
Reboot
Logged in as none
Internet

Configuration => General

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

Device Type	
Timing Mode :	○ Timing Master ● Timing Slave

Link Speeds	
Link Speeds :	☑ 10 Base T Half Duplex ☑ 10 Base T Full Duplex ☑ 100 Base T Half Duplex ☑ 100 Base T Full Duplex ***Multiple selections enable Auto Negotiation***

Web Page Configuration	
Webpage Auto Update :	0 Seconds (0 = Disable Auto Update)

Bridge Configuration	
Bridge Entry Timeout :	25 Minutes (Range : 25 -- 1440 Minutes)
Bridging Functionality :	○ Disable ● Enable

MAC Control Parameters	
SM Power Up Mode With No 802.3 Link :	○ Power up in Aim Mode ● Power up in Operational Mode
2X Rate :	● Enabled ○ Disabled

Frame Timing	
Frame Timing Pulse Gated :	● Enable (If SM out of sync then do not propagate the frame timing pulse) ○ Disable (Always propagate the frame timing pulse)

Figure 113: General tab of BHS, example

In the General tab of the BHS, you may set the following parameters.

Timing Mode

Select **Timing Slave**. This BH will receive sync from another source. Whenever you toggle this parameter to Timing Slave from Timing Master, you should also do the following:

1. Make no other changes in this or any other interface page.
2. Save this change of timing mode.
3. Reboot the BH.

RESULT: The set of interface web pages that is unique to a BHS is made available.

> *NOTE:*
> In a BHS that cannot be converted to a BHM, this parameter is not present (for example, in a BHS with Hardware Scheduling and Series P8 hardware.)

Link Speeds

Specify the type of link speed for the Ethernet connection. The default for this parameter is that all speeds are selected. The recommended setting is a single speed selection for all APs, BHs, and SMs in the operator network.

Webpage Auto Update

Enter the frequency (in seconds) for the web browser to automatically refresh the web-based interface. The default setting is 0. The 0 setting causes the web-based interface to never be automatically refreshed.

Bridge Entry Timeout

Specify the appropriate bridge timeout for correct network operation with the existing network infrastructure. Timeout occurs when the BHM encounters no activity with the BHS (whose MAC address is the bridge entry) within the interval that this parameter specifies. The Bridge Entry Timeout should be a longer period than the ARP (Address Resolution Protocol) cache timeout of the router that feeds the network.

This parameter governs the timeout interval, even if a router in the system has a longer timeout interval. The default value of this field is 25 minutes.

> *CAUTION!*
> An inappropriately low Bridge Entry Timeout setting may lead to temporary loss of communication with some end users.

Bridging Functionality

Select whether you want bridge table filtering active (**Enable**) or not (**Disable**) on this BHS. Selecting **Disable** allows you to use redundant BHs without causing network addressing problems. Through a spanning tree protocol, this reduces the convergence time from 25 minutes to mere seconds. However, you should disable bridge table filtering as only a deliberate part of your overall network design. Otherwise, disabling it allows unwanted traffic across the wireless interface.

SM Power Up Mode With No 802.3 Link

Specify the default mode in which this BHS will power up when it senses no Ethernet link. Select either

- **Power Up in Aim Mode**—the BHS boots in an aiming mode. When the BHS senses an Ethernet link, this parameter is automatically reset to Power Up in Operational Mode. When the BHS senses no Ethernet link within 15 minutes after power up, the BHS carrier shuts off.
- **Power Up in Operational Mode**—the BHS boots in Operational mode and attempts registration. Unlike in previous releases, this is the default selection in Release 8.

2X Rate

See 2X Operation on Page 91.

Frame Timing Pulse Gated

If this BHS extends the sync pulse to a BHM or an AP behind it, select either

- **Enable**—If this BHS loses sync, then *do not* propagate a sync pulse to the BHM or AP. This setting prevents interference in the event that the BHS loses sync.
- **Disable**—If this BHS loses sync, then propagate the sync pulse anyway to the BHM or AP.

See Wiring to Extend Network Sync on Page 369.

The General tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

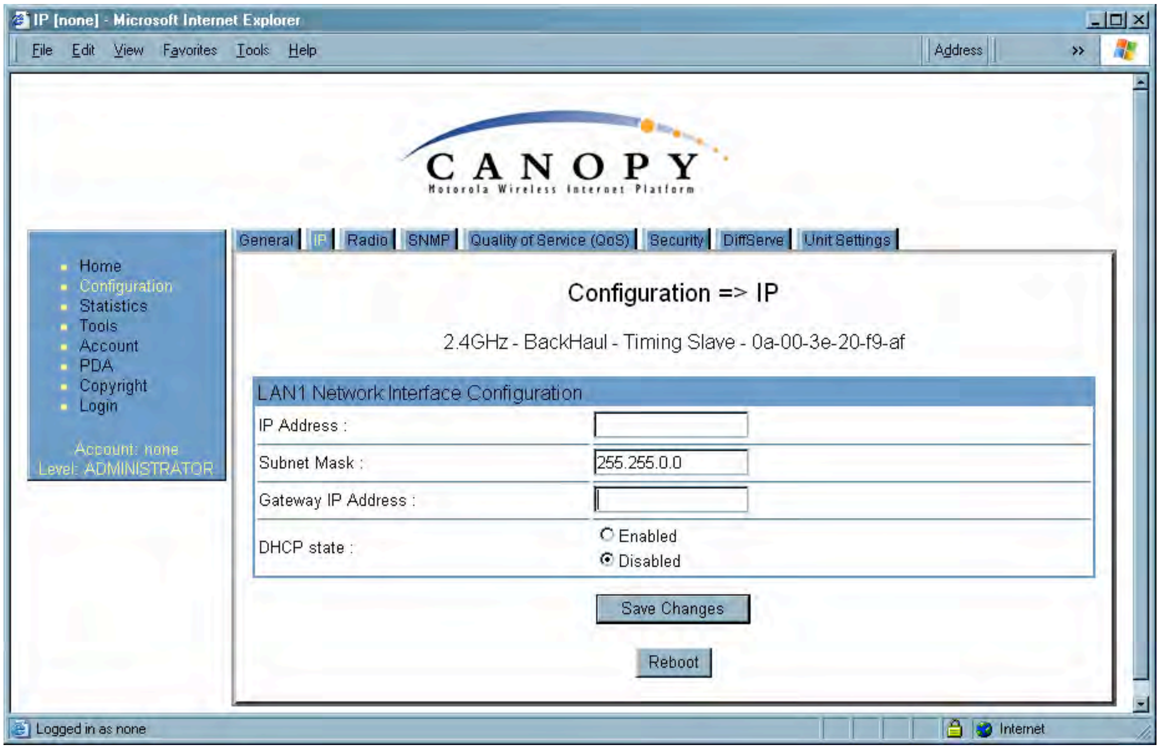
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.2 IP Tab of the BHS

An example of the IP tab in a BHS is displayed in Figure 114.



Configuration => IP

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

LAN1 Network Interface Configuration	
IP Address :	
Subnet Mask :	255.255.0.0
Gateway IP Address :	
DHCP state :	○ Enabled ● Disabled

Figure 114: IP tab of BHS, example

In the IP tab of the BHS, you may set the following parameters.

LAN1 Network Interface Configuration, IP Address

Enter the *non-routable* IP address to associate with the Ethernet connection on this BHS. (The default IP address from the factory is 169.254.1.1.) If you set and then forget this parameter, then you must both

1. physically access the module.
2. use an override plug to electronically access the module configuration parameters at 169.254.1.1. See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 377.

RECOMMENDATION:
Note or print the IP settings from this page. Ensure that you can readily associate these IP settings both with the module and with the other data that you store about the module.

LAN1 Network Interface Configuration, Subnet Mask

Enter an appropriate subnet mask for the BHS to communicate on the network. The default subnet mask is 255.255.0.0. See Allocating Subnets on Page 162.

LAN1 Network Interface Configuration, Gateway IP Address

Enter the appropriate gateway for the BHS to communicate with the network. The default gateway is 169.254.0.0.

LAN1 Network Interface Configuration, DHCP State

If you select **Enabled**, 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, but not settable, in the Network Interface tab of the Home page.

The IP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the IP Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

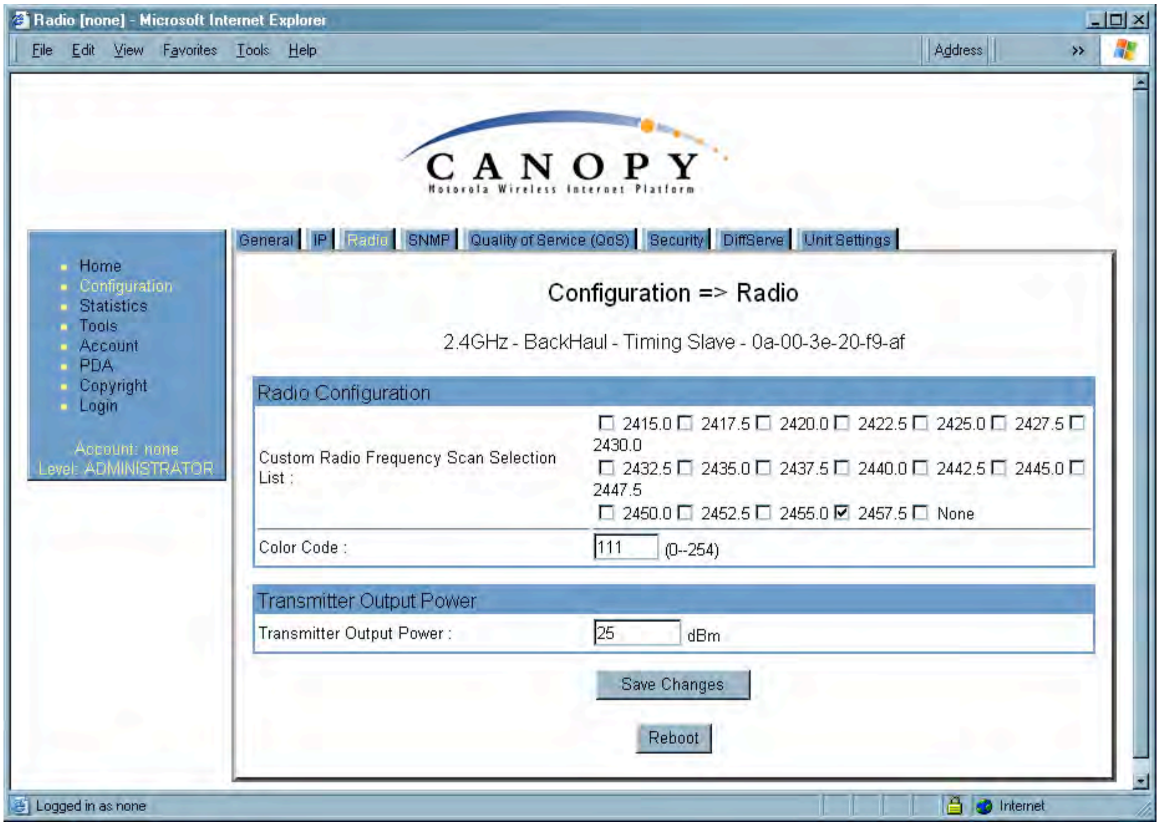
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.3 Radio Tab of the BHS

An example of the Radio tab in a BHS is displayed in Figure 115.



Configuration => Radio

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

Radio Configuration

Custom Radio Frequency Scan Selection List : □ 2415.0 □ 2417.5 □ 2420.0 □ 2422.5 □ 2425.0 □ 2427.5 □ 2430.0 □ 2432.5 □ 2435.0 □ 2437.5 □ 2440.0 □ 2442.5 □ 2445.0 □ 2447.5 □ 2450.0 □ 2452.5 □ 2455.0 ☑ 2457.5 □ None

Color Code : 111 (0--254)

Transmitter Output Power

Transmitter Output Power : 25 dBm

Figure 115: Radio tab of BHS, example

In the Radio tab of the BHS, you may set the following parameters.

Custom Radio Frequency Scan Selection List

Specify the frequency that the BHS should scan to find the BHM. The frequency *band* of the BHs affects what channels you select.

> *IMPORTANT!*
> In the 2.4-GHz frequency band, the BHS can register to a BHM that transmits on a frequency 2.5 MHz higher than the frequency that the BHS receiver locks when the scan terminates as successful. This establishes a poor-quality link. To prevent this, select frequencies that are at least 5 MHz apart.

In a 2.4-GHz BHS, this parameter displays all available channels, but has only three recommended channels selected by default. See 2.4-GHz AP Cluster Recommended Channels on Page 137.

In a 5.2- or 5.4-GHz BHS, this parameter displays only ISM frequencies. In a 5.7-GHz BHS, this parameter displays both ISM and U-NII frequencies. If you select all frequencies that are listed (default selections), then the module scans for a signal on any channel. If you select only one, then the module limits the scan to that channel. Since the frequencies that this parameter offers for each of these two bands are 5 MHz apart, a scan of *all* channels does not risk establishment of a poor-quality link as in the 2.4-GHz band. Nevertheless, this can risk establishment of a link to the wrong BHM.

A list of channels in the band is provided in Considering Frequency Band Alternatives on Page 136.

(The selection labeled **Factory** requires a special software key file for implementation.)

Color Code

Specify a value from 0 to 254. For registration to occur, the color code of the BHM and the BHS *must* match. On all Canopy modules, the default setting for the color code value is 0. This value matches only the color code of 0 (*not* all 255 color codes).

> *RECOMMENDATION:*
> Note the color code that you enter. Ensure that you can readily associate this color code both with the module and with the other data that you store about the module.

Transmitter Output Power

Nations and regions may regulate transmitter output power. For example

- Both 900-MHz and 5.7-GHz modules are available as connectorized radios, which require the operator to adjust power to ensure regulatory compliance. In addition to setting the power in the 5.7-GHz connectorized module, the operator must set the antenna gain/cable loss such that the module can accurately report received power at the antenna.

- Legal maximum allowable transmitter output power and EIRP (Equivalent Isotropic Radiated Power) in the 2.4-GHz frequency band varies by country and region. The output power of Series P9 2.4-GHz modules can be adjusted to meet these national or regional regulatory requirements.
- Countries and regions that permit the use of the 5.4-GHz frequency band (CEPT member states, for example), generally require equipment using the band to have adjustable power.

The professional installer of Canopy 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.

For information on how to calculate the permissible transmitter output power to enter in this parameter, see Adjusting Transmitter Output Power on Page 326.

The Radio tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

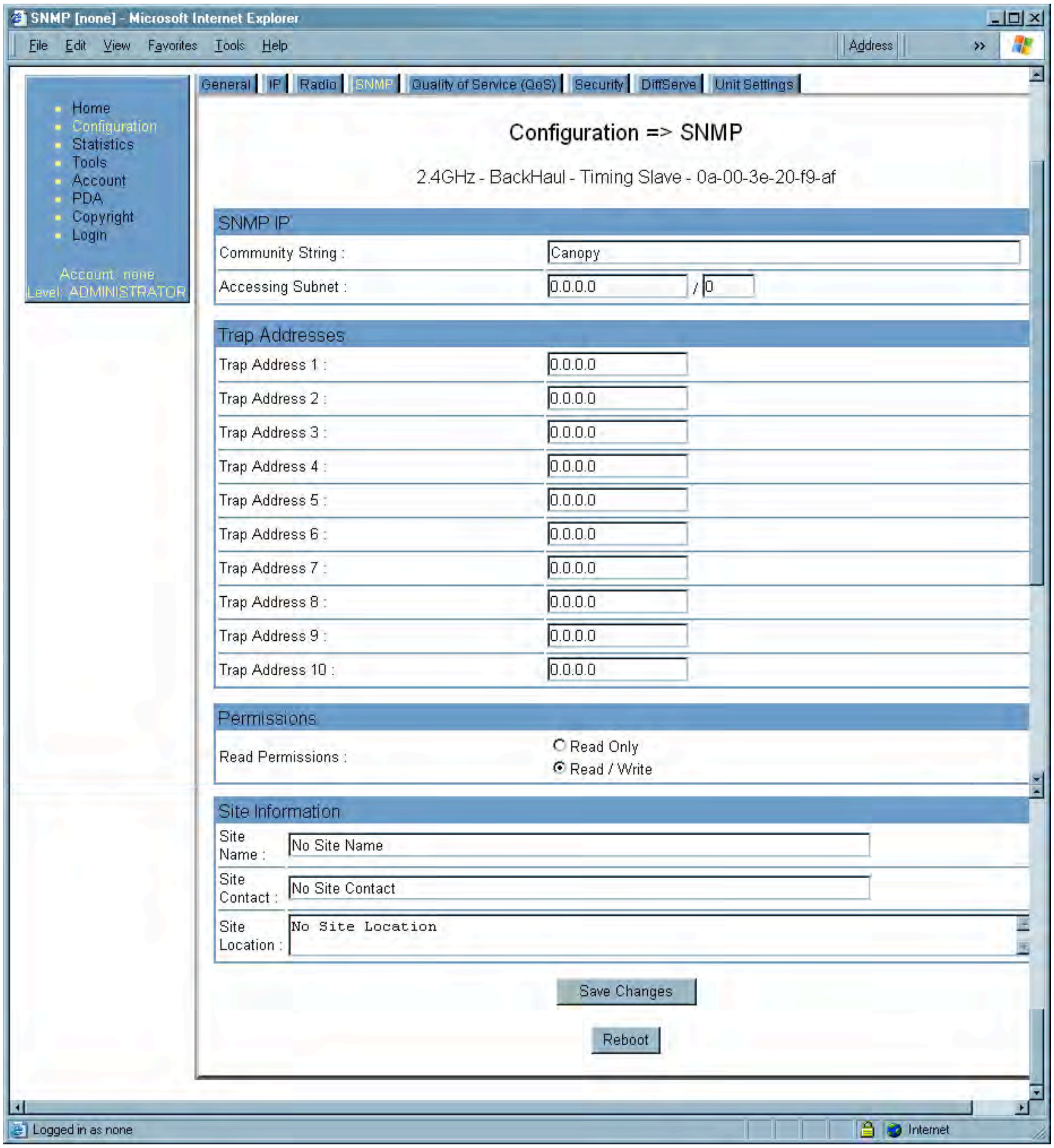
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.4 SNMP Tab of the BHS

An example of the SNMP tab in a BHS is displayed in Figure 116.



SNMP [none] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
General IP Radio SNMP Quality of Service (QoS) Security DiffServe Unit Settings
Home
Configuration
Statistics
Tools
Account
PDA
Copyright
Login
Save Changes
Reboot
Internet

Account: none
Level: ADMINISTRATOR

Configuration => SNMP

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

SNMP IP

Community String :	Canopy
Accessing Subnet :	0.0.0.0 / 0

Trap Addresses

Trap Address 1 :	0.0.0.0
Trap Address 2 :	0.0.0.0
Trap Address 3 :	0.0.0.0
Trap Address 4 :	0.0.0.0
Trap Address 5 :	0.0.0.0
Trap Address 6 :	0.0.0.0
Trap Address 7 :	0.0.0.0
Trap Address 8 :	0.0.0.0
Trap Address 9 :	0.0.0.0
Trap Address 10 :	0.0.0.0

Permissions

Read Permissions :	○ Read Only ● Read / Write

Site Information

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

Logged in as none

Figure 116: SNMP tab of BHS, example

In the SNMP tab of the BHS, you may set the following parameters.

Community String

Specify a control string that allows Prizm or an NMS (Network Management Station) to access MIB information about this BHS. No spaces are allowed in this string. The default string is **Canopy**.

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.

Accessing Subnet

Specify the addresses that are allowed to send SNMP requests to this BHS. Prizm or 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 BHS, presuming that the device supplies the correct **Community String** value.

The default treatment is to allow all networks access (set to 0). For more information on CIDR, execute an Internet search on “Classless Interdomain Routing.”

Trap Address *1 to 10*

Specify ten or fewer IP addresses (xxx.xxx.xxx.xxx) to which trap information should be sent. Trap information informs Prizm or an NMS that something has occurred. For example, trap information is sent

- after a reboot of the module.
- when Prizm or 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.

Read Permissions

Select **Read Only** if you wish to disallow Prizm or NMS SNMP access to configurable parameters and read-only fields of the SM.

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 Prizm 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 Prizm 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 Prizm or an NMS. The buffer size for this field is 128 characters.

The SNMP tab also provides the following buttons.

Save Changes

When you click this button, any changes that you made on the Configuration page are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

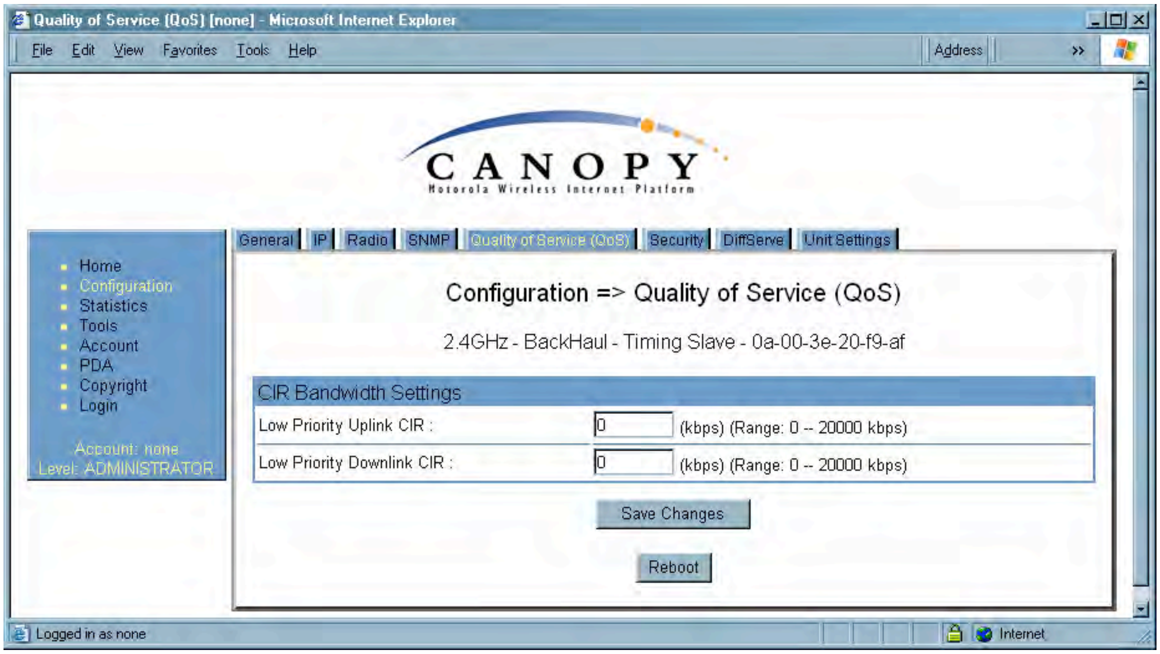
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.5 Quality of Service (QoS) Tab of the BHS

An example of the Quality of Service tab of the BHS is displayed in Figure 117.



Configuration => Quality of Service (QoS)

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

CIR Bandwidth Settings	
Low Priority Uplink CIR :	0 (kbps) (Range: 0 -- 20000 kbps)
Low Priority Downlink CIR :	0 (kbps) (Range: 0 -- 20000 kbps)

Figure 117: Quality of Service (QoS) tab of BHS, example

In the Quality of Service (QoS) tab of the BHS, you may set the following parameters.

Low Priority Uplink CIR

See

- Committed Information Rate on Page 87
- Setting the Configuration Source on Page 292.

Low Priority Downlink CIR

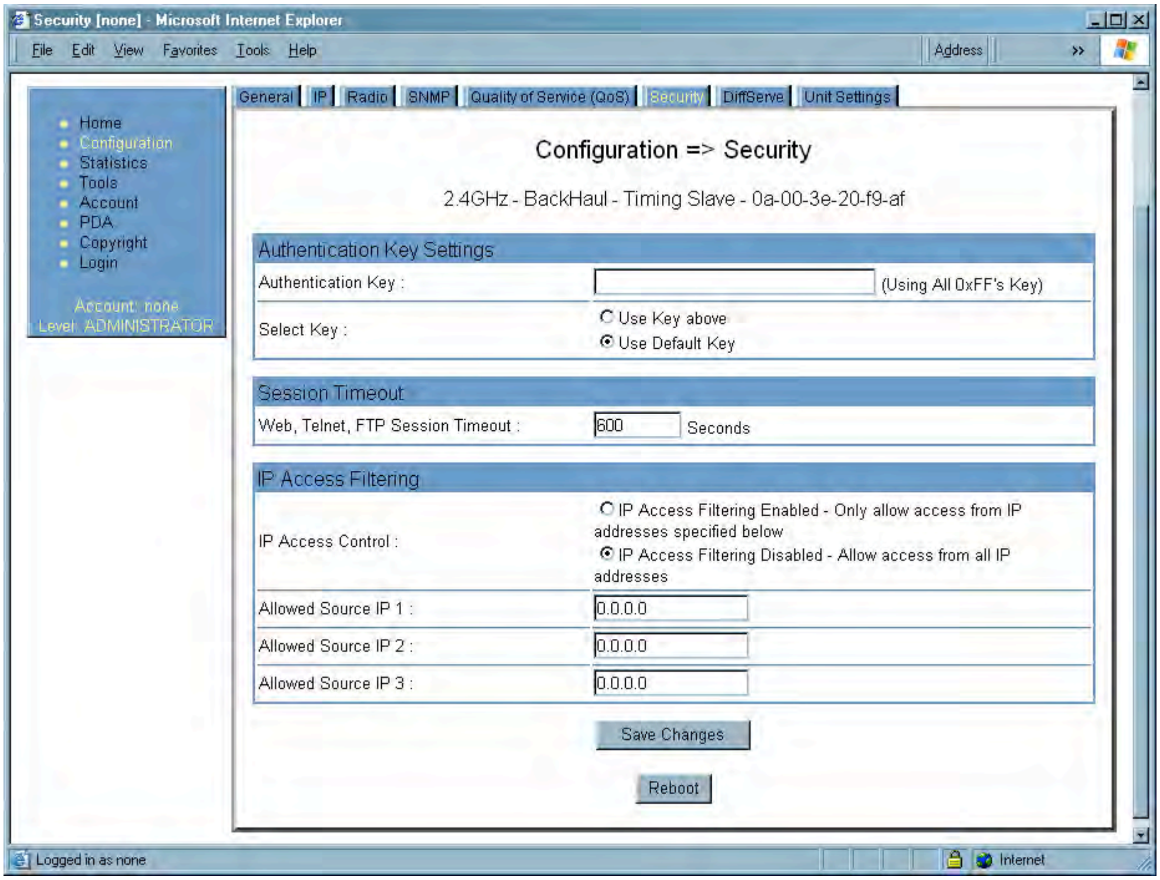
See

- Committed Information Rate on Page 87

- ◦ Setting the Configuration Source on Page 292.

18.5.6 Security Tab of the BHS

An example of the Security tab in a BHS is displayed in Figure 118.



Configuration => Security

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

Authentication Key Settings

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

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
Allowed Source IP 2 :	0.0.0.0
Allowed Source IP 3 :	0.0.0.0

Figure 118: Security tab of BHS, example

In the Security tab of the BHS, you may set the following parameters.

Authentication Key

Only if the BHM to which this BHS will register requires authentication, specify the key that the BHS should use when authenticating. For alpha characters in this hex key, use only upper case.

> *NOTE:*
> Canopy recommends that you enter 32 characters to achieve the maximal security from this feature.

Select Key

The **Use Default Key** selection specifies that the link should continue to use the automatically generated authentication key. See Authentication Manager Capability on Page 385.

The **Use Key above** selection specifies the 32-digit hexadecimal key that is permanently stored on both the BHS and the BHM.

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, including access and management by Prizm.

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.

The Security tab of the BHS also provides the following buttons.

Save Changes

When you click this button, any changes that you made on this tab are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

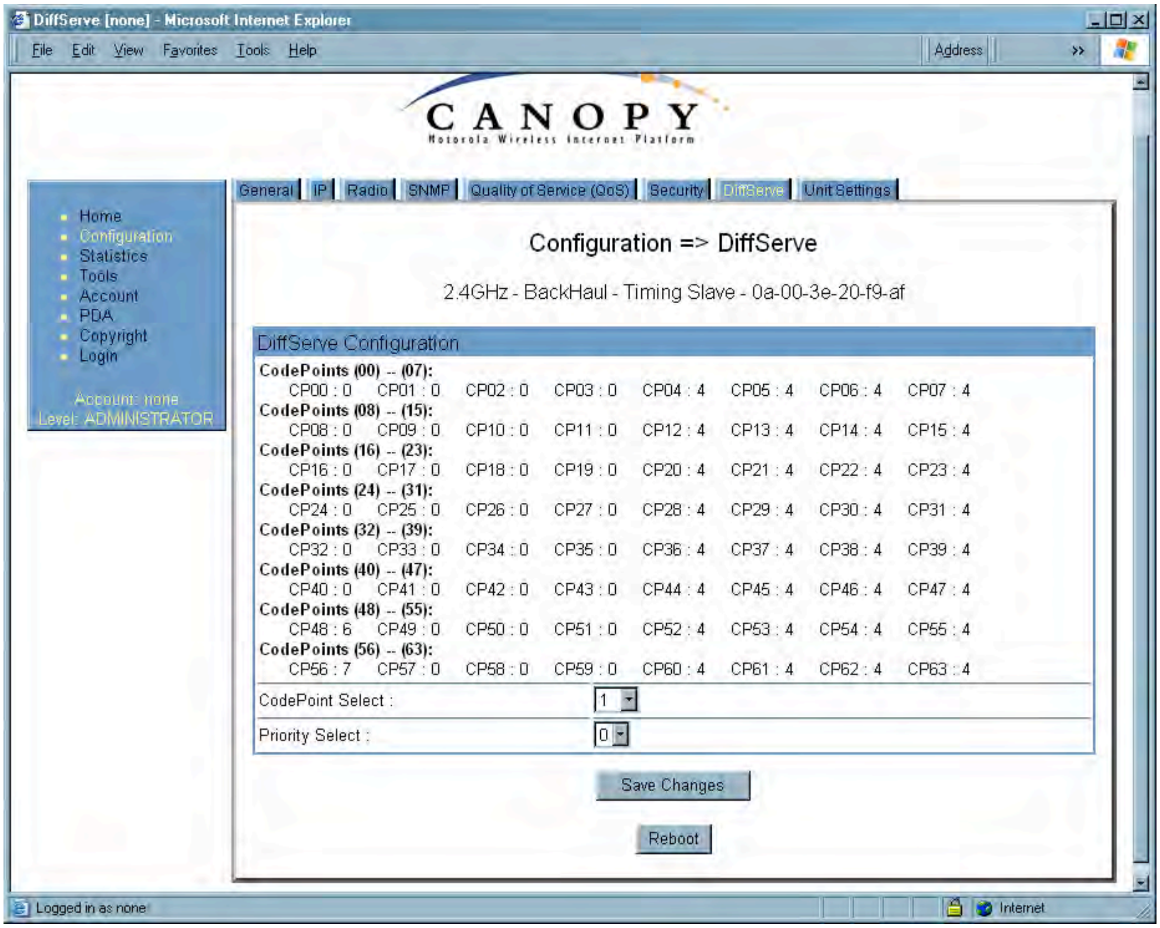
Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

18.5.7 DiffServe Tab of the BHS

An example of the DiffServe tab in a BHS is displayed in Figure 119.



Configuration => DiffServe

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

DiffServe Configuration

CodePoints (00) -- (07):
CP00 : 0 CP01 : 0 CP02 : 0 CP03 : 0 CP04 : 4 CP05 : 4 CP06 : 4 CP07 : 4

CodePoints (08) -- (15):
CP08 : 0 CP09 : 0 CP10 : 0 CP11 : 0 CP12 : 4 CP13 : 4 CP14 : 4 CP15 : 4

CodePoints (16) -- (23):
CP16 : 0 CP17 : 0 CP18 : 0 CP19 : 0 CP20 : 4 CP21 : 4 CP22 : 4 CP23 : 4

CodePoints (24) -- (31):
CP24 : 0 CP25 : 0 CP26 : 0 CP27 : 0 CP28 : 4 CP29 : 4 CP30 : 4 CP31 : 4

CodePoints (32) -- (39):
CP32 : 0 CP33 : 0 CP34 : 0 CP35 : 0 CP36 : 4 CP37 : 4 CP38 : 4 CP39 : 4

CodePoints (40) -- (47):
CP40 : 0 CP41 : 0 CP42 : 0 CP43 : 0 CP44 : 4 CP45 : 4 CP46 : 4 CP47 : 4

CodePoints (48) -- (55):
CP48 : 6 CP49 : 0 CP50 : 0 CP51 : 0 CP52 : 4 CP53 : 4 CP54 : 4 CP55 : 4

CodePoints (56) -- (63):
CP56 : 7 CP57 : 0 CP58 : 0 CP59 : 0 CP60 : 4 CP61 : 4 CP62 : 4 CP63 : 4

CodePoint Select : 1

Priority Select : 0

Figure 119: DiffServe tab of BHS, example

You may set the following Differentiated Services Configuration page parameters.

CodePoint 1 through CodePoint 47

CodePoint 49 through CodePoint 55

CodePoint 57 through CodePoint 63

The default priority value for each settable CodePoint is shown in Figure 119. Priorities of 0 through 3 map to the low-priority channel; 4 through 7 to the high-priority channel. The mappings are the same as 802.1p VLAN priorities.

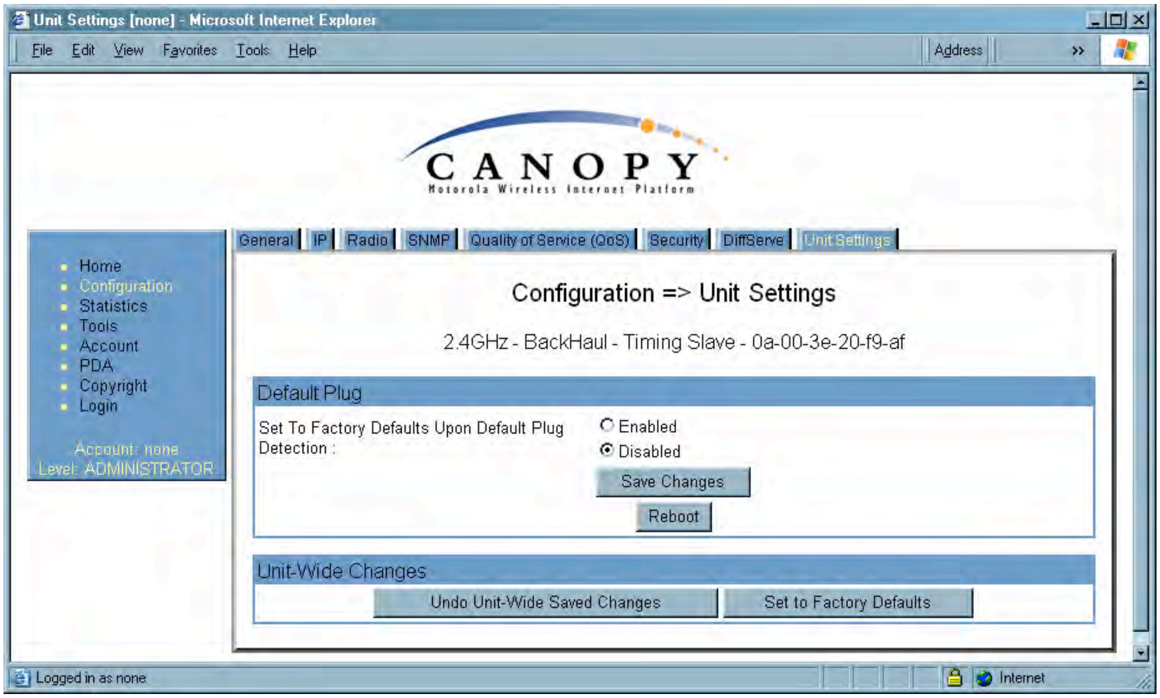
Consistent with RFC 2474

- **CodePoint 0** is predefined to a fixed priority value of **0** (low-priority channel).
- **CodePoint 48** is predefined to a fixed priority value of **6** (high-priority channel).
- **CodePoint 56** is predefined to a fixed priority value of **7** (high-priority channel).

You cannot change any of these three fixed priority values. Among the settable parameters, the priority values (and therefore the handling of packets in the high- or low-priority channel) are set in the BHM for the downlink and in the BHS for the uplink. See DSCP Field on Page 89.

18.5.8 Unit Settings Tab of the BHS

An example of the Unit Settings tab in a BHS is displayed in Figure 120.



Account: none
Level: ADMINISTRATOR

Configuration => Unit Settings

2.4GHz - BackHaul - Timing Slave - 0a-00-3e-20-f9-af

Default Plug

Set To Factory Defaults Upon Default Plug Detection : ○ Enabled ● Disabled

Unit-Wide Changes

Figure 120: Unit Settings tab of BHS, example

The Unit Settings tab of the BHS contains an option for how the BHS should react when it detects a connected override plug. You may set this option as follows.

Set to Factory Defaults Upon Default Plug Detection

If **Enabled** is checked, then an override/default plug functions as a default plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all parameter values are reset to defaults.
A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *cannot* see or learn the settings that were previously configured in it. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the default values for any that were not.

If **Disabled** is checked, then an override/default plug functions as an override plug. When the module is rebooted with the plug inserted, it can be accessed at the IP address 169.254.1.1 and no password, and all previously configured parameter values remain and are displayed. A subscriber, technician, or other person who gains physical access to the module and uses an override/default plug *can* see and learn the settings. When the module is later rebooted with no plug inserted, the module uses the new values for any parameters that were changed and the previous values for any that were not.

See Overriding Forgotten IP Addresses or Passwords on AP, SM, or BH on Page 375.

The Unit Settings tab also contains the following buttons.

Save Changes

When you click this button, any changes that you made on all tabs are recorded in flash memory. However, these changes *do not* apply until the next reboot of the module.

Reboot

When you click this button

1. the module reboots.
2. any changes that you saved by a click of the **Save Changes** button are implemented.

Undo Unit-Wide Saved Changes

When you click this button, any changes that you made in any tab but did not commit by a reboot of the module are undone.

Set to Factory Defaults

When you click this button, *all configurable parameters on all tabs* are reset to the factory settings.

18.6 ADJUSTING TRANSMITTER OUTPUT POWER

Authorities may require transmitter output power to be adjustable and/or lower than the highest that a module produces. Canopy adjustable power modules include a Radio tab parameter to reduce power to achieve compliance. If you set this parameter to lower than the range of the hardware in a given module, the value is automatically reset to the lowest value the hardware is capable of.

The best practice is to

- maintain awareness of applicable regulations.
- calculate the permissible transmitter output power for the module.
- confirm that the initial power setting is compliant.

- confirm that the power setting is compliant following any reset of the module to factory defaults.
- Adjust (usually reduce) transmit power so as to have a good signal at the receiver without transmitting excesss power. Note this usually means reducing transmit power for close-in SMs, while setting the AP to reach its most distant SM. For BHs, this usually means reducing the power symmetrically.

> ***IMPORTANT!***
> In the European Union, operators are under regulatory requirements to control transmit power so as to enhance sharing with other band users.

The total gain per antenna in 900-MHz and 5.7-GHz Canopy radios is stated in Table 52.

Table 52: Total gain per antenna

Antenna	Antenna Gain	Cable Loss[1]	Net Gain
900-MHz Integrated	12.5 dBi	0.2 dB	12 dBi
900-MHz Connectorized with Mars, MTI, or Maxrad antenna.	10 to 10.5 dBi	0.3 dB	10 dBi
5.7-GHz Connectorized	variable	0.3 dB + from any additional cable	See Note 2
5.7-GHz Connectorized with Mars antenna	15.5 dBi	0.3 dB	15 dBi

NOTES:

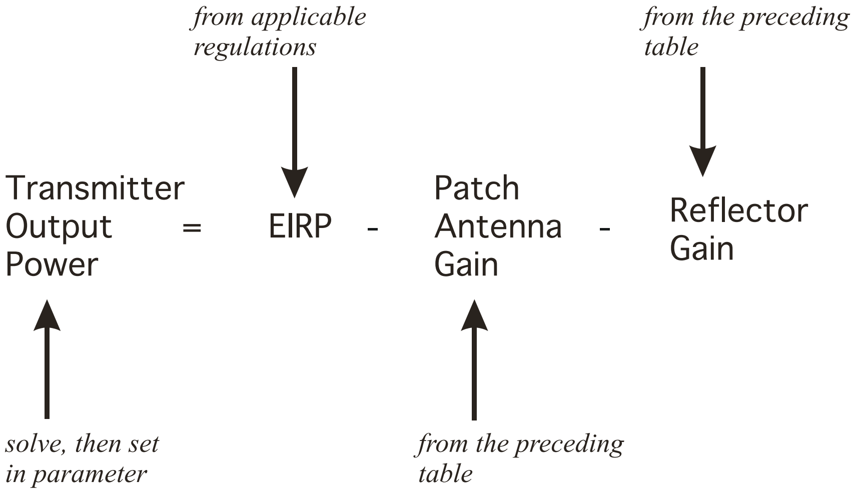
1. Received signal measurements take this loss into account, but the transmitter output power setting cannot. Set the transmitter output power higher by this amount.
2. Antenna gain minus cable loss.

Integrated patch antenna and reflector gains are provided in Table 53.

Table 53: Patch antenna and reflector gain

Frequency Band Range	Gain	
	Patch Antenna	Reflector
2.4 GHz	8 dBi	11dBi
5.2, 5.4, or 5.7 GHz	7 dBi	18dBi

The calculation of transmitter output power is as follows:



Transmitter output power is settable as dBm on the Radio tab of the module. Example cases of transmitter output power settings are shown in Table 54.

Table 54: Transmitter output power settings, example cases

Frequency Band Range and Antenna Scheme	Region	Maximum EIRP in Region	Transmitter Output Power Setting	
			AP, SM, or BH with No Reflector	SM or BH with Reflector
900 MHz Integrated	U.S.A. Canada	36 dBm (4 W)	24 dBm	
900 MHz Connectorized	U.S.A. Canada	36 dBm (4 W)	26 dBm[1]	
	Australia	30 dBm (1 W)	Depends on antenna	
2.4 GHz Integrated	U.S.A. Canada	Depends on antenna gain	25 dBm	25 dBm
	CEPT states	20 dBm (100 mW)	12 dBm	1 dBm
5.2 GHz Integrated	U.S.A. Canada	30 dBm (1 W)	23 dBm	
5.4 GHz Integrated	CEPT states U.S.A Canada	30 dBm (1 W)	23 dBm	5 dBm
5.7 GHz Connectorized	UK	33 dBm (2 W)	Depends on antenna	
5.7 GHz Connectorized[2]	U.S.A	36 dBm (4W)	21 dBm	

NOTES:

1. With Mars, MTI, or Maxrad antenna. This is the default setting, and 28 dBm is the highest settable value. The lower default correlates to 36 dBm EIRP where 10-dBi antennas are used. The default setting for this parameter is applied whenever **Set to Factory Defaults** is selected.
2. Only AP available

19 INSTALLING COMPONENTS

> ***RECOMMENDATION:***
> Use *shielded* cable for all Canopy infrastructure connections associated with BHs, APs, and CMMs. The environment that these modules operate in often has significant unknown or varying RF energy. Operator experience consistently indicates that the additional cost of shielded cables is more than compensated by predictable operation and reduced costs for troubleshooting and support.

19.1 PDA ACCESS TO CANOPY MODULES

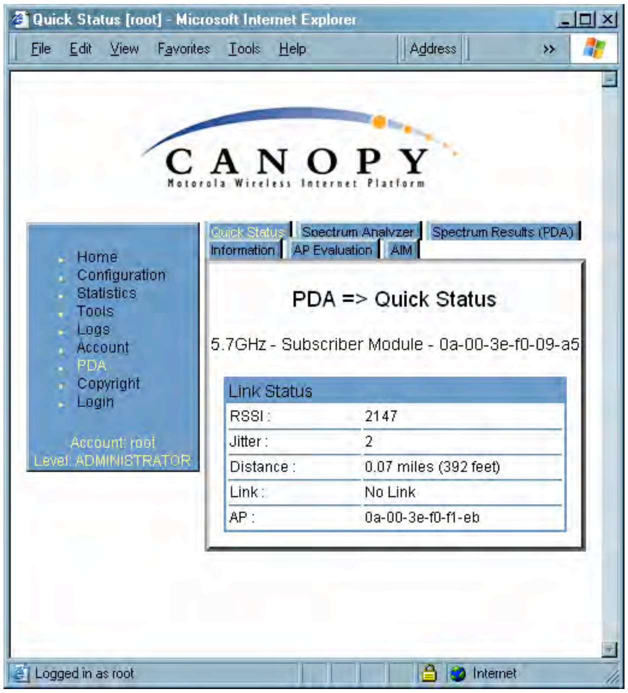
For RF spectrum analysis or module aiming on a roof or tower, a personal digital assistant (PDA) is easier to carry than, and as convenient to use as, a notebook computer. The PDA is convenient to use because no scrolling is required to view

- spectrum analysis results.
- RSSI and jitter.
- master module evaluation data.
- information that identifies the module, software, and firmware.

To access this data in a format the fits a 320 x 240 pixel PDA screen, the PDA must have all of the following:

- a Compact Flash card slot.
- any of several Compact Flash wired Ethernet cards.
- a wired Ethernet connection to the module.
- a browser directed to http://*ModuleIPAddress*/pda.html.

The initial PDA tab reports link status, as shown in Figure 121.



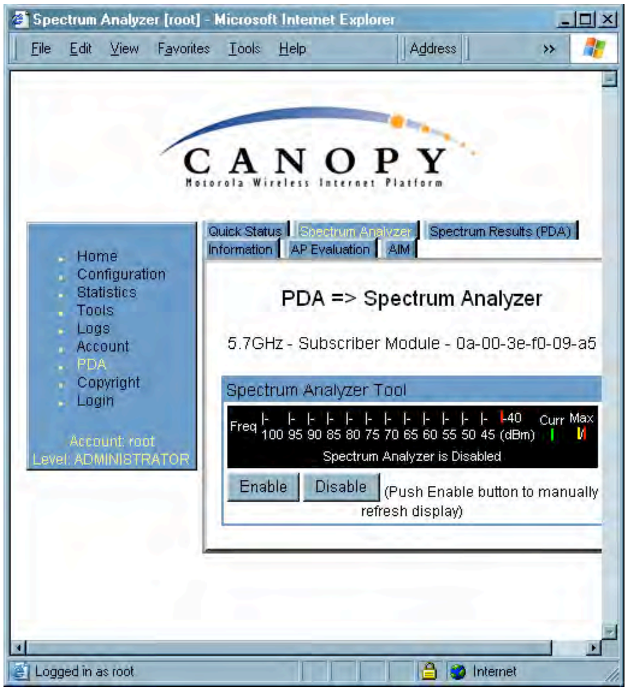
PDA => Quick Status

5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5

Link Status	
RSSI :	2147
Jitter :	2
Distance :	0.07 miles (392 feet)
Link :	No Link
AP :	0a-00-3e-f0-f1-eb

Figure 121: PDA Quick Status tab, example

An example of the Spectrum Analyzer tab for PDAs is displayed in Figure 122. For additional information about the Spectrum Analyzer feature, see Monitoring the RF Environment on Page 365.



PDA => Spectrum Analyzer

5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5

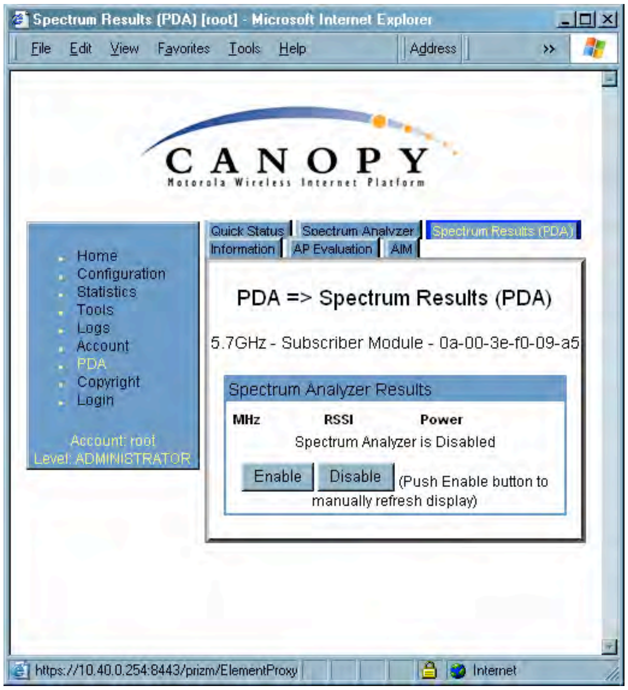
Spectrum Analyzer Tool

Spectrum Analyzer is Disabled

(Push Enable button to manually refresh display)

Figure 122: PDA Spectrum Analyzer tab of SM, example

Examples of the Spectrum Results and Information tabs for PDAs are shown in Figure 123 and Figure 124.



PDA => Spectrum Results (PDA)

5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5

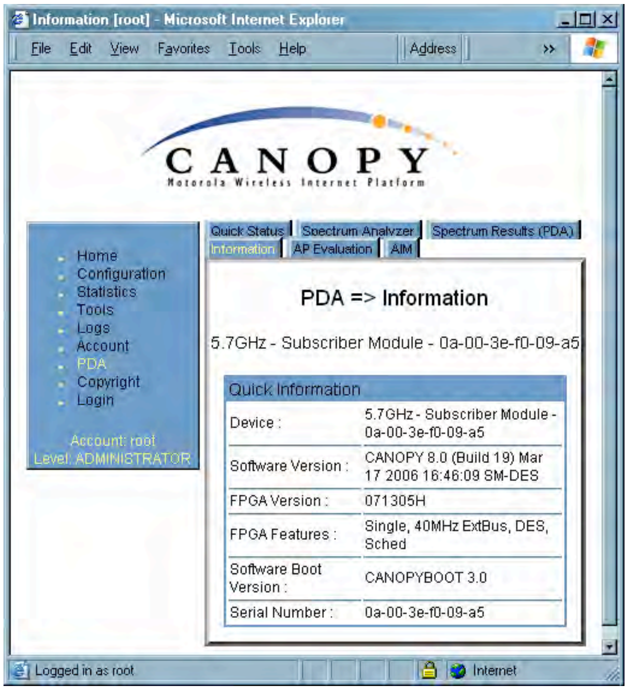
Spectrum Analyzer Results

MHz	RSSI	Power

Spectrum Analyzer is Disabled

(Push Enable button to manually refresh display)

Figure 123: PDA Spectrum Results tab of SM, example



PDA => Information

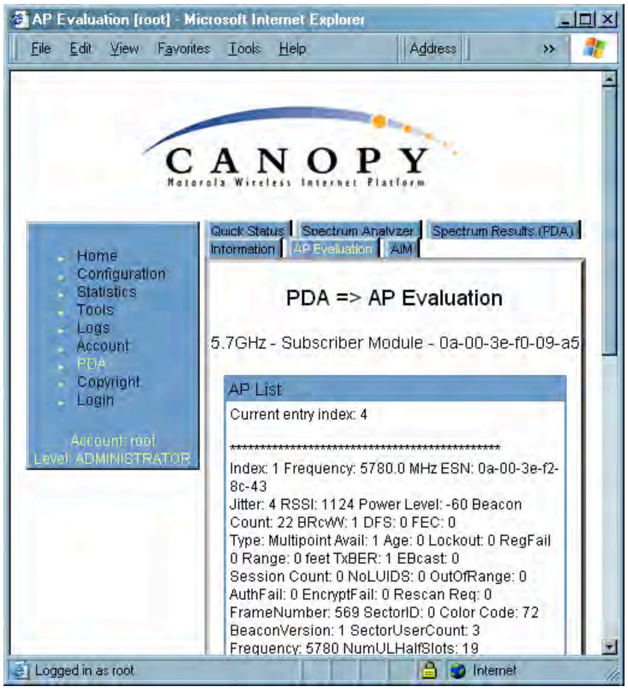
5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5

Quick Information

Device :	5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5
Software Version :	CANOPY 8.0 (Build 19) Mar 17 2006 16:46:09 SM-DES
FPGA Version :	071305H
FPGA Features :	Single, 40MHz ExtBus, DES, Sched
Software Boot Version :	CANOPYBOOT 3.0
Serial Number :	0a-00-3e-f0-09-a5

Figure 124: PDA Information tab of SM, example

Examples of the AP Evaluation and Aim tabs for PDAs are shown in Figure 125 and Figure 126.



PDA => AP Evaluation

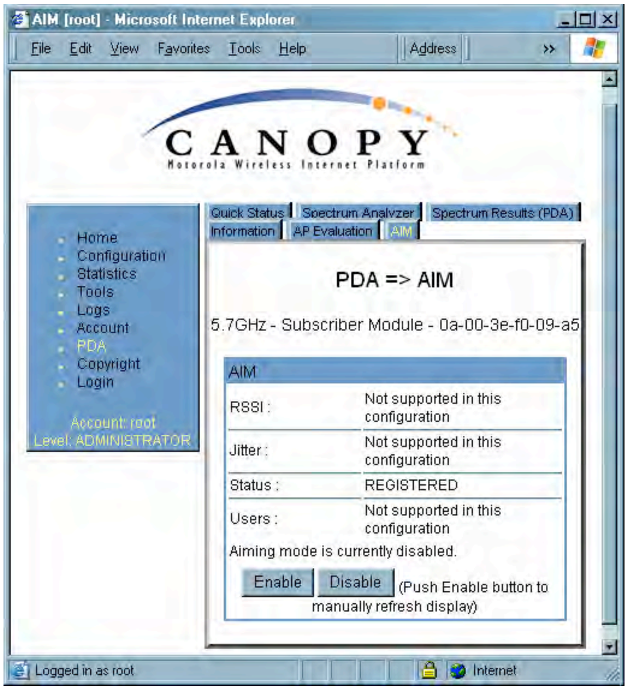
5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5

AP List

```
Current entry index: 4

************************************************
Index: 1 Frequency: 5780.0 MHz ESN: 0a-00-3e-f2-
8c-43
Jitter: 4 RSSI: 1124 Power Level: -60 Beacon
Count: 22 BRcvW: 1 DFS: 0 FEC: 0
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail
0 Range: 0 feet TxBER: 1 EBcast: 0
Session Count: 0 NoLUIDS: 0 OutOfRange: 0
AuthFail: 0 EncryptFail: 0 Rescan Req: 0
FrameNumber: 569 SectorID: 0 Color Code: 72
BeaconVersion: 1 SectorUserCount: 3
Frequency: 5780 NumULHalfSlots: 19
```

Figure 125: PDA AP Evaluation tab of SM, example



PDA => AIM

5.7GHz - Subscriber Module - 0a-00-3e-f0-09-a5

AIM

RSSI :	Not supported in this configuration
Jitter :	Not supported in this configuration
Status :	REGISTERED
Users :	Not supported in this configuration

Aiming mode is currently disabled.

Enable Disable (Push Enable button to manually refresh display)

Figure 126: PDA Aim tab of SM, example

19.2 INSTALLING AN AP

To install the Canopy AP, perform the following steps.

Procedure 19: Installing the AP

1. Begin with the AP in the powered-down state.
2. Choose the best mounting location for your particular application. Modules need not be mounted next to each other. They can be distributed throughout a given site. However, the 60° offset must be maintained. Mounting can be done with stainless steel hose clamps or another equivalent fastener.
3. Align the AP as follows:
    a. Move the module to where the link will be unobstructed by the radio horizon and no objects penetrate the Fresnel zone. (The Canopy System Calculator page AntennaElevationCalcPage.xls automatically calculates the minimum antenna elevation that is required to extend the radio horizon to the other end of the link. The Canopy System Calculator page FresnelZoneCalcPage.xls automatically calculates the Fresnel zone clearance that is required between the visual line of sight and the top of a high-elevation object.)
    b. Use a local map, compass, and/or GPS device as needed to determine the direction that one or more APs require to each cover the intended 60° sector.
    c. Apply the appropriate degree of downward tilt. (The Canopy System Calculator page DowntiltCalcPage.xls automatically calculates the angle of antenna downward tilt that is required.)
    d. Ensure that the nearest and furthest SMs that must register to this AP are within the beam coverage area. (The Canopy System Calculator page BeamwidthRadiiCalcPage.xls automatically calculates the radii of the beam coverage area.)
4. Using stainless steel hose clamps or equivalent fasteners, lock the AP in the proper direction and downward tilt.
5. Remove the base cover of the AP. (See Figure 52 on Page 178.)
6. Attach the cables to the AP.
   (See Procedure 5 on Page 184.)

NOTE: When power is applied to a Canopy module or the unit is reset on the web-based interface, the module requires approximately 25 seconds to boot. During this interval, self-tests and other diagnostics are being performed. See Table 44 on Page 179.

============================ **end of procedure** ============================

19.3 INSTALLING A CONNECTORIZED FLAT PANEL ANTENNA

To install a connectorized flat panel antenna to a mast or structure, follow instructions that the manufacturer provides. Install the antenna safely and securely, consistent with industry practices.

The Universal Mounting Bracket available from Motorola (Part Number SMMB-1 and consisting of a mounting bracket and L-shaped aluminum tube) holds one Canopy module, but cannot hold both the module and a connectorized antenna. The SMMB-2 is a heavy duty bracket that can hold both a 900-MHz module and its connectorized antenna. See Module Support Brackets on Page 59.

IMPORTANT!
Connectorized antennas *require* professional installation.

The professional installer is responsible for

- selection of an antenna that the regulatory agency has approved for use with the Canopy 900-MHz AP and SM.
- setting of the gain consistent with regulatory limitations and antenna specifications.
- ensuring that the polarity—horizontal or vertical—is identical on both ends of the link. (This may be less obvious where an integrated antenna is used on one end and a connectorized on the other.)
- use of moisture sealing tape or wrap to provide long-term integrity for the connection.

19.4 INSTALLING A GPS ANTENNA

The following information describes the recommended tools and procedures to mount the GPS antenna.

Recommended Tools for GPS Antenna Mounting

The following tools may be needed for mounting the GPS antenna:

- 3/8” nut driver
- 12” adjustable wrench
- 7/16” wrench
- Needle-nose pliers

Mounting a GPS Antenna

Perform the following procedure to mount a GPS antenna.

Procedure 20: Mounting the GPS antenna

1. Ensure that the mounting position
    - has an unobstructed view of the sky to 20º above the horizon.
    - *is not* the highest object at the site. (This is important for lightning protection.)
    - *is not* further than 100 feet (30.4 meters) of cable from the CMM2 or CMMmicro.
2. Select a pole that has an outside diameter of 1.25 to 1.5 inches (3 to 4 cm) to which the GPS antenna bracket can be mounted.
3. Place the U-bolts (provided) around the pole as shown in Figure 127.
4. Slide the GPS antenna bracket onto the U-bolts.
5. Slide the ring washers (provided) onto the U-bolts.

6. Slide the lock washers (provided) onto the U-bolts.
7. Use the nuts (provided) to securely fasten the bracket to the U-bolts.

============================ **end of procedure** ============================

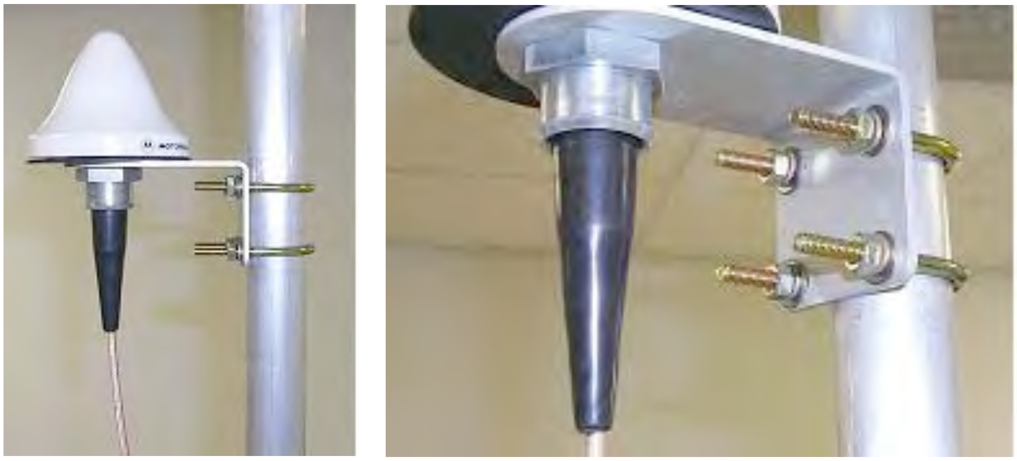


Figure 127: Detail of GPS antenna mounting

19.4.1 Recommended Materials for Cabling the GPS Antenna

The following materials are required for cabling the GPS antenna:

- up to 100 feet (30.4 meters) of LMR200 coaxial cable
- 2 Times Microwave N-male connectors (Times Microwave P/N TC-200-NM) or equivalent connectors.

19.4.2 Cabling the GPS Antenna

Connect the GPS coax cable to the female N-connector on the GPS antenna.

19.5 INSTALLING A CMM2

Ensure that you comply with standard local or national electrical and climbing procedures when you install the CMM2.

19.5.1 CMM2 Installation Temperature Range

Install the CMM2 outside only when temperatures are above –4° F (–20° C). The bulkhead connector and the bushings and inserts in the bulkhead connector are rated for the full –40° to +131° F (–40° to +55° C) range of the CMM2. However, for dynamic operations (loosening, tightening, and inserting), they are compliant at, and rated for, only temperatures at or above –4° F (–20° C).

19.5.2 Recommended Tools for Mounting a CMM2

The following tools may be needed for mounting the CMM2:

- 3/8” nut driver
- 12” adjustable wrench
- 14-mm wrench for pole-mounting
- needle-nose pliers

19.5.3 Mounting a CMM2

Perform the following procedure to mount the CMM2.

Procedure 21: Mounting the CMM2

1. Ensure that the mounting position
   - *is not* further than 328 feet (100 meters) of cable from the furthest AP or BH that the CMM2 will serve.
   - *is not* closer than 10 feet (3 meters) to the nearest AP or BH.
   - *is not* further than 100 feet (30.4 meters) of cable from the intended mounting position of the GPS antenna.
   - allows you to fully open the door of the CMM2 for service.
2. Select a support structure to which the flanges of the CMM2 can be mounted.
3. If the support structure is a wall, use screws or bolts (neither is provided) to attach the flanges to the wall.
4. If the support structure is an irregular-shaped object, use adjustable stainless steel bands (provided) to attach the CMM2 to the object.
5. If the support structure is a pole that has an outside diameter of 3 to 8 cm, or 1.25 to 3 inches, use a toothed V-bracket (provided) to
   a. attach the V-bracket to the pole as shown in Figure 128.
   b. attach the CMM2 flanges to the V-bracket.

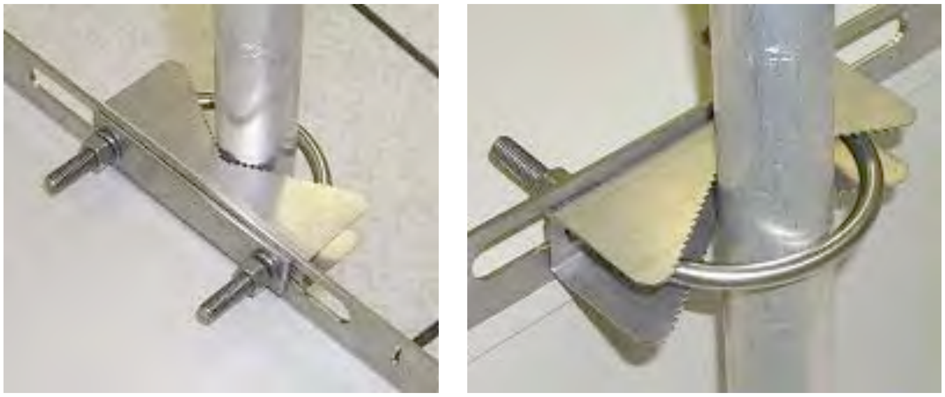


Figure 128: Detail of pole mounting

========================== **end of procedure** ==========================

19.5.4 Cabling a CMM2

> *IMPORTANT!*
> Where you deploy CMM2s, one AP in each AP cluster must be connected to the master port on the CMM2, and each module connected to a CMM2 must be configured to **Sync to Received Signal (Timing Port)**. If either is not done, then the GPS receiver sends no sync pulse to the remaining ports.

Perform the following procedure to attach the CMM2 cables on both ends:

Procedure 22: Cabling the CMM2

1. Carefully review the practices recommended in Best Practices for Cabling on Page 182.
2. Remove the base cover from any AP or BH that is to be connected to this CMM2. See Figure 52 on Page 178.
3. Remove the GPS sync cable knockout from the base cover.
4. For any AP that is to be connected to this CMM2, set the AP **Sync Input** Configuration Page parameter to the **Sync to Received Signal (Timing Port)** selection.
5. Review the schematic drawing inside the CMM2.

6. Set the 115-/230-volt switch in the CMM2 consistent with the power source. See Figure 129.

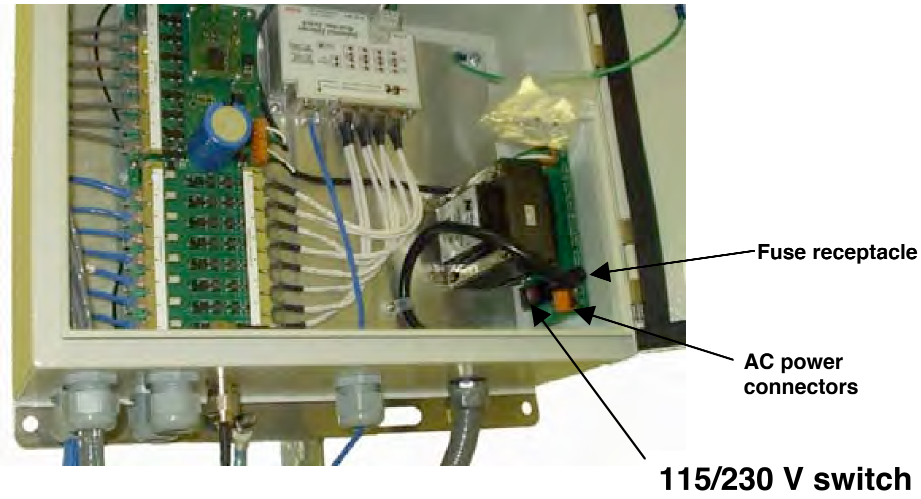


Figure 129: Location of 115-/230-volt switch

CAUTION!
Failure to set the 115-/230-volt switch correctly can result in damage to equipment.

IMPORTANT!
The AC power connectors are labeled **N** for Neutral, **L** for Line, and **PE** for Protective Earth (PE) ⏚ or ground. The maximum thickness of wire to be used is 4 mm^2 or 12 AWG.

7. Route the Ethernet cables from the APs and or BHs to the CMM2.

   The strain relief plugs on the CMM2 have precut holes. Each hole of the strain relief is designed to hold two CAT 5 UTP cables or one shielded cable. The Ethernet cables have RJ-45 (standard Ethernet) connectors that mate to corresponding ports inside the CMM2.

   These ports are labeled **J3**. Eight J3 ports are available on the CMM2 to accommodate any combination of APs and BHs.

   The logical connections in the CMM2 are displayed in Figure 130.

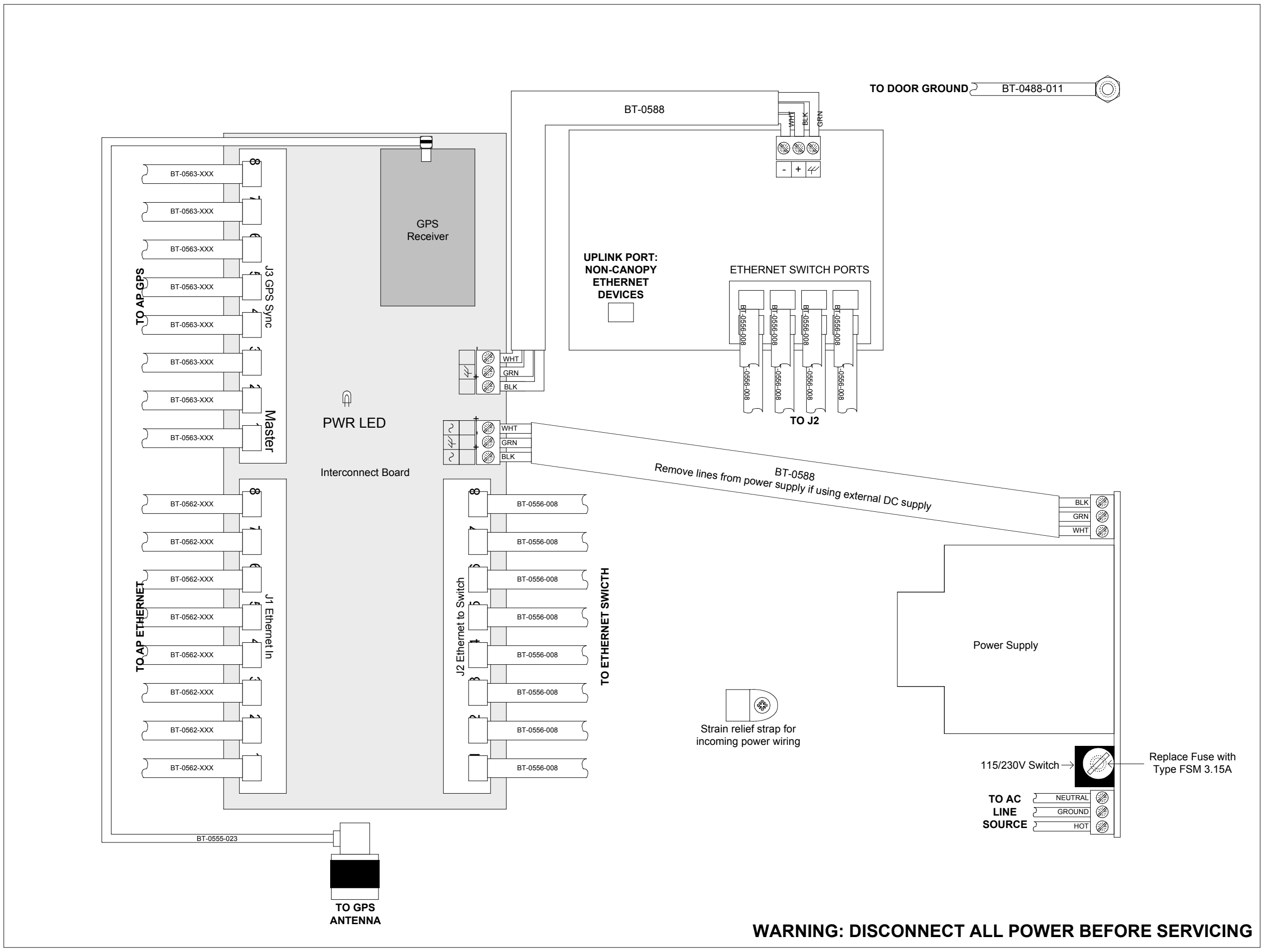


Figure 130: Layout of logical connections in CMM2

8. Connect the Ethernet cable from the first AP or BH to the **Port 1** in the J3 ports in the CMM2. This port is the *master* Ethernet port for the CMM2 and should be connected first in all cases. Figure 131 on Page 341 is a photograph of a properly wired CMM2.

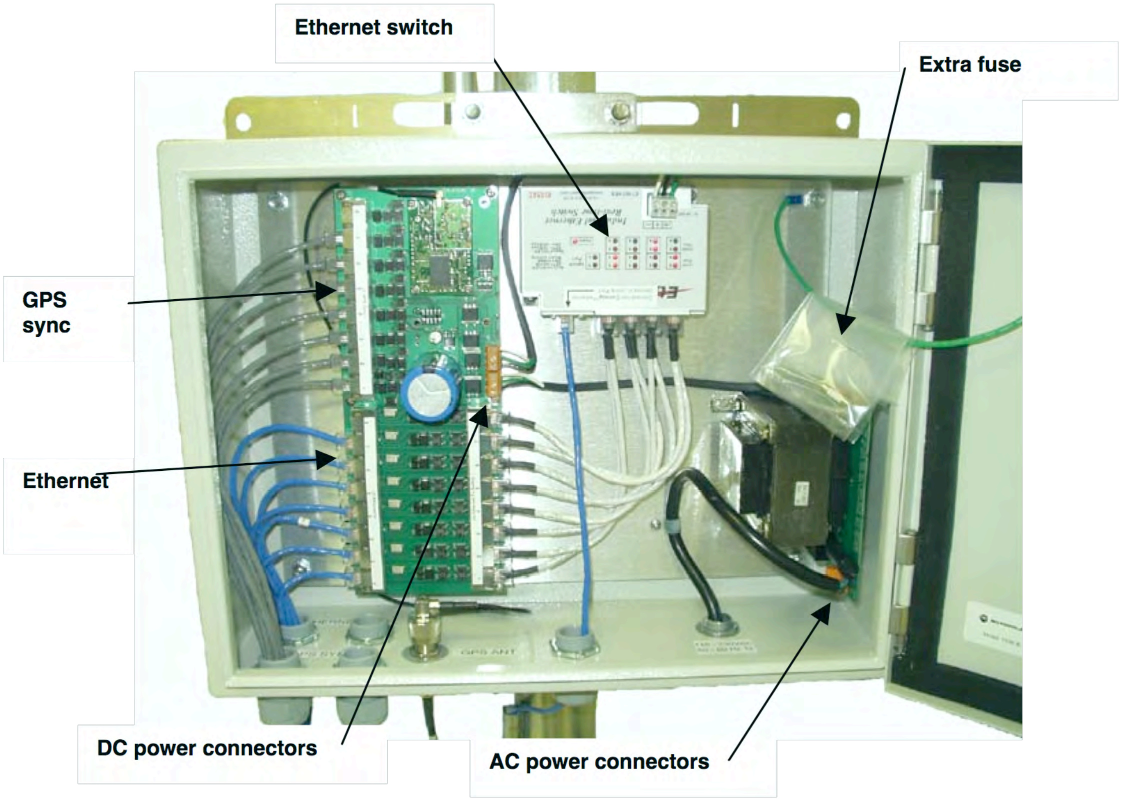


Figure 131: Canopy CMM2, front view

9. Connect the remaining Ethernet cables to the remaining J3 ports.
10. Route the GPS sync (serial) cables from the APs to the CMM2.

    The GPS sync cables have 6-conductor RJ-11 connectors that mate to corresponding ports inside the CMM2.

    These ports are labeled **J1**. Eight J1 ports are available on the CMM2 to accommodate any combination of APs and BHs.
11. Connect the GPS sync cable from the first AP or BH to the **Port 1** in the J1 ports in the CMM2. See Figure 131 on Page 341.

    This port is the *master* GPS sync port for the CMM2 and should be connected first in all cases. This is necessary to initialize the GPS on the CMM2.
12. Connect the remaining GPS sync cables to the remaining J1 ports.
13. If this CMM2 requires network connection, perform the following steps:
    a. Route a network cable into the CMM2.
    b. Connect to the uplink port on the switch.
    c. Properly ground (connect to Protective Earth [PE] ⏚) the Ethernet cable. The Canopy Surge Suppressor provides proper grounding for this situation. ***NOTE:*** Instructions for installing a Canopy Surge Suppressor are provided in Procedure 28 on Page 346.

14. Connect GPS coaxial cable to the N-connector on the outside of the CMM2. See Figure 53 on Page 180.
15. Connect AC or DC power to the CMM2, consistent with Figure 130 on Page 340.
    NOTE: When power is applied, the following indicators are lighted:
    - the power LED on the Ethernet switch
    - the green LED on the circuit board, as shown in Figure 132.

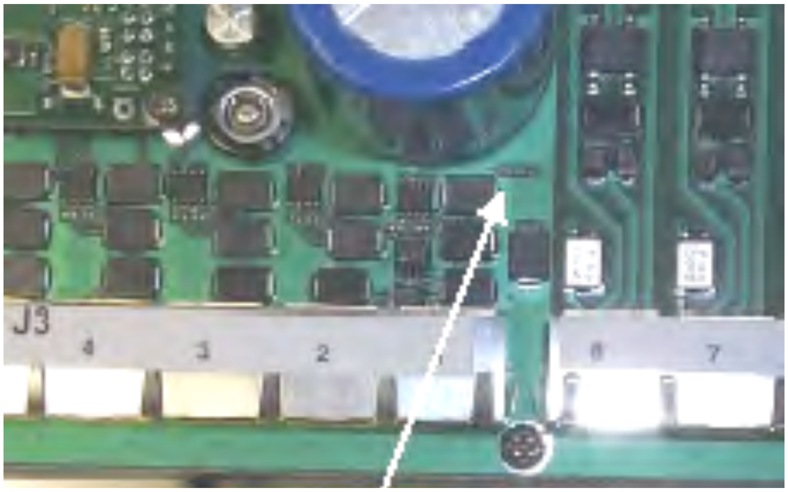


Figure 132: Port indicator LED on Ethernet switch

16. Verify that each port indicator LED on the Ethernet switch is lit (each AP or BH is reliably connected to the Ethernet switch).
17. Replace the base cover on each AP or BH.
18. Close and lock the CMM2.

============================ **end of procedure** ============================

19.5.5 Verifying CMM2 Connections

To verify the CMM2 connections after the APs and or BHs have been installed, perform the following steps:

Procedure 23: Verifying CMM2 connections

1. Access the web-based interface for each AP or BHM by opening http://<ip-address>, where the <*ip-address*> is the address of the individual module.
2. In the General Status tab of the Home page, verify that the System Time field displays the time in GMT.

============================ **end of procedure** ============================

19.6 INSTALLING A CMMmicro

Ensure that you comply with standard local or national electrical and climbing procedures when you install the CMMmicro.

19.6.1 CMMmicro Temperature Range

Install the CMMmicro outside only when temperatures are above –4° F (–20° C). The bulkhead connector and the bushings and inserts in the bulkhead connector are rated for the full –40° to +131° F (–40° to +55° C) range of the CMMmicro. However, for dynamic operations (loosening, tightening, and inserting), they are compliant at, and rated for, only temperatures at or above –4° F (–20° C).

19.6.2 Recommended Tools for Mounting a CMMmicro

The following tools may be needed during installation:

- 3/8” nut driver
- 12” adjustable wrench
- 14-mm wrench for installation of pole-mounting brackets
- needle-nose pliers

19.6.3 Mounting a CMMmicro

Perform the following procedure to mount the CMMmicro.

Procedure 24: Mounting the CMMmicro

1. Ensure that the mounting position
   - *is not* further than 328 feet (100 meters) from the furthest AP or BH that the CMMmicro will serve.
   - *is not* closer than 10 feet (3 meters) to the nearest AP or BH.
   - *is not* further than 100 feet (30.5 meters) of cable from the intended mounting position of the GPS antenna.
   - allows you to fully open the door for service.
2. Select a support structure to which the flanges can be mounted.
3. If the support structure is a wall, use screws or bolts (neither is provided) to attach the flanges to the wall.

   If the support structure is an irregular-shaped object, use adjustable stainless steel bands (provided) to attach the CMMmicro to the object.
4. If the support structure is a pole that has an outside diameter of 1.25 to 3 inches (3 to 8 cm), use a toothed V-bracket (provided) to
   d. attach the V-bracket to the pole as shown in Figure 128 on Page 338.
   e. attach the CMMmicro flanges to the V-bracket.

=========================== **end of procedure** ===========================

19.6.4 Installing the Power Supply for the CMMmicro

Install the CMMmicro power converter in only a hut, wiring closet, or weatherized NEMA-approved enclosure. This is imperative to keep moisture away from the power converter, not to shield it from harsh temperatures.

> ***WARNING!***
> Although the output of the power converter is 24 V, the 100-W power rating classifies the converter as a Class 2 electric device. For this reason, whenever you work on power in the CMMmicro, you must *first* disconnect the DC converter from the AC power source.

Perform the following procedure to install the provided power supply.

Procedure 25: Installing the Power Supply for the CMMmicro

1. Connect the 6-ft (2-m) AC power cord to the power converter (but not yet to an AC receptacle).
2. Select the length of power cord as follows:
   a. If either mounting the unit inside with the power converter or outside within 9 ft (2.8 m) of the power converter, select the 10-ft (3-m) DC power cord (rated for outdoor use).
   b. If mounting the unit outside and further than 9 ft (2.8 m) from the power converter, ensure that this additional length of cord is either UV-resistant or shielded from UV rays.
      - use a terminal block, connector, or splice to add the additional length.
      - protect the terminal block, connector, or splice (as inside a weatherized enclosure, for example).

Table 55: Wire size for CMMmicro power runs of longer than 9 feet (2.8 m)

DC Power Cord Length	Proper Wire Size
9−90 ft (3−25 m)	12 AWG (4 mm^2)
91−145 ft (26−45 m)	10 AWG (6 mm^2)
146−230 ft (46−70 m)	8 AWG (10 mm^2)
>230 ft (>70 m)	6 AWG (16 mm^2)

3. Refer to Figure 76: CMMmicro connections on Page 220.
4. Feed the power cord through the bulkhead connector of the CMMmicro.
5. Connect the converter lead whose insulation has a white stripe to +V on the CMMmicro terminal block.
6. Connect the converter lead whose insulation is solid black to −V on the CMMmicro terminal block.

============================ **end of procedure** ============================

19.6.5 Cabling a CMMmicro

Perform the following procedure to attach the CMMmicro cables on both ends:

Procedure 26: Cabling the CMMmicro

1. Remove the base cover from any AP or BH that is to be connected to this CMMmicro. See Figure 52 on Page 178.

2. Review the schematic drawing inside the CMMmicro and see Figure 76: CMMmicro connections on Page 220.
3. Note that the inserts in the bulkhead connector bushings have precut holes.
4. Remove the hard silicon spacer.
5. Route the Ethernet cables from the APs through the bulkhead connectors to the Ethernet switch inside the CMMmicro.
6. If the BH at this site is a 30/60- or 150/300-Mbps BH
   a. connect the BH outdoor unit (ODU) to the ODU port of the power indoor unit (PIDU).
   b. connect the PIDU to an unpowered port of the CMMmicro.

   If the BH is of another modulation rate, route the Ethernet cables from the BH through the bulkhead connectors to the Ethernet switch in the CMMmicro.
7. If the site has a wired network feed, route the cable into the CMMmicro and connect it to an *unpowered* port on the switch.
8. Mount a Canopy surge suppressor at a low point of the network feed and connect the surge suppressor to solid ground.
9. On the door label, record the MAC and IP addresses of the CMMmicro and all connected equipment.
10. Consistent with practices in your company, note the above information to add later to the company equipment database.
11. Connect the GPS coax cable from the GPS antenna to the female BNC connector in the CMMmicro.
12. If this CMMmicro requires network connection, perform the following steps:
    a. Route a network cable into the CMMmicro.
    b. Connect to the uplink port on the switch.
    c. Properly ground (connect to Protective Earth [PE] ⏚) the Ethernet cable. The Canopy Surge Suppressor provides proper grounding for this situation. ***NOTE:*** Instructions for installing a Canopy Surge Suppressor are provided as part of Procedure 28 on Page 346.
13. Connect the DC power cable to the CMMmicro.
14. Plug the DC converter into an AC receptacle.
15. Verify that the LEDs light.

============================ **end of procedure** ============================

19.6.6 Verifying CMMmicro Connections

To verify the CMMmicro connections after the APs and or BHs have been installed, perform the following steps.

Procedure 27: Verifying CMMmicro connections

1. Access the web-based interface for each AP or BH by opening http://<ip-address>, where the <*ip-address*> is the address of the individual module.
2. In the Status page, verify that the time is expressed in GMT.
3. In the menu on the left-hand side of the web page, click on **GPS Status**.
4. Verify that the AP or BH is seeing and tracking satellites. (To generate the timing pulse, the module must track at least 4 satellites.)

============================== **end of procedure** ==============================

19.7 INSTALLING AN SM

Installing a Canopy SM consists of two procedures:

- Physically installing the SM on a residence or other location and performing a course alignment using the alignment tone (Procedure 28).
- Verifying the AP to SM link and finalizing alignment using review of power level and jitter, link tests, and review of registration and session counts (Procedure 29 on Page 349).

Procedure 28: Installing the SM

1. Choose the best mounting location for the SM.
2. Select the type of mounting hardware appropriate for this location. (For mounting 2.4, 5.2, 5.4, and 5.7 GHz SMs, Motorola offers the SMMB-1 mounting bracket. For mounting 900 MHz SMs, Motorola offers the SMMB-2 mounting bracket.)
3. Remove the base cover of the SM. (See Figure 52 on Page 178.)
4. Terminate the UV outside grade Category 5 Ethernet cable with an RJ-45 connector, and connect the cable to the SM. (See Procedure 8 on Page 192.)
5. Optionally, attach the SM to the arm of the Canopy Passive Reflector dish assembly as shown in Figure 133.

> ***RECOMMENDATION:***
> A reflector in this instance reduces the beamwidth to reduce interference. The arm is molded to receive and properly aim the module relative to the aim of the dish. Use stainless steel hose clamps for the attachment.

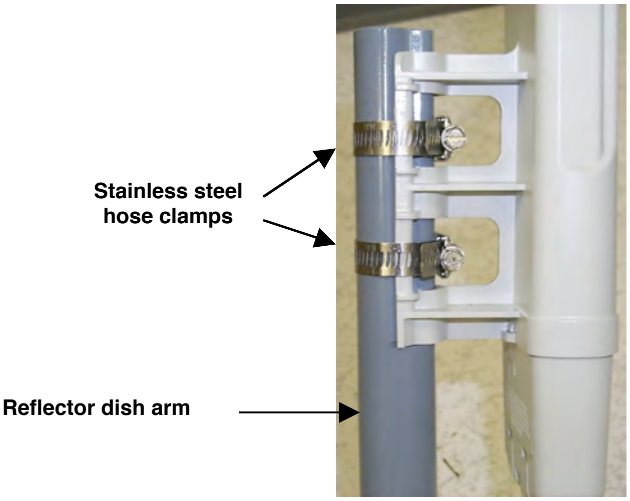


Figure 133: SM attachment to reflector arm

6. Use stainless steel hose clamps or equivalent fasteners to lock the SM into position.
   NOTE: The SM grounding method is shown in Figure 134.

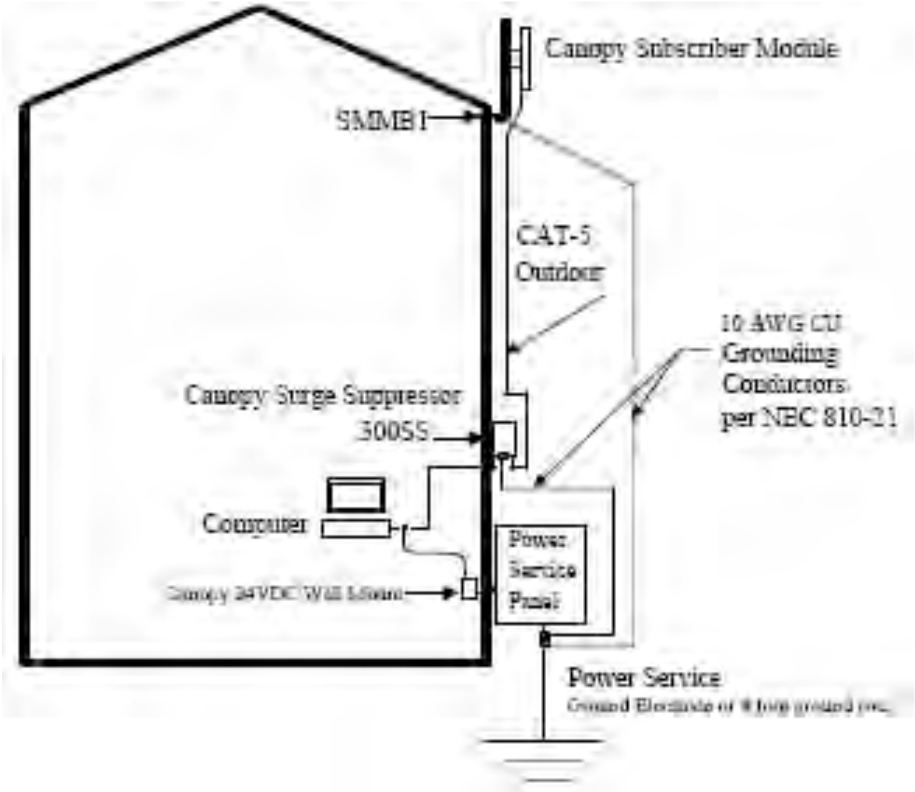
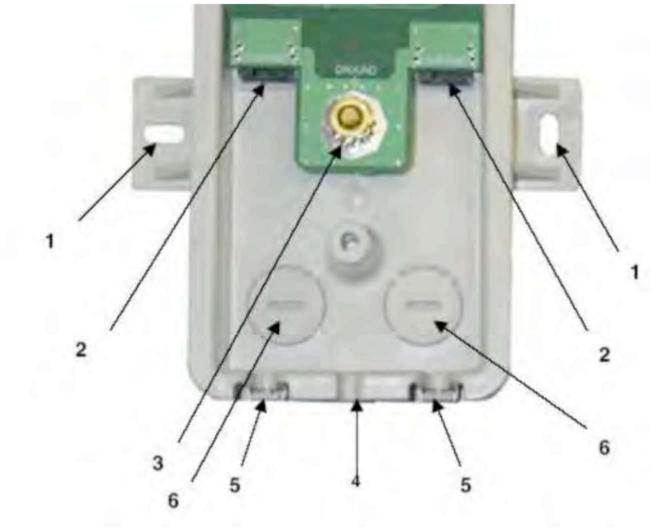


Figure 134: SM grounding per NEC specifications

7. Remove the cover of the 300SS Surge Suppressor.



KEY TO CALLOUTS

1 **Holes—for mounting the Surge Suppressor to a flat surface (such as an outside wall). The distance between centers is 4.25 inches (108 mm).**

2 **RJ-45 connectors—One side (neither side is better than the other for this purpose) connects to the Canopy product (AP, SM, BHM, BHS, or cluster management module). The other connects to the AC adaptor's Ethernet connector.**

3 **Ground post—use heavy gauge (10 AWG or 6 mm^2) copper wire for connection. Refer to local electrical codes for exact specifications.**

4 **Ground Cable Opening—route the 10 AWG (6 mm^2) ground cable through this opening.**

5 **CAT-5 Cable Knockouts—route the two CAT-5 cables through these openings, or alternatively through the Conduit Knockouts.**

6 **Conduit Knockouts—on the back of the case, near the bottom. Available for installations where cable is routed through building conduit.**

Figure 135: Internal view of Canopy 300SS Surge Suppressor

8. With the cable openings facing downward, mount the 300SS to the *outside* of the subscriber premises, as close to the point where the Ethernet cable penetrates the residence or building as possible, and as close to the grounding system (Protective Earth) as possible.
9. Using diagonal cutters or long nose pliers, remove the knockouts that cover the cable openings to the 300SS.
10. Connect an Ethernet cable from the power adapter (located inside the residence or building, outward through the building penetration) to either RJ-45 port of the 300SS.
11. Connect another Ethernet cable from the other RJ-45 port of the 300SS to the Ethernet port of the SM.
12. Refer to Grounding SMs on Page 172.

13. Wrap an AWG 10 (or 6mm^2) copper wire around the Ground post of the 300SS.
14. Tighten the Ground post locking nut in the 300SS onto the copper wire.
15. Securely connect the copper wire to the grounding system (Protective Earth) according to applicable regulations.
16. Connect a ground wire to the 300SS.
17. Replace the cover of the 300SS surge suppressor.
18. For coarse alignment of the SM, use the Audible Alignment Tone feature as follows:
    a. Set the **2X Rate** parameter in the SM to **Disable**.
    b. At the SM, connect the RJ-11 6-pin connector of the Alignment Tool Headset to the RJ-11 utility port of the SM.

       Alternatively, instead of using the Alignment Tool Headset, use an earpiece or small battery-powered speaker connected to Pin 5 (alignment tone output) and Pin 6 (ground) of an RJ-11 connector.

    c. Listen to the alignment tone for
       - pitch, which indicates greater signal power (RSSI/dBm) by higher pitch.
       - volume, which indicates better signal quality (lower jitter) by higher volume.

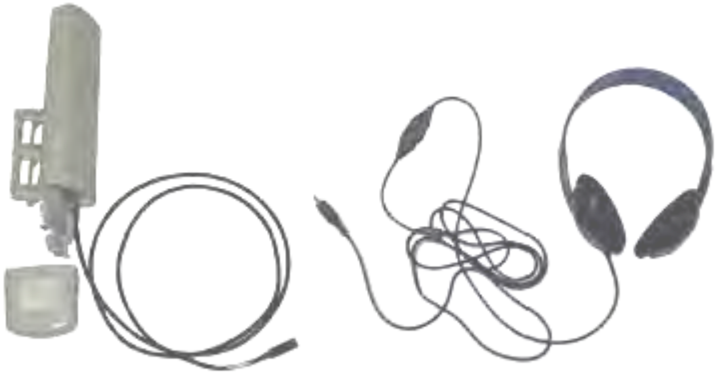


Figure 136: Audible Alignment Tone kit, including headset and connecting cable

    d. Adjust the module slightly until you hear the highest pitch and highest volume.
    e. If the Configuration web page of the SM contains a **2X Rate** parameter, set it back to **Enable**.
19. When you have achieved the best signal (highest pitch, loudest volume), lock the SM in place with the mounting hardware.

=========================== **end of procedure** ===========================

19.8 VERIFYING AN AP-SM LINK

To verify the AP-SM link after the SM has been installed, perform the following steps.

Procedure 29: Verifying performance for an AP-SM link

1. Using a computer (laptop, desktop, PDA) connected to the SM, open a browser and access the SM using the default IP address of http://169.254.1.1 (or the IP address configured in the SM, if one has been configured.)
2. On the General Status tab of the Home page in the SM (shown in Figure 66 on Page 198), look for **Power Level** and **Jitter**.
   IMPORTANT: The received **Power Level** is shown in dBm and should be maximized. **Jitter** should be minimized. However, better/lower jitter should be favored over better/higher dBm. For example, if coarse alignment gives an SM a power level of −75 dBm and a jitter measurement of 5, and further refining the alignment drops the power level to −78 dBm and the jitter to 2 or 3, the latter would be better, with the following caveats:
   - When the receiving link is operating at 1X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 4.
   - When the receiving link is operating at 2X, the **Jitter** scale is 0 to 15 with desired jitter between 0 and 9.

> *NOTE:*
> For historical reasons, **RSSI** is also shown and is the unitless measure of power. The best practice is to use **Power Level** and ignore **RSSI**, which implies more accuracy and precision than is inherent in the measurement.

3. Fine-adjust the SM mounting, if needed, to improve **Jitter** or **Power Level**.
4. Click the Link Capacity Test tab of the Tools web page in the SM.
   NOTE: Use of this tool is described under Using the Link Capacity Test Tool (All) on Page 434.
5. Perform several link tests of 10-second duration as follows:
   a. Type into the **Duration** field how long (in seconds) the RF link should be tested.
   b. Leave the **Packet Length** field (when present) set to the default of 1522 bytes or type into that field the packet length at which you want the test conducted.
   c. Leave the **Number of Packets** field set to 0 (to flood the link).
   d. Click the **Start Test** button.
   e. View the results of the test.
6. If these link tests fail to consistently show 90% or greater efficiency in 1X operation or 50 to 60% efficiency in 2X, troubleshoot the link, using the data as follows:
   - If the downlink is consistently 90% efficient, but the uplink is only 40%, this indicates trouble for the SM transmitting to the AP. Have link tests performed for nearby SMs. If their results are similar, investigate a possible source of interference local at the AP.
   - If the uplink is consistently 90% efficient, but the downlink is only 40%, this indicates trouble for the AP transmitting to the SM. Investigate a possible source of interference near the SM.

   If these link tests consistently show 90% or greater efficiency in 1X operation, or 50 to 60% efficiency in 2X operation, in both uplink and downlink, continue this procedure.